Monday, October 25
4:30pm-6:00pm

410 - Data Breach Preparedness & Prevention

Jonathan Ellman
General Counsel
Litle & Co.

Charles Kallenbach
General Counsel
Heartland Payment Systems, Inc.

Douglas Meal
Partner
Ropes & Gray

Session 410

Faculty Biographies

Jonathan Ellman
Litle & Co.

Charles Kallenbach

Charles H.N. Kallenbach is general counsel and chief legal officer of Heartland Payment Systems Inc. He is responsible for securities compliance, corporate governance, mergers & acquisitions, litigation management, corporate transactions, and other legal, regulatory and compliance matters.

Prior to joining Heartland, Mr. Kallenbach was senior vice president, legal and regulatory, and secretary for SunCom Wireless Holdings Inc., an NYSE-listed wireless communications company that was acquired by T-Mobile. Prior to joining SunCom, Mr. Kallenbach was vice president and general counsel for Eureka Broadband Corporation (now part of Broadview Networks Holdings Inc.). He was also general counsel of 2nd Century Communications and in-house counsel at e.spire Communications. Mr. Kallenbach started his legal career in private practice with Jones Day and later Swidler & Berlin (now part of Bingham McCutchen) in Washington, D.C. He also served as legislative assistant to United States Senator Arlen Specter.

Mr. Kallenbach received a BA from the University of Pennsylvania and a JD from New York University School of Law.

Douglas Meal
Ropes & Gray

What To Do If Compromised

Visa Inc. Fraud Control and Investigations Procedures

Version 2.0 (Global)
Effective February 2010
Visa Public

Contents

Introduction

What constitutes a security incident? The answer to this question is crucial to any organization looking to minimize the impact an incident might have on its business operations.

In general, incidents may be defined as deliberate electronic attacks on communications or information processing systems. Whether initiated by a disgruntled employee, a malicious competitor, or a misguided hacker, deliberate attacks often cause damage and disruption to the payment system. How you respond to and handle an attack on your company's information systems will determine how well you will be able to control the costs and consequences that could result. For these reasons, the extent to which you prepare for security incidents, and work with Visa Inc., will be vitally important to the protection of your company's key information.

In the event of a security incident, Visa clients and their agents must take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa, and report investigation findings to Visa.[1]

The *What To Do If Compromised* guide is intended for Visa clients (i.e., acquirers and issuers), merchants, agents, and third-party service providers. It contains step-by-step instructions on how to respond to a security incident and provides specific time frames for the delivery of information or reports outlining actions taken by Visa, its clients, and its agents.

In addition to the general instructions provided here, Visa may also require an investigation that includes, but is not limited to, access to premises and all pertinent records including copies of analysis.

[1] Visa International Operating Regulations: Member Investigation of Suspected Fraud (2.1.A.1); Additional Investigation (2.1.A.2); Member Reporting of Loss or Theft of Information (2.1.E.2).

Identifying and Detecting Security Breaches

It is often difficult to detect when a system has been attacked or an intrusion has taken place. Distinguishing normal events from those that are related to an attack or intrusion is a critical part of maintaining a secure payment processing environment.

Security breaches come in many different forms and, while detecting them may be challenging, there are certain signs that tend to appear when a security breach has occurred:

- Unknown or unexpected outgoing Internet network traffic from the payment card environment
- Presence of unexpected IP addresses on store and wireless networks
- Unknown or unexpected network traffic from store to headquarter locations
- Unknown or unexpected services and applications configured to launch automatically on system boot
- Unknown files, software and devices installed on systems
- Anti-virus programs malfunctioning or becoming disabled for unknown reasons
- Failed login attempts in system authentication and event logs
- Vendor or third-party connections made to the cardholder environment without prior consent and/or a trouble ticket
- SQL Injection attempts in web server event logs
- Authentication event log modifications (i.e., unexplained event logs are being deleted)
- Suspicious after-hours file system activity (i.e., user login or after-hours activity to Point-of-Sale (“POS”) server)
- Presence of .zip, .rar, .tar, and other types of unidentified compressed files containing cardholder data
- Presence of a rootkit, which hides certain files and processes in, for example, Explorer, the Task Manager, and other tools or commands
- Systems rebooting or shutting down for unknown reasons
- If you are running Microsoft, check Windows registry settings for hidden malicious code. (**Note:** Make sure you back up your registry keys before making any changes and consult with Microsoft Help and Support).

Attack Vectors

The following are examples of attack vectors that hackers use to gain unauthorized access to organization's systems and steal sensitive information, such as payment card data and passwords.

SQL Injection Attacks

SQL injection is a technique used to exploit Web-based applications that use client-supplied data in SQL queries. SQL injection attacks can occur as a result of unpatched Web servers, improperly designed applications (i.e., incorrectly filtered escape characters or error-type handling) or poorly configured Web and database servers.

The SQL attack methods most recently detected were targeted against Websites and Web applications that were improperly designed or resided on unpatched systems, making them susceptible to attack. These latest SQL injection attacks pose serious additional risks to cardholder data stored or transmitted within systems (e.g., Microsoft and UNIX-based) and networks connected to the affected environment.

Improperly Segmented Network Environment

Payment card account information has been compromised at organizations that lack proper network segmentation. This attack method originates on the Internet, resulting in penetration to the organization's payment card environment and often leading to costly remediation efforts and increased fraud attacks. Such compromises can often be prevented if the organization's networks are properly segmented, limiting intruders to non-sensitive parts of the network that do not contain payment card information.

Network segmentation is a concept that refers to the practice of splitting a network into functional segments and implementing an access control mechanism between each of the boundaries. The most common example of network segmentation is the separation between the Internet and an internal network using a firewall/router.

Malicious Code Attacks

Malicious codes or malware can be programs such as viruses, worms, Trojan applications, and scripts used by intruders to gain privileged access and capture passwords or other confidential information (e.g., user account information). Malicious code attacks are usually difficult to detect because certain viruses can be designed to modify their own signatures after inflicting a system and before spreading to another. Some malicious codes can also modify audit logs to hide unauthorized activities.

In recent investigations, Visa has identified malicious codes designed to capture payment card data. These are examples of malicious code attacks:

- **Malware that allows interactive command shell or backdoor.** This type of malware allows an intruder to run commands to the compromised system. In some cases, the malware is hard-coded with the intruder's Internet Protocol ("IP") address.

- **Packet sniffers.** Packet sniffing is the practice of using computer software or hardware to intercept and log traffic passing over a computer network. A packet sniffer, also known as a network analyzer or protocol analyzer, captures and interprets a stream or block of data (referred to as a "packet") traveling over a network.

  Packet sniffers are typically used in conjunction with malicious software or malware. Once intruders gain entry into a critical system using backdoor programs or deploying rootkits, the sniffer programs are installed, making the malware more difficult to detect. Intruders can then "sniff" packets between network users and collect sensitive information such as usernames, passwords, payment card data or Social Security numbers. Once a critical system or network is compromised, sniffers are used to eavesdrop or spy on network users and activity. This combination of tools makes this attack scheme effective in compromising systems and networks.

- **Key logger malware.** Key logging is a method of capturing and recording keystrokes. There are key logger applications that are commercially available and are used by organizations to troubleshoot problems within computer systems. Visa Investigations reveal that there are key logger applications that are developed by intruders to capture payment card data and/or users credentials, such as passwords. The key logger captures information in real time and sends it directly to the intruder over the Internet. Additionally, newer advances provide the ability to intermittently capture screenshots from the key logged computer.

  Key logger malware are widely available via the Internet and can be installed on virtually any operating system. Key loggers, like most malware, are distributed as part of a Trojan horse or virus, sent via e-mail (as an attachment or by clicking to an infected web link or site) or, in the worst case, installed by a hacker with direct access to a victim's computer.

Insecure Remote Access

Many Point-of Sale ("POS") vendors, resellers and integrators have introduced remote access management products into the environments of organizations that they support. A variety of remote access solutions exists, ranging from command-line based (e.g., SSH, Telnet) to visually-driven packages (e.g., pcAnywhere, Virtual Network Computing, Remote Desktop). The use of remote management products comes with an inherent level of risk that may create a virtual backdoor on your system. The exploitation of improperly configured and unpatched remote management software tools is the method of attack most frequently used by hackers against POS payment systems. An improperly configured system can be vulnerable in the following ways:

- Failure to regularly update or patch a system can render the system vulnerable to exploits that defeat the security mechanisms built into the product.
- Lack of encryption or weak encryption algorithms can lead to the disclosure of access credentials.
- Use of default passwords can provide easy access to unauthorized individuals.
- Disabled logging mechanisms eliminate insight into system access activity and signs of intrusion.

Insecure Wireless

The adoption of wireless technology is on the rise among participants in the payment industry; particularly merchant retailers, many of whom use wireless technology for inventory systems or check-out efficiency (e.g., “line busting,” ringing up customers while they are in line). Wireless technologies have unique vulnerabilities; organizations must carefully evaluate the need for such technology and understand the risks, as well as the security requirements, before deploying wireless systems.

Following are some of the common methods used to attack wireless networks. These methods are widely documented on the Internet, complete with downloadable software and instructions.

- **Eavesdropping** — An attacker can gain access to a wireless network just by “listening” to traffic. Radio transmissions can be freely and easily intercepted by nearby devices or laptops. The sender or intended receiver has no means of knowing whether the transmission has been intercepted.
- **Rogue Access** — If a wireless Local Area Network (LAN) is part of an enterprise network, a compromise of the LAN may lead to the compromise of the enterprise network. An attacker with a rogue access point can fool a mobile station into authenticating with the rogue access point, thereby gaining access to the mobile station. This is known as a “trust problem,” and the only protection against it is an efficient access-authentication mechanism.
- **Denial of Service (DOS)** — Due to the nature of radio transmission, wireless LANs are vulnerable to denial-of-service attacks and radio interference. Such attacks can be used to disrupt business operations or to gather additional information for use in initiating another type of attack.
- **Man-in-the-Middle (MITM)** — Packet spoofing and impersonation, whereby traffic is intercepted midstream then redirected by an unauthorized individual for malicious purposes, are also valid threats.

For more information on additional attack vectors and mitigation strategies, please visit *www.Visa.com/cisp,* under “Alerts, Bulletins and Webinars.”

Steps and Requirements for Compromised Entities

Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), PCI Payment Application Data Security Standard (PA-DSS), and PCI PIN Security Requirements.

1. Immediately contain and limit the exposure. Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. Compromised entities should consult with their internal incident response team. To preserve evidence and facilitate the investigation:
   - Do not access or alter compromised system(s) (i.e., don't log on at all to the compromised system(s) and change passwords; do not log in as ROOT). Visa highly recommends compromised system not be used to avoid losing critical volatile data.
   - Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (i.e., unplug network cable).
   - Preserve evidence and logs (i.e., original evidence, security events, web, database, firewall, etc.)
   - Document all actions taken.
   - If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised).
   - Be on "high" alert and monitor traffic on all systems with cardholder data.
2. Alert all necessary parties immediately:
   - Your internal incident response team and information security group.
   - If you are a merchant, contact your merchant bank.
   - If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Manager immediately:
     - U.S. – (650) 432-2978 or *usfraudcontrol@Visa.com*
     - Canada – (416) 860-3090 or *CanadaInvestigations@Visa.com*
     - Latin America & Caribbean – (305) 328-1713 or *lacrmac@Visa.com*
     - Asia Pacific – (65) 96307672 or *APInvestigations@Visa.com*
     - CEMEA – +44 (0) 207-225-8600 or *CEMEAFraudControl@Visa.com*

     If you are a financial institution, contact the appropriate Visa region at the number provided above.
3. Notify the appropriate law enforcement agency. Contact the Visa Incident Response Manager above for assistance in contacting local law enforcement agency.

Key Point to Remember

To minimize the impact of a cardholder information security breach, Visa has created an Incident Response Team to assist in forensic investigations. In the event of a compromise, Visa will coordinate a team of forensic specialists to go onsite immediately to help identify security deficiencies and control exposure. The forensic information collected by this team is often used as evidence to prosecute criminals.

4. The compromised entity should consult with its legal department to determine if notification laws are applicable.
5. Provide all compromised Visa, Interlink, and Plus accounts to the Visa acquiring bank or to Visa within ten (10) business days. All potentially compromised accounts must be provided and transmitted as instructed by the Visa acquiring bank and Visa. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. **Note:** If you are an issuer, provide foreign accounts or accounts from other financial institutions to Visa.
6. Within three (3) business days of the reported compromise, provide an Incident Report to the Visa client or to Visa. (See *Appendix C,* on page 25, for the Incident Report template.) If you are a financial institution, provide the Incident Report to Visa.

   Note: If Visa deems necessary, an independent forensic investigation by a Visa-approved Qualified Incident Response Assessor (QIRA) will be initiated on the compromised entity.

Steps and Requirements for Visa Clients (Acquirers and Issuers)

Notification

1. Immediately report to Visa the suspected or confirmed loss or theft of Visa cardholder data. Clients must contact the Visa Risk Management group immediately at the appropriate Visa region.
2. Within 48 hours, advise Visa whether the entity was in compliance with PCI DSS and, if applicable, PCI PA-DSS and PCI PIN Security requirements at the time of the incident. If so, provide appropriate proof.

Preliminary Investigation

3. Perform an initial investigation and provide written documentation to Visa within three (3) business days. The information provided will help Visa understand the potential exposure and assist entities in containing the incident. Documentation must include the steps taken to contain the incident.

For More Information

To find out more about conducting an initial investigation, see *Appendix A: Initial Investigation Request* on page 23.

Independent Forensic Investigation

If Visa deems necessary, an independent forensic investigation must be conducted by a QIRA.

4. Upon receipt of an initial independent forensic investigation notification from Visa, clients must:
   - Identify the QIRA within five (5) business days.
   - Ensure that the QIRA is engaged (or the contract is signed) within ten (10) business days.
   - The QIRA must be onsite to conduct a forensic investigation within five (5) business days from the date the contract agreement is signed.

The Visa client or compromised entity should engage the QIRA directly. However, Visa, has the right to engage a QIRA to perform a forensic investigation as it deems appropriate, and will assess all investigative costs to the client in addition to any fine that may be applicable.

Key Point to Remember

The entity must have the QIRA evaluate whether the entity complies with each of the 32 PCI PIN Security Requirements, available on *www.Visa.com/pinsecurity.*

5. If there is a suspected PIN compromise, the QIRA will perform a PIN security and key management investigation and a PCI PIN security assessment.

6. Provide a preliminary forensic report to Visa within five (5) business days from the onsite review. *The QIRA or the compromised entity can work with the appropriate region in the event that the preliminary report is delayed.*
7. Provide a final forensic report to Visa within ten (10) business days from the completion of the review.

   Note: Visa has the right to review the forensic report and reject the report if it does not meet Visa's requirements.

PIN Security

8. If there is a suspected PIN compromise, provide a PIN security report within ten (10) business days from the onsite review. This report should also review PIN-related cryptographic keys to determine if the keys might have been compromised.

Account Numbers

9. Provide "at risk" account numbers to Visa within ten (10) business days from the date that Visa requests the account numbers.

Containment/Remediation

10. Ensure that the compromised entity has contained the incident and has implemented security recommendations provided by the QIRA, including any non-compliance with the PCI PIN Security Requirements.
11. If the entity is retaining full-track data, CVV2, and/or PIN blocks, ensure that the entity has removed the data (this includes any historical data).
12. Validate that full-track data, CVV2, and/or PIN blocks are no longer being stored on any systems. Even though this is the client's responsibility, Visa requires that the validation be performed by the QIRA.
13. Submit a remediation plan to Visa within five (5) business days after receiving the final forensic report. As required by Visa, clients must provide a remediation plan with implementation dates related to findings identified by the QIRA.

    A revised remediation plan must be provided to Visa, as needed.
14. Monitor and confirm that the compromised entity has implemented the action plan. Confirmation must be done by the QIRA or Qualified Security Assessor (QSA).

PCI DSS Compliance

15. Ensure that the compromised entity achieves full PCI compliance by adhering to the PCI DSS, PCI PA-DSS and, if applicable, the PCI PIN Security Requirements. Compliance validation is required per *Visa International Operating Regulations*.

Key Point to Remember
Please visit *www.pcisecuritystandards.org* for more information on PCI DSS and the PCI PIN Entry Device Testing Program. For more information on PCI PIN Security Requirements, please visit *www.Visa.com/pinsecurity*.

Requirements for Account Data Requests

In the event of a compromise, Visa requires that "at risk" accounts be provided to Visa through Visa's Compromised Account Management System (CAMS).

In some cases, Visa may require the entity to provide accounts via a CD using encryption software such as PGP[2] or Winzip[3] with 256-AES encryption and strong password. The following guidelines must be followed when providing accounts to Visa:

Account Data Format

The account data provided must be **authorization** data only.

File submitted must be a plain-text, comma delimited file containing account numbers and expiration dates. For example:

– The card number, followed by a comma, followed by the expiration date in YYMM format:

4xxxxxxxxxxx1234,0801

Key Point to Remember

Visa may require additional data for further fraud analysis and will inform the compromised entity and the Visa client if additional data is required.

Please refer to *Appendix E* for information on the Advanced Account Data Format and Account Data File Layout.

1. Submitted data should be limited to **one** file. In cases where one file isn't possible, make every effort to minimize total file counts. If multiple files are provided, all of them **MUST** be consistent (i.e., they **MUST** contain the same formatting and transaction details).
2. The following information must be provided in separate files and clearly labeled:
   - Signature and PIN-based transactions (Interlink and Plus)
   - Track and non-track data
   - Data sniffed/captured by the hacker
   - Data stored by the compromised entity
   - Data transferred out of the compromised entity's network

[2] PGP (Pretty Good Privacy) is a computer program that provides cryptographic privacy and authentication. For more information on PGP, go to *www.pgp.com*.
[3] WinZip is a data compression utility with the ability to compress using 256-AES encryption. For more information on WinZip, go to *www.winzip.com*.

Account Data Upload

When providing a file to Visa via Compromised Account Management System (CAMS) or copying to a CD, the user must provide a description of the data being uploaded or copied. For example:

1. Transaction date(s) of “at risk” accounts
2. Data elements at risk:
   - Primary Account Number (PAN)
   - Expiration date
   - Track 1 or 2
   - CVV2
   - PIN blocks
   - Other cardholder information, such as billing address, e-mail addresses, SSN, DOB, etc.
3. Name of compromised entity
4. Name of Visa investigator handling the incident

Key Point to Remember
Visa accounts copied to a CD or other removable media must be encrypted using PGP or Winzip with 256-AES encryption with strong password.

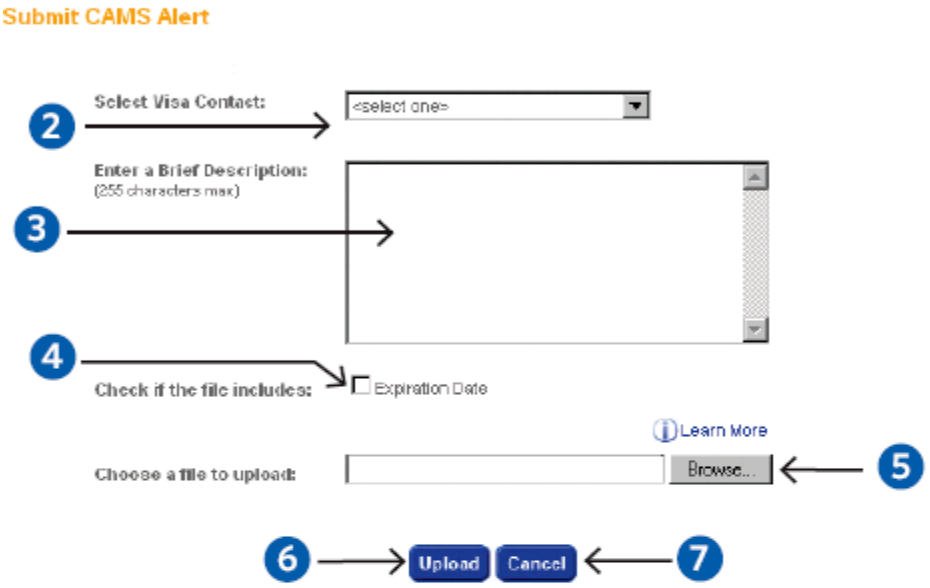
Compromised Account Management System (CAMS)

The Compromised Account Management System (CAMS) offers a secure and efficient way for acquirers, merchants, law enforcement agencies, and financial institutions to transmit compromised and recovered account data to and from Visa through an encrypted site. Using CAMS, acquirers, merchants, and law enforcement officers can upload potentially compromised and recovered accounts directly to Visa.

Subscribing financial institutions can access CAMS by logging on to *www.us.Visaonline.com* and receive compromise alerts via e-mail regarding their accounts.

To Upload File(s):

1. Access the "Submit CAMS Alert" screen to upload your file data. At this screen, you must enter a description, indicate whether you are providing an expiration date, and select a file to upload from your hard drive.



2. From the drop down menu, select your assigned Visa contact. **This field is required.**
3. Enter a brief description of the files you are uploading for the compromise.
4. If applicable, indicate whether the file includes an expiration date. (Indicating an account expiration date will help the issuer identify which accounts are good candidates for monitoring.)
5. Click "Browse" to select a file from your local hard drive.
   - Files must be either plain text or a .zip file containing plain text files.
   - Files cannot exceed 100 MB in size.
   - The uploaded file should contain 11-19 digit account numbers.
6. Click the "Upload" button to begin the file transfer process. *The progress box will display how much of the upload has been completed.*

7. To stop the file transfer, click the "**Cancel**" button at any time.

To Upload Additional File(s):

After a successful upload, the "Submit CAMS Alert" screen will reappear with a message that confirms that your upload has been completed successfully. You will also be asked if you would like to add another file to the same alert. If you add another file, please remember that you will only be allowed to submit one description for each alert; the first description that you submit will apply.

If an error occurs during the upload, an error message will appear and you will be asked to upload the file again. You should also receive an e-mail message describing the upload error.

In response, you can either resubmit the file or contact the CAMS Administrator at *VisaRiskManager@Visa.com* or 1-800-439-9013 for assistance.

Appendix A: Initial Investigation Request

Upon notification of a suspected account data compromise, Visa will request that the Visa client initiate a preliminary investigation of any entity involved in a potential track data, CVV2, and/or PIN compromise. The initial investigation will assist Visa in understanding the compromised entity's network environment.

To comply with Visa's initial investigation request, the Visa client must provide the following information:

Key Point to Remember
The information required below is applicable to suspected/confirmed compromised entities such as Visa clients, merchants, processors, or third-party service providers.

Entity Information

Description	Response
Name of entity	
Is entity a direct-connect to Visa?	
If entity is a merchant, provide the Merchant Category Code (MCC)	
Acquirer BIN	
Entity PCI DSS Level (e.g., Level 1-4)	
Entity PCI DSS Compliance Status (If compliant, please provide proof of PCI DSS compliance documentation.)	
If merchant, date entity began processing with acquirer	
If merchant, date entity stopped processing with acquirer (if applicable)	
Approximate number of transactions/accounts handled per year	
1) ATM	
2) POS PIN/Debit	
3) Credit	
If merchant, is entity corporate-owned or an individual franchise?	
If merchant, does entity have other locations? If so, please provide a list of locations, the name of the payment application, and version information.	

Network/Host Information

Description	Response
Is there Internet connectivity?	
Is there wireless connectivity?	
Does entity utilize a high-speed connection (e.g., cable modem, DSL)	
Is there remote access connectivity? If so, who has remote access?	
Is remote access always on or is it enabled upon request?	
What type of remote access software is used?	
Is the terminal PC-based or is it connected to a PC-based environment?	
Has entity noticed any abnormal activity on its systems?	
Is the entity retaining full track data, CVV2 or encrypted PIN blocks?	
How long is the data stored on the system(s)?	
Have there been any recent changes to the network and host such as: • Upgrade to the payment application • Installation of a firewall • Installation of anti-virus program Changes to remote access connectivity	
Provide a transaction flow for credit and debit, as well as remote access to the network. The data flow must include: • Cardholder data sent to a central corporate server or data center • Upstream connection to third-party service providers • Connection to entity bank/acquirer Remote access connection by third-party service providers or internal staff	

Third-Party Connectivity

Description	Response
Does the entity send transactions to a processor(s)? If so, who is the processor(s)?	
Name of payment application vendor	
Name of reseller, if applicable	
Is the entity hosted? If so, who is the hosting provider?	

List of Payment Applications and PIN Entry Device (PED) in Use

Description	Response
Payment application and version information	
Is this a corporate-mandated payment application and version?	
PIN Entry Device (PED) information, if applicable. Include the name of the PED firmware version. Visit *www.pcisecuritystandards.org/pin* for a list of PCI-approved PIN entry devices.	
Shopping cart and version information	
Are the payment applications in use PCI PA-DSS compliant? Visit *www.Visa.com/PABP* for a list of PA-DSS compliant payment applications.	
Is entity using a compliant PED? Visit *www.pcisecuritystandards.org/pin* for a list of compliant PEDs.	

Potential Skimming/PED Tampering

Description	Response
Can entity trace legitimate transactions to a single employee, device, or lane(s)?	
Did entity have any employees who were employed for a short period of time?	
Did other employees notice suspicious behavior of the new employee (e.g., eager to handle all credit card transactions)?	
Is there any video surveillance and has it been reviewed?	
Can all PEDs be accounted for at all times?	
Are any of the POS PEDs in use listed on the November 2007 Security Alert available at *www.Visa.com/cisp*?	

Other Information

Description	Response
Has entity received complaints regarding fraudulent transactions from their customers?	
Has entity been contacted by law enforcement regarding fraudulent transactions?	
Can law enforcement provide intelligence that skimming groups are active in the area?	

Appendix B: Forensic Investigation Guideline

A Visa client or compromised entity must ensure that only a Visa-approved Qualified Incident Response Assessor (QIRA) is engaged to perform a forensic investigation. It is the compromised entity's responsibility to pay for the cost of the forensic investigation. Visa has the right to engage a QIRA to perform a forensic investigation as it deems appropriate, and will assess all investigative costs to the Visa Member in addition to any fine that may be applicable.

All QIRAs are required to adhere to the following forensic investigation guidelines. Visa clients can also use these guidelines to monitor the work by the QIRA. Visa will **NOT** accept forensic reports from non-approved forensic companies. QIRAs are required to release forensic reports and findings to Visa.

Note: For a list of Visa Inc. QIRAs, go to *www.visa.com/cisp*, under If Compromised section. The .PDF file is labeled "Qualified Incident Response Assessor List."

All QIRAs must utilize Visa's reporting template (see Appendices C and D for more information).

Note: Visa has the right to review the QIRA forensic report and reject the report if it does not meet Visa's requirements. QIRAs are required to resolve with Visa and compromised entity any discrepancies with the report.

Forensic investigations must be conducted using the following scope and methodology:

1. QIRA will assess compromised entity's computing environment to determine the scope of the forensic investigation and relevant sources of electronic evidence. This includes, but is not limited to:
   - Assessment of all external and internal connectivity points within each location involved.
   - Assessment of network access controls between compromised system(s) and adjacent and surrounding networks.

Key Point to Remember
Visa reserves the right to engage the QIRA.

2. QIRA will acquire electronic evidence from the compromised entity's host and network-based systems.
   - Forensic evidence acquisition must be conducted onsite at the compromised entity's premises.
   - Both live and memory acquisitions must be performed.
   - If circumstances do not permit onsite evidence acquisition, QIRA must notify Visa.
   - Preservation of all potential electronic evidence on a platform suitable for review and analysis by a court of law, if applicable.
3. Forensically examine electronic evidence to find cardholder data and establish an understanding of how a compromise may have occurred.
4. Verify that cardholder data is no longer at risk and/or has been removed from the environment.
5. Verify that the compromised entity has contained the incident.

6. QIRA must use Visa's Incident Report template and provide a forensic report to all parties involved in the incident.
7. Perform external and internal vulnerability scans, including network and application scans.
8. The following actions must be included as part of the forensic investigation:
   - Determine and describe the type of processing environment:
     - Organization Description (check all that apply):
     - VisaNet processor
     - Issuer only
     - Acquirer only
     - Both issuer and acquirer
     - Pre-paid issuer
     - Third-party processor
     - Merchant
     - Other: _____
   - Estimated annual number of credit and or debit transactions for Visa-branded products (based on interview; exact numbers are not required):
     - Visa credit
     - Visa debit (Visa Signature only)
     - Visa with PIN (ATM with PIN)
     - Interlink (POS with PIN)
     - Plus (ATM with PIN)
     - Visa Prepaid (include list of Prepaid products)
     - Other: _____
9. Check and determine cardholder information that is at risk. This includes:
   - Number of and types of Visa/Plus/Interlink/Prepaid accounts at risk. Identity those stored and captured by malware (e.g., packet sniffer, key logger).
   - List of associated account information at risk:
     - Full magnetic-stripe data (e.g., Track 1 and 2)
     - PIN blocks and clear-text PINs. To identify potential presence of PIN blocks, also look for the PIN block format code field (see *Account Data Layout Format, Appendix E,* for more information).
     - CVV2
     - Account number
     - Expiration date
     - Other sensitive data elements (e.g., SSN, DOB)
     - Cardholder name
     - Cardholder address
     - Cardholder e-mail address

- QIRA to examine all potential locations, including payment applications, to determine if full magnetic-stripe data, CVV2, and/or PIN blocks are stored (whether encrypted or unencrypted) on production, backups, tables, development, test, software engineer, and administrator's machines.
- QIRA should also check volatile memory for cardholder data.
- If malware was used to capture cardholder data, QIRA must review any malware output logs and validate whether cardholder data was captured and stored.
- Other logs that must be reviewed include the following:
  - Server
  - Application
  - Transaction
  - Troubleshooting
  - Debug
  - Exception or error files
- QIRA must provide account information to Visa (see *Requirements for Account Data Requests*, page 18).

10. Determine time frame of accounts at risk. For example:
    - Determine how long accounts were stored on the system(s).
    - Determine the transaction date(s) of accounts stored on the system(s).
11. Perform incident validation and assessment. This includes:
    - Establishing how a compromise occurred.
    - Identifying the source of the compromise.
    - Window of system vulnerability. This is defined as the frame of time in which a weakness(s) in an operating system, application or network could be exploited by a threat to the time that weakness(s) is properly remediated.
    - Determining if any cryptographic keys have been exposed or compromised.
    - Reviewing the entire debit and/or credit processing environment to identify all compromised or affected systems; considering the e-commerce, corporate, test, development, production systems, VPN, modem, DSL, cable modem connections, and any third-party connections, **regardless of whether or not the compromised systems stores, processes, or transmits cardholder data.**
    - If applicable, review VisaNet endpoint security and determine risk.
    - Identifying the date(s) that account data was transferred out of the network by the intruder or malware.
    - Date(s) when the entity began using the payment application and version number. Determine if the payment application is PA-DSS compliant.
      - If available, identify the date(s) when the entity installed a patch or an upgrade to no longer retain prohibited data.
    - The date(s) that malware was installed on the system, if applicable.
    - Date(s) when malicious code, such as packet sniffer and/or key logger, was activated to capture payment card data on the network and system. QIRA must include date(s) of when malware was de-activated.

- Determine the window of intrusion. This is the first confirmed date that the intruder or malware entered the system to the date of containment

12. Determine what applicable PCI security requirements apply:
    - PCI DSS
    - PCI PIN Security Requirements
    - PCI POS PIN Entry Device Security Requirements
    - PCI Encrypting PIN PAD (EPP) Security Requirements
    - PCI PA-DSS
13. Determine which PCI DSS requirements and sub-requirements contributed to the breach of cardholder data.
14. If malware and bad IPs are identified in the compromise, the QIRA must submit the malware code and bad IPs via a secure distribution to *uscyberforensics@Visa.com.*

Table of Entities and Requirements Applicability

Description	Response
Payment application and version information	
Is this a corporate-mandated payment application and version?	
PIN Entry Device (PED) information, if applicable. Include the name of the PED firmware version. Visit *www.pcisecuritystandards.org/pin* for a list of PCI-approved PIN entry devices.	
Shopping cart and version information	
Are the payment applications in use PCI PA-DSS compliant? Visit *www.Visa.com/PABP* for a list of PA-DSS compliant payment applications.	
Is entity using a compliant PED? Visit *www.pcisecuritystandards.org/pin* for a list of compliant PEDs.	

Table of Entities and Requirements Applicability

Requirements	Types of Entities						
	Issuer Processor	**Acquirer Processor**	**Credit Only Merchant**	**Debit Accepting Merchant**	**Issuer and Acquirer Processor**	**ATM Processor**	**Third-Party Servicer**
PCI DSS	Applies	Applies	Applies	Applies	Applies	Applies	Applies
PCI PIN Security Requirements	Applies if driving their own ATMs	Applies if processing debit	N/A	Applies	Applies	Applies	Applies if processing debit
PCI POS and PCI EPP PIN Entry Device Security Requirements	N/A	Applies if processing debit	N/A	Applies	Applies	Applies	Applies if processing debit
PCI PA-DSS	Applies	Applies	Applies	Applies	Applies	Applies	Applies

15. QIRAs must utilize Visa's report template. See *Appendices C and D, Incident Report template* for more information.

Appendix C: Preliminary Incident Report Template

This section contains the content and format standards that must be followed when completing a Preliminary Incident Response Report.

The Preliminary Incident Response Report document can be completed by the compromised entity or by an approved QIRA. Once completed, the report must be distributed to Visa, the client, and the compromised entity. Visa will classify the report as Visa Confidential.

Questions	Responses
Name of compromised entity	
Date arrived onsite	
Evidence of a breach (Y/N)	
First confirmed date that the intruder or malware entered the network	
Scope of forensic investigation (e.g., single vs. numerous locations)	
Type of data impacted (e.g., full track, CVV2, PIN blocks)	
Window of system vulnerability	
Initial thoughts on attack vector	
Is the security breach ongoing or has it been contained?	
Other comments	

Appendix D: Final Incident Report Template

I. Executive Summary (include the following information):

- Date when the forensic company was engaged
- Date(s) when forensic investigation began
- Location(s) visited or forensically reviewed
- A brief summary of the scope of the forensic investigation
- A brief summary of the environment reviewed (details must be documented under the “Findings” section)
- Cause of intrusion
- Date(s) of intrusion (if inconclusive or no evidence of a breach, list security deficiencies that would allow the breach
- Data elements at risk (e.g., full track, CVV2, PIN blocks)
- Specify whether or not the security breach has been contained

II. Background

- Brief summary of compromised entity company:
- Type of business entity:
  - Merchant (brick and mortar, e-commerce or both)
  - Prepaid issuer
  - Issuer
  - Acquirer
  - Acquirer processor
  - Issuer processor
  - ATM processor
  - Third-party service provider (web hosting; co-location)
  - Encryption Support Organization (ESO)
  - Payment application vendor
  - Payment application reseller
- PCI compliance and other information:
  - PCI DSS level and compliance status
  - Number of locations
  - Parent company (if applicable)
  - Franchise or corporate-owned

III. Incident Dashboard

Client	Type of Business Entity
Date when entity identified compromise	
Method of identification	Self Detection or Common Point of Purchase
Window of system vulnerability	
Window of intrusion	
Malware installation date(s), if applicable	
Date(s) of real time capture, if applicable	
Date(s) that data was transferred out of the network, if applicable	
Window of payment card data storage	
Transaction date(s) of stored accounts	
Type of data exposed	• Cardholder name • Cardholder address • PAN • Expire date • CVV2 • Track data • Encrypted PINs
Brand exposure	• Visa • MC • DISC • AMEX • JCB
Number of cards exposed (both live system space and unallocated space)	• Include breakdown by card brand type • Include breakdown of the following: – Signature – PIN-based transactions – Issuer-only data – Non-issuer data – Prepaid data

Client	Type of Business Entity
Logs that provided evidence: • Firewall logs • Intrusion detection systems • Database queries • FTP server logs • System login records • Web server logs	• File integrity monitoring output • Transaction logs • Remote access logs • Wireless connection logs • Anti-virus logs • Security event logs • File creation/access date
Payment Application Information:	• Name, version, and install date of payment application used at the time of the security breach • Name, version, and install date of current payment application • Payment application vendor • Reseller/IT support that manages payment application/network
Suspected cause summary	Insert brief case summary. Detailed findings should be included in the “Findings” section of the report.

If applicable, document the type of cryptographic keys at risk. (See “*PIN Security Requirements*”, page 44 of this section.)

Issuer Side Cryptographic Keys	Acquirer Side Cryptographic Keys
Issuer Working Keys (IWK)	Acquirer Working Keys (AWK)
PIN Verification Keys (PVK)	POS, ATM, EPP PIN Encryption Keys
CVV, DCVV, ICVV Verification Keys CVV2 Verification Keys (CVK2) Cardholder Authentication Verification Value Keys (CAVV and CAK) Cardholder Authentication Attempts Value Keys (CAAV)	POS, ATM, EPP Key Encrypting Keys (KEKs)
PIN Generation Keys	Remote Initialization Keys
Master Derivation Keys (MDK)	Host to Host Working Keys Key Encrypting Keys (KEKs)
Host to Host Working Keys Key Encrypting Keys (KEKs)	Switch Working Keys
Switch Working Keys	

IV. Network Infrastructure Overview

- Provide a diagram of the network that includes the following:
  - Cardholder data sent to central corporate server or data center
  - Upstream connections to third-party processors
  - Connections to Visa or Visa client bank networks
  - Remote access connections by third-party vendors or internal staff
  - Inbound/outbound network connectivity
  - Network security controls and components (network security zones, firewalls, hardware security modules, etc.)
  - Clearly identify all infrastructure components implemented or modified after the time frame of the compromise

V. Findings

- Provide specifics on firewall, infrastructure, host, and personnel findings
- Identify network and host security configurations at the time of the breach
- Identify any and all changes made to the compromised entity's computing environment after the identification of a compromise
- Provide specific dates of network, system, or payment application changes
- Include any and all forensic evidence supporting changes made to networks, systems, and POS components
- Identify any data accessed by unauthorized user(s)

- Identify any data transferred out of the network by unauthorized user(s)
- Identify any evidence of data deletion from systems involved in a compromise
- If applicable, identify any deleted data recovered through forensic file recovery methods
- Identify any third-party payment applications, including version number
- Identify any upgrades/patches to the payment application that address removal of magnetic-stripe data, CVV2, and/or encrypted PIN blocks
- Provide an attack timeline of events. Include relevant date(s) and activities (e.g., date/time created, system/file evidence, description of evidence)
- Include a list of compromised systems/hosts (e.g., operating system; application and its functionality)
- Include a list of malicious IPs. Include any information related to malicious IPs (e.g., part of hacker group)
- Include a list of all malware identified. Include the following information on malware:
  - Name of malware
  - MD5 Hash
  - Registry settings
  - File size
  - System path

VI. Compromised Entity Containment Plan

- Document what the entity has done to contain the incident. Include date(s) of containment.

VII. Recommendation (s)

- List recommendations by priority level

VIII. PCI DSS Compliance Status

- Based on findings identified in the forensic investigation, indicate the compliance status for each of the 12 basic requirements under the PCI DSS
- Document the specific PCI DSS requirements and sub-requirements that contributed to the security breach and include the forensic findings/evidence.

PCI DSS				
Requirements	**In Place**	**Not in Place**	**Cause of breach (y/n)**	**Include Forensic Findings**
Build and Maintain a Secure Network				
Requirement 1: Install and maintain a firewall configuration to protect cardholder data				
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters				
Protect Cardholder Data				
Requirement 3: Protect stored cardholder data				
Requirement 4: Encrypt transmission of cardholder data across open, public networks				
Maintain a Vulnerability Management Program				
Requirement 5: Use and regularly update anti-virus software				
Requirement 6: Develop and maintain secure systems and applications				
Implement Strong Access Control Measures				
Requirement 7: Restrict access to cardholder data by business need-to-know				
Requirement 8: Assign a unique ID to each person with computer access				
Requirement 9: Restrict physical access to cardholder data				

PCI DSS				
Requirements	**In Place**	**Not in Place**	**Cause of breach (y/n)**	**Include Forensic Findings**
Regularly Monitor and Test Networks				
Requirement 10: Track and monitor all access to network resources and cardholder data				
Requirement 11: Regularly test security systems and processes				
Maintain an Information Security Policy				
Requirement 12: Maintain a policy that addresses information security				

Appendix E: Account Data Layout Format

As mentioned in the previous section, clients are required to follow the following format on all account data requests. The account data must be **AUTHORIZATION DATA ONLY.**

Submitted data should be limited to one file. In cases where one file isn't possible, make every effort to minimize total file counts. If multiple files are provided, all of them must be consistent and contain the same formatting and transaction details.

The data submission may be a fixed width or delimited text file. Acceptable field delimiters are comma, tab, semicolon, space, or pipe (with or without text qualifiers). Field headers must be in the file or included on a separate file layout document.

Acceptable formats for each field (alpha (A), numeric (N), alphanumeric (AN), or alphanumeric special character (ANS)) are included in the descriptions. The International Standards Organization (ISO) field is noted if there is a corresponding field for further information.

The following are acceptable examples of file layouts and account data formats.

Advanced Format

In some cases, Visa will require additional transaction detail for further analysis. Provide information in as many fields as possible.

- Credit accounts signature (to include transaction details, see following bulleted list)
- Debit accounts signature (to include transaction details, see following bulleted list)
- Debit accounts used with a PIN (to include transaction details, see following bulleted list)
- Key-entered accounts (to include transaction details, see following bulleted list)

Transaction details are defined as follows:

- Primary account number (PAN)
- Expiration date
- Transaction amount
- Transaction date
- Merchant Category Code (MCC)
- Point-of-Service Entry Mode Code (POS entry)
- Visa Acquiring Bank Identification Number (BIN)
- Visa Acquiring Processor Control Record (PCR)
- Card Acceptor Identification Code (CAID)
- Card Acceptor Terminal Identification
- PIN transaction indicator

- Card acceptor name/location
- Card acceptor city
- Card acceptor country

Descriptions

Primary Account Number (PAN)

Format: N

ISO Field 2

The PAN contains the number identifying the cardholder account or relationship. The value is a cardholder account number of up to 19 numeric digits embossed on the card and also encoded on Track 1 and Track 2 of the magnetic stripe. The PAN is present in both face-to-face and card not present (CNP) transactions.

Allowable Card Account Number Lengths

Visa Card 16 digits.

16-digit example: 4444333322221111

Expiration Date

Format: N

ISO Field 7 (Track 1)

ISO Field 4 (Track 2)

Transaction Amount

Format: N

Cardholder transaction amount is in either U.S. dollars or per the currency code in Field 49. If the amount is not in U.S. dollars, then the currency code should also be present in a separate field.

Examples:

$45.30

45.30

45.30, 250 (ISO currency code)

Transaction Date

Format: AN

Field contains the date of cardholder transaction. Acceptable formats should include the month, day, and year of transaction. Julian date is allowable.

Examples:

MM/DD/YYYY (03/15/2006)

DD/MM/YYYY (15/03/2006)

MM/DD/YY (03/15/06)

DD-MMM-YY (15-MAR-06)

March 15, 2006

YYDDD (06074) – Julian date

Merchant Category Code (MCC)

Format: N

ISO Field 18

Field contains a code describing the merchant's type of business product or service (also known as the Merchant Category Code (MCC)). Valid codes are listed in the *Visa International Operating Regulations.*

Examples:

5192 – Books, Periodicals, and Newspapers

5542 – Automated Fuel Dispensers

6011 – Financial Institutions – Automated Cash Disbursements

7230 – Hair Salon

Point-of-Service Entry Mode Code (POS entry)

Format: N

ISO Field 22: Positions 1 and 2 required

Field contains codes that identify the actual method used to capture the account number and expiration date and, when a point-of-transaction terminal is used, its PIN capture capability. This field is fixed-length with three sub-fields. The position assignments are as follows:

Positions 1 and 2

PAN and Date Entry Mode: A two-digit code that identifies the actual method used to enter the cardholder account number and card expiration date. This code specifies whether the entire magnetic stripe is included in an authorization or financial request.

Position 3

PIN Entry Capability – A one-digit code that identifies the capability of a terminal to accept PINs; it does not necessarily mean that the PIN was entered or is included in the message. A value of "1" means that the terminal can accept PINs; a value of "2" indicates that the terminal can not accept PINs.

Examples:

90 – Magnetic-stripe read and exact contents of Track 1 or Track 2 included. CVV or dCVV check is possible.

02 – Magnetic-stripe read; CVV checking may not be possible.

01 – Manual key entry

Visa Acquiring Bank Identification Number (BIN)

Format: N

This field identifies the financial institution acting as the acquirer of this customer transaction. The acquirer is the client or system user that signed the merchant, installed the ATM or ADM, or dispensed cash.

Visa BINs are six (6) digits. For processing centers handling multiple acquirers, this code identifies the individual acquirer or system user, not the overall processing center.

Examples:

400850

458307

Visa Acquiring Processor Control Record ("PCR")

Format: N

This field, consisting of four (4) digits, identifies the processing center acting as the agent of the acquiring client that provides authorization, clearing, or settlement services for the merchant.

Examples:

4321 – ABC Processing Services

5678 – ABC Merchant

Card Acceptor Identification Code (CAID)

Format: ANS

ISO Field 42

This field contains the identifier of the card acceptor operating the point-of-sale or point-of-service (POS) terminal (or at the ATM) in local and in interchange environments. The CAID can be up to 15 bytes; if the ID is less than 15 positions, it must be left-justified and space-filled.

Examples:

140000015613401

58678062890003

6922I858RP357H

3655139M

Card Acceptor Terminal Identification

Format: ANS

ISO Field 41

This field contains a code that identifies the card acceptor terminal or ATM. For electronic POS terminals, when the ID is not unique to a specific terminal, Field 42 (CAID) can be used along with this field. ATM terminal IDs must be unique within the acquirer's network.

An identification code of fewer than eight (8) bytes must be left-justified and the remainder of the field space filled.

Examples:

80046578

8RNL9055

073

RI895B

PIN Transaction Indicator

Format: AN

This field indicates whether or not the transaction was PIN-based. This is the field that is used to differentiate signature-based versus PIN-based transactions.

Examples:

PIN, No PIN

Yes, No

Numeric codes: 1=PIN, 2=No PIN

Personal Identification Number (PIN) Data

ISO Field 52

Attributes: Fixed Length 8 bytes; 64-bit string/16 hex

Hex values include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Description: Field 52 contains an encrypted PIN block, formatted as a block of 16 hexadecimal digits. (0 – 9, A – F)

Examples:

2B9FFC29A40A25F3

9A40A252B9FFCBB1

40A2529A4077440A

BA669A40A2527229

2529A40A90ACD199

C510AE889FA92B7F

Security-Relate Control Information

ISO Field 53

Attributes: Fixed Length 8 bytes; 16 numeric 4-bit BCD

Positions 5 - 6 PIN Block Format Code

The code in Field 53.3 (“PIN Block Format Code”) defines the format of Field 52 (“The PIN Block”). This field describes the PIN block format used by the acquirer/merchant and indicates the presence of a PIN. Values for Positions 5 – 6 are “01”, “02”, “03” and “04” and indicate the format of the PIN block used.

Note: Visa PIN block format numbering is different than that of ISO 9564, which is used in the PIN Security Requirements.

Card Acceptor Name/Location

Format: ANS

ISO Field 43

This field contains the name and location of the card acceptor (such as merchant or ATM) and includes the city name and country code. Field 43 has a single fixed length format, but the content of positions 1-25 depends on whether the request is for a Visa Interlink POS transaction, a Visa or Visa Plus ATM, or a VisaPhone transaction.

For Visa Interlink POS/ATM and Visa Plus ATM transactions, when the point of service is not in the same country as the acquirer, Field 43 must identify the card acceptor country. Field 43 also identifies the merchant or ATM location.

Positions 1-25, Card Acceptor Name:

POS: Merchants name as known to the cardholder.

ATM: The ATM location, branch number, or street address only (**Note**: the institution name is in Field 42).

Examples:

Bob’s Fish Shack

AM RED CROSS DONATION

WWW MOULIN COM

Bookstore 53

Position 26-38, City Name:

POS: City where the customer transaction occurs.

Custom Payment Service (CPS) Card Not Present: Instead of the city name, these positions must contain the merchant's customer service telephone number, including country and area codes.

ATM: City where the ATM is located, branch number or street address only (**Note**: the institution name is in Field 42).

Examples:

Savannah

888 777 8888

PARIS

Madrid

Positions 39-40, Country Code:

POS and ATM: The two-character alpha code in uppercase format for the country where the cardholder transaction occurs or the ATM is located.

Examples:

US

FR

ES

PE

The following are samples of File Layouts:

Sample 1

File Layout

Primary Account Number|Transaction Amount|Transaction Date|Merchant Category Code|POS entry|Acquirer BIN|Acquirer PCR|Card Acceptor ID|Card Acceptor Terminal ID|PIN Indicator|Card Acceptor Name|Card Acceptor City|Card Acceptor Country

File

411111111111111|87.5|06057|4816|01|426696|4008|426696100008681|1954|N|GO MAN COM|BALTIMORE|US

4321432143214321|570.28|06068|5912|01|400088|9088|1420005995|05995TS0|N|WALRUS|MT WHISKEY|US

4222222222222222|50|06066|7399|02|469216|2840|924944000192138||N|J2 COMMUNICATE|323 850 3214|US

4141414141414141|11.89|06057|4816|01|400088|9088|106171000991232||N|YABO VOICE|0821230270|EU

4564564564564568|174.5|06063|5399|01|400088|9088|000324202994996|00110825|N|SOYLENT VENTURES|SUNNYTOWN|US

4987654321987654|1|06066|4814|01|461043|4401|67211400015P003|Q3B50F0Q|N|UNICYCLE INTERNET|866 844 1849|US

4846512378945678|60.16|06056|4900|90|461043|8402|67354430019P003|Q3AAF40Q|Y|AQUILA INC|800 378 3357|US

4123456789123456|5.33|06058|7311|01|400088|9088|22628782|24680137|N|GOGGLE CC GOGGLE|OG ADWORDS|GB

Sample 2 for PIN Debit

File Layout (Debit Accepting Merchant)

Primary Account Number|Transaction Amount|Transaction Date|Merchant Category Code|POS entry|Acquirer BIN|Acquirer PCR|Card Acceptor ID|Card Acceptor Terminal ID|PIN Entry Capability|Card Acceptor Name|Card Acceptor City|Card Acceptor Country | PIN Block Format Code | PIN block

File

4111111111111111|87.5|06057|4816|01|426696|4008|426696100008681|1954|1|GO MAN COM|BALTIMORE|US|01| 2B9FFC29A40A25F3

4321432143214321|570.28|06068|5912|01|400088|9088|1420005995|05995TS0|1|WALRUS|MT WHISKEY|US|01| 9A40A252B9FFCBB1

4222222222222222|50|06066|7399|02|469216|2840|924944000192138||1|J2 COMMUNICATE|323 850 3214|US |01|40A2529A4077440A

4141414141414141|11.89|06057|4816|01|400088|9088|106171000991232||1|YABO VOICE|0821230270|EU|01| BA669A40A2527229

4564564564564568|174.5|06063|5399|01|400088|9088|000324202994996|00110825|1|SOYLENT VENTURES|SUNNYTOWN|US |01|2529A40A90ACD199

4987654321987654|1|06066|4814|01|461043|4401|67211400015P003|Q3B50F0Q|1|UNICYCLE INTERNET|866 844 1849|US |01|C510AE889FA92B7F

4846512378945678|60.16|06056|4900|90|461043|8402|67354430019P003|Q3AAF40Q|1|AQUILA INC|800 378 3357|US |01|8A2527229C510AE8

4123456789123456|5.33|06058|7311|01|400088|9088|22628782|24680137|1|GOGGLE CC GOGGLE|OG ADWORDS|GB |01|9FA92B7FA2527229

Sample 3

File Layout

“PAN”;”Transaction Amount”;”Transaction Date”;”MCC”;”POS entry”;”Acq BIN”;”Acq PCR”;”CAID”;”CA Terminal ID”;”PIN Indicator”;”CA Name”;”CA City”;”CA Country”

File

“4111111111111111”;”87.5”;”06057”;”4816”;”01”;”426696”;”4008”;”426696100008681”;”1954”;”N”;”GO MAN COM”;”BALTIMORE”;”US”

“4321432143214321”;”570.28”;”06068”;”5912”;”01”;”400088”;”9088”;”1420005995”;”05995TS0”;”N”;”WALRUS”;”MT WHISKEY”;”US”

“4222222222222222”;”50”;”06066”;”7399”;”02”;”469216”;”2840”;”924944000192138”;;”N”;”J2 COMMUNICATE”;”323 850 3214”;”US”

“4141414141414141”;”11.89”;”06057”;”4816”;”01”;”400088”;”9088”;”106171000991232”;;”N”;”YABO VOICE”;”0821230270”;”EU”

“4564564564564568”;”174.5”;”06063”;”5399”;”01”;”400088”;”9088”;”000324202994996”;”00110825”;”N”;”SOYLENT VENTURES”;”SUNNYTOWN”;”US”

“4987654321987654”;”1”;”06066”;”4814”;”01”;”461043”;”4401”;”67211400015P003”;”Q3B50F0Q”;”N”;”UNICYCLE INTERNET”;”866 844 1849”;”US”

“4846512378945678”;”60.16”;”06056”;”4900”;”90”;”461043”;”8402”;”67354430019P003”;”Q3AAF40Q”;”Y”;”AQUILA INC”;”800 378 3357”;”US”

“4123456789123456”;”5.33”;”06058”;”7311”;”01”;”400088”;”9088”;”22628782”;”24680137”;”N”;”GOGGLE CC GOGGLE”;”OG ADWORDS”;”GB”

Sample 4

File Layout

Primary Account Number,Amount,Date,Merchant Category Code,POS entry,Acquirer BIN,Acquirer PCR,Card Acceptor ID,Card Acceptor Terminal ID,PIN Transaction ID,Card Acceptor Name,Card Acceptor City,Card Acceptor Country

File

4111111111111111,87.5,06057,4816,01,426696,4008,426696100008681,1954,N,GO MAN COM,BALTIMORE,US

4321432143214321,570.28,06068,5912,01,400088,9088,1420005995,05995TS0,N,WALRUS,MT WHISKEY,US

4222222222222222,50,06066,7399,02,469216,2840,924944000192138,,N,J2 COMMUNICATE,323 850 3214,US

4141414141414141,11.89,06057,4816,01,400088,9088,106171000991232,,N,YABO VOICE,0821230270,EU

4564564564564568,174.5,06063,5399,01,400088,9088,000324202994996,00110825,N,SOYLENT VENTURES,SUNNYTOWN,US

4987654321987654,1,06066,4814,01,461043,4401,67211400015P003,Q3B50F0Q,N,UNICYCLE INTERNET,866 844 1849,US

4846512378945678,60.16,06056,4900,90,461043,8402,67354430019P003,Q3AAF40Q,Y,AQUILA INC,800 378 3357,US

4123456789123456,5.33,06058,7311,01,400088,9088,22628782,24680137,N,GOGGLE CC GOGGLE,OG ADWORDS,GB

Sample 5

File Layout

Field Name, Field Length

Primary Account Number, 19

Transaction Amount, 25

Transaction Date, 25

Merchant Category Code, 4

POS Entry Mode, 2

Acquirer BIN, 6

Acquirer PCR, 4

Card Acceptor ID, 15

Card Acceptor Terminal ID, 8

PIN Transaction ID, 1

Card Acceptor Name, 25

Card Acceptor City, 15

Card Acceptor Country, 2

File

4111111111111111 87.5 06057 481601426696400842669610000868119 54 NGO MAN COM BALTIMORE US

4321432143214321 570.28 06068 591201400088908814200059 95 05995TS0NWALRUS MT WHISKEY US

4222222222222222 50 06066 739902469216284092494400019 2138 NJ2 COMMUNICATE 323 850 3214 US

4141414141414141 11.89 06057 481601400088908810617100099 1232 NYABO VOICE 0821230270 EU

4564564564564568 174.5 06063 539901400088908800032420299499600110825NSOYLENT VENTURES SUNNYTOWN US

4987654321987654 1 06066 481401461043440167211400015P003Q3B50F0QNUNICYCLE INTERNET 866 844 1849 US

4846512378945678 60.16 06056 490090461043840267354430019P003Q3AAF40QYAQUILA INC 800 378 3357 US

4123456789123456 5.33 06058 731101400088908822628782 24680137NGOGGLE CC GOGGLE OG ADWOR

Appendix F: PIN Security Requirements

PCI PIN Security Requirements

Objective 1

PINs used in transactions governed by these requirements are processed using equipment and methodologies to ensure that they are kept secure.

	YES	NO	N/A
1. All cardholder-entered PINs are processed in equipment that conforms to the requirements for Tamper-Resistant Security Modules (TRSMs). TRSMs are considered tamper responsive or physically secure devices (i.e., penetration of the device will cause immediate erasure of all PINs, secret and private cryptographic keys, and all useful residues of PINs and keys contained within it). All newly deployed ATMs and POS PIN acceptance devices are compliant with the applicable PCI PIN Entry Device and Encrypting PIN Pad Security Requirements.	☐	☐	☐
2a. All cardholder PINs processed online are encrypted and decrypted using an approved cryptographic technique that provides a level of security compliant with international and industry standards. Any cryptographic technique implemented meets or exceeds the cryptographic strength of TDEA using double length keys.	☐	☐	☐
2b. All cardholder PINs processed offline using IC Card technology must be protected in accordance with the requirements in Book 2 of the *EMV IC Card Specifications for Payment Systems* and ISO 9564.	☐	☐	☐
3. For online interchange transactions, PINs are only encrypted using ISO 9564–1 PIN block formats 0, 1 or 3. Format 2 must be used for PINs that are submitted from the IC card reader to the IC card.	☐	☐	☐
4. PINs are not stored except as part of a store-and-forward transaction, and only for the minimum time necessary. If a transaction is logged, the encrypted PIN block must be masked or deleted from the record before it is logged.	☐	☐	☐

Objective 2

Cryptographic keys used for PIN encryption/decryption and related key management are created using processes to ensure that it is not possible to predict any key or determine that certain keys are more probable than other keys.

	YES	NO	N/A
5. All keys and key components are generated using an approved random or pseudo-random process.	☐	☐	☐
6. Compromise of the key-generation process is not possible without collusion between at least two trusted individuals.	☐	☐	☐
7. Documented procedures exist and are demonstrably in use for all key-generation processing.	☐	☐	☐

Objective 3			
Keys are conveyed or transmitted in a secure manner.			
8. Secret or private keys are transferred by: a. Physically forwarding the key as at least two separate key shares or full-length components (hard copy, smart card, TRSM) using different communication channels, **or** b. Transmitting the key in ciphertext form **Note:** Public keys must be conveyed in a manner that protects their integrity and authenticity.	**YES** ☐	**NO** ☐	**N/A** ☐
9. Any single unencrypted key component is at all times during its transmission, conveyance, or movement between any two organizational entities: a. Under the continuous supervision of a person with authorized access to this component, **or** b. Locked in a security container (including tamper-evident packaging) in such a way that it can be obtained only by a person with authorized access to it, **or** c. In a physically secure TRSM	**YES** ☐	**NO** ☐	**N/A** ☐
10. All key encryption keys used to transmit or convey other cryptographic keys are (at least) as strong as any key transmitted or conveyed.	**YES** ☐	**NO** ☐	**N/A** ☐
11. Documented procedures exist and are demonstrably in use for all key transmission and conveyance processing.	**YES** ☐	**NO** ☐	**N/A** ☐

Objective 4			
Key loading to hosts and PIN entry devices is handled in a secure manner.			
12. Unencrypted keys are entered into host Hardware Security Modules (HSMs) and PIN Entry Devices (PEDs) using the principles of dual control and split knowledge.	**YES** ☐	**NO** ☐	**N/A** ☐
13. The mechanisms used to load keys (such as terminals, external PIN pads, key guns, or similar devices and methods) are protected to prevent any type of monitoring that could result in the unauthorized disclosure of any component.	**YES** ☐	**NO** ☐	**N/A** ☐
14. All hardware and passwords used for key loading are managed under dual control.	**YES** ☐	**NO** ☐	**N/A** ☐
15. The loading of keys or key components must incorporate a validation mechanism such that the authenticity of the keys is ensured and it can be ascertained that they have not been tampered with, substituted, or compromised.	**YES** ☐	**NO** ☐	**N/A** ☐
16. Documented procedures exist and are demonstrably in use (including audit trails) for all key-loading activities.	**YES** ☐	**NO** ☐	**N/A** ☐

Objective 5

Keys are used in a manner that prevents or detects their unauthorized usage.			
17. Unique secret cryptographic keys must be in use for each identifiable link between host computer systems.	YES ☐	NO ☐	N/A ☐
18. Procedures exist to prevent or detect the unauthorized substitution (i.e., unauthorized key replacement and key misuse) of one key for another or the operation of any cryptographic device without legitimate keys.	YES ☐	NO ☐	N/A ☐
19. Cryptographic keys are only used for their sole intended purpose and are never shared between production and test systems.	YES ☐	NO ☐	N/A ☐
20. All secret and private cryptographic keys ever present and used for any function (e.g., key-encipherment or PIN-encipherment) by a transaction-originating terminal (i.e., PED) that processes PINs must be unique (except by chance) to that device.	YES ☐	NO ☐	N/A ☐

Objective 6			
Keys are administered in a secure manner.			
21. Keys used for enciphering PIN encryption keys (or for PIN encryption) must never exist outside of TRSMs, except when encrypted or securely stored and managed using the principles of dual control and split knowledge.	YES ☐	NO ☐	N/A ☐
22. Procedures exist and are demonstrably in use to replace any known or suspected compromised key and its subsidiary keys (those keys enciphered with the compromised key) to a value not feasibly related to the original key.	YES ☐	NO ☐	N/A ☐
23. Key variants are only used in devices that possess the original key. Key variants are not used at different levels of the key hierarchy (e.g., a variant of a key encipherment key used for key exchange cannot be used as a working key or as a master file key for local storage).	YES ☐	NO ☐	N/A ☐
24. Secret and private keys and key components that are no longer used or have been replaced are securely destroyed.	YES ☐	NO ☐	N/A ☐
25. Access to secret and private cryptographic keys and key materials must be limited to a need-to-know basis so that the fewest number of key custodians are necessary to enable their effective use.	YES ☐	NO ☐	N/A ☐
26. Logs are kept for any time that keys, key components, or related materials are removed from storage or loaded to a TRSM.	YES ☐	NO ☐	N/A ☐
27. Backups of secret and private keys must exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.	YES ☐	NO ☐	N/A ☐
28. Documented procedures exist and are demonstrably in use for all key administration operations.	YES ☐	NO ☐	N/A ☐

Objective 7
Equipment used to process PINs and keys is managed in a secure manner.

	YES	NO	N/A
29. PIN-processing equipment (PEDs and HSMs) is placed into service only if there is assurance that the equipment has not been substituted or made subject to unauthorized modifications or tampering prior to the loading of cryptographic keys.	☐	☐	☐
30. Procedures exist that ensure the destruction of all cryptographic keys and any PINs or other PIN-related information within any cryptographic devices removed from service.	☐	☐	☐
31. Any TRSM that is capable of encrypting a key and producing cryptograms of that key is protected against unauthorized use to encrypt known keys or known key components. This protection takes the form of either or both of the following: a. Dual access controls are required to enable the key encryption function. b. Physical protection of the equipment (e.g., locked access to it) under dual control.	☐	☐	☐
32. Documented procedures exist and are demonstrably in use to ensure the security and integrity of PIN-processing equipment (e.g., PEDs and HSMs) placed into service, initialized, deployed, used, and decommissioned.	☐	☐	☐

Appendix G: List of Supporting Documents

The following documents can be downloaded at *www.Visa.com/cisp*, *www.Visa.com/pinsecurity, www.Visa.com/pin, www.pcisecuritystandards.org*

- Qualified Incident Response Assessor (QIRA) List – List of forensic companies qualified to perform a PCI forensic investigation on compromised entities.
- Qualified Security Assessor (QSA) - List of assessors qualified to perform PCI assessments for those entities requiring onsite validation of PCI compliance.
- PCI Data Security Standard (PCI DSS) – Detailed security requirements to which Visa clients, merchants, and service providers must adhere to ensure the protection of cardholder data.
- PCI Security Audit Procedures – Detailed security requirements, guidelines, and testing procedures to assist a PCI QSA in verifying that an entity is in compliance with the PCI DSS.
- PCI Self-Assessment Questionnaire (SAQ) - The PCI SAQ is an important validation tool primarily used by smaller merchants and service providers to demonstrate compliance to the PCI DSS. Responses must address any system(s) or system component(s) involved in processing, storing, or transmitting Visa cardholder data. **Note**: For any answers where N/A is marked, a brief explanation should be attached.
- PCI Security Scanning Procedures - Procedures and guidelines for conducting network security scans for entities and third-party service providers who are scanning their infrastructures to demonstrate compliance to the PCI DSS.
- Acquiring institutions and agents involved with PIN transaction processing must comply with the security requirements and guidelines specified in the PIN Security documents that can be downloaded from *www.visa.com/pinsecurity*.
- PCI PIN Security Requirements (visit *www.visa.com/pinsecurity*).
- Visa PIN Security Program Auditor's Guide (visit *www.Visa.com/pinsecurity).*

Appendix H: Glossary of Terms

802.11	IEEE 802.11 is a set of standards for wireless local area network (WLAN) computer communication, developed by the IEEE LAN/MAN Standards Committee (IEEE 802) in the 5 GHz and 2.4 GHz public spectrum bands.
Acquirer	Financial institution that enters into agreements with merchants to accept Visa cards as payment for goods and services. Commonly referred to as the "merchant bank".
Agent	Any contractor, including third-party processors and servicers, whether a client or non-client, engaged by a client to provide services or act on its behalf in connection with Visa payment services.
At Risk Accounts	Refers to accounts that were included in a CAMS "Alert" of a suspected or confirmed compromised event.
Authentication	The process of verifying the true origin or nature of the sender and/or the integrity of the text of a message.
Authorization	A process by which an issuer approves a transaction for a specified amount with a merchant.
Backdoor	A method of bypassing normal authentication and obtaining access to plaintext information while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice), or could be a modification to an existing program or hardware device.
Bank Identification Number (BIN)	A unique number assigned by the bankcard association to its members. On a cardholder's account number, the BIN appears as the first six digits. Visa BINs begin with the number "4."
Card Authorization Acceptor ID	Information found in the authorization message (Field 42) from a legitimate transaction at the Acceptor ID CPP-identified merchant.
Common Point of Purchase (CPP)	Refers to the location of a legitimate transaction (usually a purchase or cash advance transaction) common to a number of accounts involved in a fraud scheme of similar character. The "common point of purchase" is assumed to be the point of compromise.

Card Verification Value (CVV)	A unique three-digit “check number” encoded on the magnetic stripe of all valid cards. The number is calculated by applying an algorithm (a mathematical formula) to the stripe-encoded account information, and is verified online at the same time that a transaction is authorized.
Card Verification Value 2 (CVV2)	A Visa fraud prevention system used in card-not-present transactions to ensure that the card is valid. The CVV2 is the three-digit value that is printed on the back of all Visa cards. Card-not-present merchants ask the customer for the CVV2 and submit it as part of their authorization request. For information security purposes, merchants are prohibited from storing CVV2 data.
Cardholder	The person or entity whose name is embossed on the face of a card or encoded on the magnetic stripe.
Cardholder Data	All identifiable personal data about the cardholder and the relationship to the client (e.g., account number, expiration date, data provided by the client, other electronic data gathered by the merchant/agent). This term also applies to other personal insights gathered about the cardholder such as address, telephone number, etc.
Client	An organization that is a member of Visa and issues cards and/or signs merchants.
Compromise	Process that exposes cardholder account information to third parties, placing cardholders at risk of fraudulent use.
Compromised Account	Accounts downloaded by an intruder or found in criminal possession.
Compromised Account Management System (CAMS)	Via CAMS, acquirers, merchants and law enforcement officers can safely upload compromised and stolen/recovered accounts directly to Visa. As this information is received by CAMS, e-mail alert messages are automatically sent to registered issuer users to notify them of the compromised and stolen/recovered accounts.

Cryptographic Key	A parameter used in conjunction with a cryptographic algorithm that determines: • The transformation of plaintext data into ciphertext data • The transformation of ciphertext data into plaintext data • A digital signature computed from data • The verification of a digital signature computed from data • An authentication code computed from data or • An exchange agreement of a shared secret
Denial of Service (DoS)	Denial of Service (DoS) is a tool or program used by intruders to cause networks and/or computers to cease operating effectively or to erase critical programs running on the system.
Electronic Commerce (e-commerce)	The purchase of goods and services over the Internet without a paper transaction between buyer and seller.
Entity	An organization that stores, processes or transmits account information. Typically the victim in a compromise. Also refers to any payment industry organization that must be PCI DSS compliant.
Encryption	An online data security method that scrambles data so that it is difficult to interpret without a corresponding decryption key.
Event	Refers to a single event of a known or suspected data compromise. It is used interchangeably with the term “incident”.
Full-Track Data	There are two tracks of data on a bankcard’s magnetic stripe: • Track 1 is 79 characters in length. It is alphanumeric and contains the account number, the cardholder name, and the additional data listed on Track 2. • Track 2 is the most widely read. It is 40 characters in length and is strictly numeric. This track contains the account number, expiration date, secure code, and discretionary institution data.
Hacker	A person who deliberately logs on to other computers by circumventing the log-on security system. This is sometimes done to steal valuable information or to cause damage that might be irreparable.

IEEE (Institute of Electrical and Electronics Engineers, Inc.)	The Institute of Electrical and Electronics Engineers, Inc., is an international non-profit, professional organization for the advancement of technology. More info at www.ieee.org.
Incident	Refers to each single occurrence of known or suspected data compromise. It is used interchangeably with the term “event”.
Incident Response Managers	Visa staff designated by a regional office to coordinate response to incidents.
Issuer	A financial institution that issues Visa products.
Magnetic Stripe (Mag Stripe)	A strip of magnetic tape located on the back of all bankcards. The magnetic stripe is encoded with identifying account information as specified in the Visa Operating Regulations. On a valid card, the account information on the magnetic stripe matches similar embossed information located on the front of the card.
Man-in-the-Middle (MITM)	A form of eavesdropping in which an attacker makes independent connections with the victims and relays messages between them, making the victims believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.
MD5 Hash	The MD5 hash (also known as checksum) for a file is a 128-bit value, similar to taking a fingerprint of a file.
Member	An organization that is a member of Visa and issues Visa cards and/or acquires merchant transactions.
Merchant	An entity that enters into a card acceptance agreement with a Visa acquirer or processor.
Merchant Bank	See Acquirer.
Merchant Level	All merchants fall into one of four merchant levels based on Visa transaction volume over a 12-month period.
PAN	Primary Account Number.

Payment Card Industry Data Security Standard (PCI DSS)	A set of requirements established by the payment card industry to protect cardholder data. These requirements apply to all members, merchants, and service providers that store, process, or transmit cardholder data.
Payment Card Industry (PCI) PIN Security Requirements	A comprehensive set of measures created for the safe transmission and processing of cardholder PINs during ATM and point-of sale (POS) PIN-entry device (PED) transactions. All participants in the payment processing chain that manage cardholder PINs and encryption keys must be in full compliance with the PCI PIN Security Requirements. This document can be downloaded from the PIN website at www.Visa.com/pinsecurity.
PCI Security Standards Council ("PCI SSC")	The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and Pin-Entry Device (PED) Requirements. For more information on PCI SSC, visit www.pcisecuritystandards.org/.
Personal Identification Number (PIN) Identification Number (PIN)	An alphabetic and/or numeric code which may be used as a means of cardholder identification.
Point of Compromise (POC)	Refers to the location where account number data was obtained by unauthorized third parties.
Qualified Incident Response Assessor (QIRA)	Visa-approved security vendors who perform forensic investigations in the event of a security incident. A list of QIRAs can be obtained at *www.Visa.com/cisp*.
Qualified Forensic Investigator (QFI)	An individual or entity approved by the Payment Card Industry Security Standards Council (PCI SSC) to respond in the event of a security incident and perform forensic investigations.
Rootkit	A program designed to take administrative control of a computer system without authorization from the system's owners.
Secure Shell (SSH)	"Secure Shell" is a network protocol that allows data to be exchanged using a secure channel.
Service Set Identifier (SSID)	"Service Set Identifier" is the name used to identify the particular 802.11 wireless LAN to which a user wants to attach.

Telnet (Telecommunications Network)	A network protocol used on the Internet or on Local Area Network (LAN) connections.
Third-Party Processor	A service provider organization acting as the client's agent to provide authorization, clearing, or settlement services for merchants and members.
Third-Party Servicer	A service provider organization that is not a client of Visa and is not directly connected to VisaNet, but provides the following services to the client: • Response processing for Visa program solicitations • Transaction processing (including gateways) • Data capture • Other administrative functions such as chargeback processing, risk/security reporting, and customer service
Visa Cardholder Information Security Program (CISP)	A Visa program that establishes data security standards, procedures, and tools for all entities (merchants, service providers, issuers, and merchant banks) that store Visa cardholder account information. CISP compliance is mandatory. CISP requirements prohibit merchants and service providers from storing the full contents of any magnetic stripe, CVV2, or PIN-block data. For more information regarding CISP, visit www.Visa.com/cisp.
VisaNet	The data processing systems, networks and operations used to support and deliver authorization services, exception file services, clearing and settlement services and any other services.
WAP (Wireless Application Protocol)	An open international standard for application layer network communications in a wireless communication environment.
WAP or AP (Wireless Access Point)	A computer networking device that allows wireless communication devices to connect to a wireless network using Wi-Fi and related standards. The WAP usually connects to a wired network and can relay data between both wireless and wired devices (such as computers or printers) on the network.
WEP (Wired Equivalent Privacy)	An algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio and are more susceptible to eavesdropping than wired networks.

Appendix I: Investigation Definitions

Terminology	Description
Date(s) that data was transferred out of the network	The confirmed date(s) that data was transferred out of the network by the intruder or malware.
Date and Version of POS Installation (s)	Date(s) of when the entity began using the POS application and version number. If available, include date(s) of when entity installed a patch or an upgrade to no longer retain prohibited data.
Malware Installation Date(s)	The date(s) that malware was installed on the system, if applicable.
Date(s) of Real-Time Capture	Date(s) of when malicious code/malware, such as packet sniffer and/or key logger, was activated to capture payment card data on the network and system. Should also include date(s) of when malware was de-activated.
Window of Intrusion	First confirmed date that intruder or malware entered the system to the date of containment. Examples of containment include, but not limited to: • Removal of malware or rebuilt of compromised systems • Compromised system removed from the network • Blocking of malicious IPs on the firewall • Rotation of compromised passwords
Window of Storage	"Window of Storage" is defined as the frame of time in which a given set of prohibited data is initially placed on a system to the time that same data was removed. It answers the question, "how long was the given set of data stored?"
Transaction date(s) of stored accounts	Transaction date(s) is defined as the date of the transactions stored on the system.
Window of System Vulnerability	"Window of Vulnerability" is defined as the frame of time in which a weakness in an operating system, application or network could be exploited by a threat to the time that weakness is properly remediated. It answers the question, "how long was the system at risk to a given compromise?" Overall time period that a system was vulnerable to attack due to system weaknesses. For example, lack of/or poorly configured firewall, missing security patches, insecure remote access configuration, default passwords to POS systems, insecure wireless configuration.

2010 Financial Services Global Security Study

The faceless threat

Contents

Foreword

The new decade marks a turning point for those of us in the information security industry. We now live in an age of cyber warfare. The environment is dangerous and sinister. The children who used to make mischief in their basements are now only bit players and rarely make the news anymore. They have been superseded by organized crime, governments and individuals who make computer fraud their full-time business, either for monetary gain or for competitive or technological advantage. Countries now accuse each other of cyber warfare. Every network of substantial size has been compromised in some way. Governments are appointing senior military brass to focus on cyber warfare. The stakes have never been higher and the battle is being fought in every corner of the world. It's all out there: botnets, zombie networks, Trojans, malware, spam, phishing, much of it now so sophisticated even the most wary of us can be tricked.

We talk a lot about the increasing sophistication of threats. Now we have something else to deal with as well: the decreasing level of competence required to pose a threat. Consider Mariposa, the botnet that originated in Spain and infected millions of computers. The perpetrators had "limited computer skills" and they didn't write their own brilliant computer program – they simply downloaded what they needed from the internet. A new reality is the increasing availability of tools on the internet, allowing those with less know-how to get in on the cyber crime act.

This year's security study responses support the reality that a turning point in the industry has arrived:

- For the first time, organizations are proactive, embracing new technologies as "early majority adopters", no longer content, as "late majority adopters", to simply be reactive.

- For the first time, the lowest percentage of respondents (36%) stated that "lack of sufficient budget", is the major barrier to ensuring information security, compared to 56% last year. During the worst economic downturn in recent memory when so many budgets are being cut, information security budgets are safe for the most part and many have increased.

- For the first time, information security compliance (internal/external audit) remediation is a top-five security initiative as organizations gear up for increased regulation and legislation.

- For the first time, more than half of organizations state that physical information, such as paper, is within the mandate and scope of the executive responsible for information security. The response (59%) is still too low – and indicates a security gap – but, in our opinion, it is moving in the right direction.

This is now the seventh year of our survey. These survey questions involve time and effort on the part of busy people who take time away from very important jobs. My sincere thanks go out to the Chief Information Security Officers, their designates, the security management teams from financial institutions around the world and all the people behind the scenes who make it possible to produce this global security study. Without you it simply could not be done.

We've been discussing change for years. Now it's here. It will take all our smarts, all our knowledge and all our expertise to wage and win the cyber war. It will be challenging and exciting but there will be progress on many fronts. In our view, there is no better time than the present decade to be part of the information security industry.

Adel Melek
DTT Global Leader, Information & Technology Risk
DTT Global Leader, Enterprise Risk Services
– Global Financial Services Industry

Participant profile

Participant breakdown

The data that allow us to discuss findings and current trends comes directly from those who are on the front lines of the global financial services industry. Deloitte* agreed to preserve the anonymity of the organizations who participated in the survey.

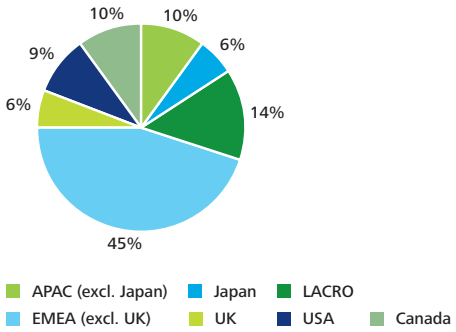
Overall, the participants represent:

- 27% of the top 100 global financial institutions.
- 26% of the top 100 global banks.
- 28% of the top 50 global insurance companies.

More than 350 major financial institutions worldwide have been interviewed by senior Information & Technology Risk practitioners for the 2010 Financial Services Industry (FSI) Global Security Study.

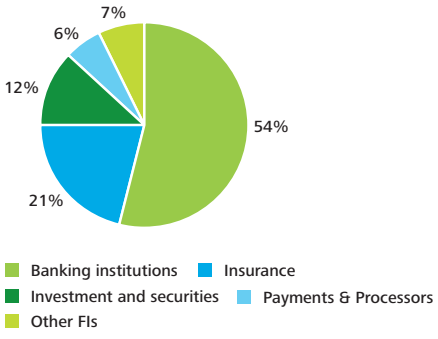
Regional breakdown

Financial services industry respondents to the 2010 FSI Global Security Study are from 45 countries around the world. The regional breakdown is as follows:



Sector breakdown

This year, the survey had good representation from the main sectors of the industry. The sector breakdown is as follows:

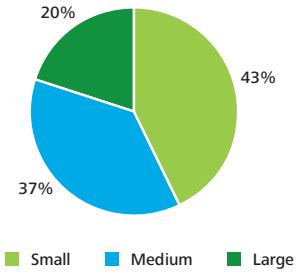


* As used in this document, Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms

Size breakdown

For the purpose of this study, organizations considered "small" are those with fewer than 1,000 employees; organizations considered "medium" are those with 1,000 to 10,000 employees, and those considered "large" are those with more than 10,000 employees.

The size breakdown is as follows:



Revenue breakdown

Respondent organizations represent eight revenue categories.

The revenue breakdown is as follows:

<500M	33%
500M to 1B	11%
1B to 1.99B	5%
2B to 4.99B	9%
5B to 9.9B	4%
10B to 14.99B	2%
15B to 20B	3%
>20B	7%

Results may not total 100% as this survey is reporting selected information only; responses from those who decline to answer may not be included in the reported data.

Key findings

Cyber warfare has taken a chilling turn

There was a time when the perpetrators of cyber crime were bright children in basements making mischief. Fast forward to 2010. U.S. President Obama has made cyber war defence a top national priority. The U.S. government has appointed a national cyber coordinator. NATO has set up the Cooperative Cyber Defence Centre of Excellence (CCDCOE). When asked what external breaches they had experienced in the last 12 months, the greatest number of financial services industry respondents to the survey indicated repeated occurrences of malicious software originating from outside the organization. The survey reveals CISOs are far less confident that traditional controls will protect their organizations – with good reason. Cyber warfare has gone global and governments and organized crime are piling in.

Perhaps most unsettling of all are the lessons from the Mariposa botnet that infected more than 15 million computers around the world.* Mariposa was not the brainchild of brilliant computer programmers but individuals with "limited computer skills". They downloaded the software they needed from the internet for less than a thousand dollars and were so unsophisticated that one of them, using his home computer, led police to his door.

Today, the security environment is virtually unrecognizable from the early days – a single decade has produced fascinating but chilling developments. The bottom line is that the game has changed and no one is immune.

Identity and Access Management (IAM) is undergoing a metamorphosis

Respondents indicate that IAM is a top security initiative for 2010. Governance, Risk and Compliance (GRC) tend to be the driving forces behind IAM. Key issues, borne out by the top internal/external audit findings, are access certification, knowing who has access to information, whether it is appropriate, and documenting it – and strong governance that establishes automated, continuous processes for managing user access to information resources. IAM is a significantly higher priority for large organizations with more than 10,000 employees (63%) compared to small organizations with less than 1,000 employees (35%). Geography also influences respondents' responses: IAM is less of a priority in the U.K (35%) than in other parts of the world, particularly the U.S. (67%) and Japan (65%).

In the early days of information security (over the last decade), IAM performed the function of a gatekeeper, essentially keeping the bad guys out.

But IAM has evolved far beyond that, not only in authentication but in the level of granularity of access as well as in the ability to track back, stroke by stroke, what events took place, when, and by whom. Today, many organizations realize that simply entering a user ID and password is no longer adequate and are experimenting with two-factor authentication.
In addition, IAM has evolved to the point that solutions can be business enablers, allowing the organization to aggregate identities across the enterprise into a single view, simplify user access to multiple applications, reduce IT costs and increase productivity. Organizations are beginning to look at IAM for customers (i.e. using IAM tools for customer identification). On a final note, IAM processes and practices tend to be expensive and thus require buy-in from the lines of business to ensure its success. The security function needs to learn how to sell itself in order to get the required funding for IAM initiatives.

As organizations lose confidence in their ability to protect themselves against internal threats, data loss prevention takes on new urgency

Respondents state that data protection is their second highest priority after IAM. The greatest percentage (42%) is only "somewhat confident" in their ability to thwart attacks that originate internally and only 34% are "very confident". There is a marked difference between internal and external attacks – a respectable 56% state that they are "very confident" in their ability to thwart external attacks. Data loss prevention is a major undertaking that begins with the most time-consuming part: classifying existing information to identify what information needs protection and from whom. But as daunting as the project may be, organizations appear to recognize how crucial it is – respondents indicate that data loss prevention will be one of the most piloted technologies in the next 12 months. Both data protection as a priority and data loss prevention technology piloting show a rise from last year. Key issues around data loss prevention are access certification and data governance.

Regulatory compliance is a key priority for financial institutions

Financial institutions are clearly expecting more regulatory pressure. They also recognize the competitive and reputational requirement to meet – or exceed – industry "leading practice" and standards set by associations such as ISACA, ISO, IIA, etc.

Respondents to the survey include regulatory and legislative compliance as one of their top five initiatives and are hiring more internal auditors to resolve internal and external audit findings.

* Downloaded from http://www.theglobeandmail.com/news/technology/canadian-firm-helps-disable-massive-botnet/article1488838/on March 10, 2010)

For the first time in the history of the survey, information security compliance remediation based on the findings of internal and external auditors is one of the top five security initiatives of organizations. Although "lack of oversight and compliance to security control requirements" is far down the list of internal/external audit findings (only 13%) organizations are shoring up for the anticipated increase in regulation. This is a clear indication that the environment has moved from one of "tell me you're in control" of significant financial and non-financial risks to "prove to me". Therefore, the need to be able to evidence this at any time for regulators, in particular, and as part of good governance practice, is an enterprise-wide issue for financial institutions.

While organizations are increasingly recognizing the need for a formal security strategy, the alignment of security and business objectives is lacking

It is not the existence of a security strategy that is at issue in financial institutions in 2010 (87% of respondents have one or plan to have one within the next 12 months; only 12% do not have one at all). What is more pertinent is that many organizations' security functions do not get input or involvement from the lines of business when the security strategy is being developed, which means that the strategy tends to be security function driven rather than business goals driven. This is clearly not the ideal situation and one that thwarts continued visibility and recognition of the value of the function. In addition, more and more organizations have a centralized security function, which is a positive development from a protection standpoint but may also prevent organizations from collecting feedback from the lines of business. Consequently, security goals are not aligned with those of the business and the security function suffers from lack of impact and business alignment. The absence of clear measurable security metrics that can be understood by lines of business means that the security function cannot clearly demonstrate its value and consequently may have a hard time getting funding for important projects. While 65% of respondents maintain that they actively engage both lines of business and IT decision makers in their security strategy, that still means that at least 30% of organizations do not. Predictably, only 37% of respondents maintain that business and information security initiatives are "appropriately aligned."

Involving business in the creation of the security strategy takes perseverance, consistency and some short-term pain to realize benefits that extend well into the future. The security strategy – developed and utilized in the right way – is the key to changing the profile of the security function.

Security budgets appear to be bucking the current trend of cost-cutting

The survey reveals that, in 2010, despite the global economic downturn of the past two years, there is a significant drop, as compared to last year, in the number of respondents who state that "lack of sufficient budget" is a major barrier that their organization faces (only 36% of respondents this year versus 56% of respondents last year). This may well be a product of a general dawning of the realization that, as the information security environment gets more dangerous, investment in data protection must get more serious. Given this, the security function must now be prepared to demonstrate ROI to further cement this trend. Top spending priorities in 2010 include identity and access management (IAM), data protection, security infrastructure improvement, regulatory and legislative compliance, and information security compliance remediation based on the findings of internal and external auditors.

Security technologies are experiencing a new maturity and a higher profile

There was a time when executives of financial services institutions viewed investment in emerging technologies as unnecessary and risky "budget gobblers". They were content for their organizations to be considered "late adopters" of technology, the theory being that it was more cost-effective to invest in technologies only after they were tried and true. In 2010, that scenario appears to be no longer valid. There are a number of reasons for this shift in attitude. First of all, technologies are much more mature. As an example, early versions of logging/monitoring tools generated endless reports that were of little value. Current technology allows the aggregation of events and automates their analysis.

In addition, Security Information and Event Management (SIEM) is one of the fastest growing segments of the market according to analysts. SIEM solutions analyze security event data in real time to identify threats, and analyze and report on log data for compliance monitoring. With SIEM solutions, gone are the endless reports that caused IT security teams to drown in security event data and lose control of corporate security. Another reason for the higher profile of emerging technologies is that, as revealed by the survey, spending on IT security has remained a priority for organizations. That makes it easier for organizations to improve security infrastructure and invest in products for which they previously had no room in their budgets. The other reason for the changing scenario is that more than 70% of survey respondents indicated they are planning to implement at least one information security-related technology in the next 12 months.

Given the increasing sophistication of threats and the increasing volume of regulation, sitting back and waiting is now viewed as riskier than taking action.

Convergence between information and technology risk functions is moving from concept to reality

Back in 2006, when Deloitte's security survey of the global financial services industry first introduced a question related to convergence, the idea was very much a concept. In 2010, the survey reveals that, in four short years, convergence has come a long way. This result could be attributable to the fact that convergence (formal cooperation between previously disjointed functions and not simply merging the groups on the organizational chart) is now better understood. In the survey, more than 57% of respondents either use enterprise risk councils, have the separate functions report into one common executive or have structurally converged. Only 26% have not undergone a process toward convergence. This is a welcome trend for those in the industry since the advantages of convergence, such as aligning security goals with corporate goals, a single point of contact, and increased information sharing are a clear benefit to the organization.

Paper-based information remains a low priority for the CISO

Paper is still the most prevalent information medium, and paper is still considered the legal copy of record in many disciplines. Yet the responsibility for the protection of paper-based information in organizations appears to have fallen through the cracks. Only 59% of respondents state that assets in physical form, i.e., paper, are within the mandate and scope of the CISO. However, this is an increase from the previous year (45%) and may also support our previous assertion that convergence is becoming more of a reality. Recognition of the risk that paper-based information poses indicates a greater understanding of information security as different from IT security.

Geography as a factor in security practices

	2009 Global	2010 Global	APAC (excl. Japan)	Japan	LACRO	EMEA (excl. UK)	ME	UK	USA	Canada
Respondents who indicated that their information security executive reports to the CIO	33%	24%	22%	0%	18%	26%	20%	15%	45%	24%
Respondents who feel they have both commitment and funding to address regulatory security requirements	59%	62%	74%	30%	48%	64%	61%	60%	74%	71%
Respondents who indicated that they have a documented and approved information security strategy	61%	60%	71%	65%	54%	61%	47%	50%	55%	56%
Respondents who feel that information security and business initiatives are appropriately aligned	32%	37%	56%	35%	34%	35%	38%	40%	33%	35%
Respondents who indicated that their information security budget has increased	60%	56%	56%	16%	64%	53%	56%	70%	56%	76%
Respondents who indicated that their expenditures on information security were 'on plan' or 'ahead of requirements'	43%	45%	50%	40%	58%	41%	27%	50%	30%	53%
Respondents who feel that their internal staff have all the required competencies to handle existing and foreseeable security requirements	34%	45%	49%	20%	37%	50%	42%	45%	45%	44%
Respondents who have one or more executive(s) responsible for privacy	57%	53%	37%	100%	30%	42%	11%	60%	77%	71%
Respondents who have a program for managing privacy compliance	48%	50%	44%	95%	24%	44%	17%	55%	70%	71%
Respondents who train employees to identify and report suspicious activities	71%	64%	83%	35%	62%	59%	58%	75%	82%	62%
Respondents who included Identity and Access Management into the list of their priority initiatives for 2010	54%	44%	42%	65%	38%	35%	15%	35%	67%	62%
Respondents who are very or extremely confident in their third parties' security practices		36%	29%	90%	40%	33%	35%	15%	6%	41%
Respondents who fully implemented encryption for mobile devices		44%	42%	50%	12%	42%	13%	80%	61%	65%
Respondents who indicated that they have and maintain a loss event database		54%	53%	70%	43%	52%	40%	79%	68%	44%

Highest score Lowest score

Asia Pacific (excluding Japan)*

Despite the fact that Japan is in the APAC region, for the purposes of this document we discuss Japan separately from the rest of APAC. Overall, APAC ranks higher than the global average on most issues. APAC is consistent with most other regions, with the exception of Japan, in having their CISO report to the Chief Information Officer (CIO), indicating that, as it is with the other regions, information security is viewed primarily as an IT function. Respondents report having 1 to 5 full time information security professionals (54%), slightly higher than the global average of 52%. They have a documented and approved security strategy (71%), the best showing of any of the regions, and much higher than the global average of 60%.

The most unique feature about APAC survey participants is that they state they have both commitment and adequate funding to fulfill regulatory security requirements (74%). This is far higher than the global average of 62% and on par with the United States. APAC led the pack on the same question in last year's survey as well. Since they have no funding issues, they appear to have security in check: the security strategy is in place, initiatives are aligned, and they have the time and resources for awareness training, which has helped them get up to speed on competencies. APAC has made a big leap in this area.

* For the purposes of this document, we have separated Japan from the rest of Asia Pacific

This year, 49% of respondents reported that their internal staff had the required competencies to handle existing and foreseeable security requirements, a huge improvement over 34% last year and higher than the global average of 45%. APAC also leads in training employees to identify and report suspicious activities with 83%, far higher than the global average (64%) and slightly higher than the United States.

The only "red flag" issue for APAC may be in the area of privacy. Along with LACRO, they have the highest number of respondents (23%) who state that they have no privacy program in place. When posed the question "Who does your organization's executive(s) responsible for privacy report to?" a high 61% of respondents state that they did not know.

APAC is one of few regions that have no lowest scores this year. It appears that when APAC respondents recognize a problem they do something about it. Privacy may be their issue to improve for the coming year.

Japan

Far more than any other region, Japan reports having their CISO report to the Board of Directors (50% versus a global average of only 10%). This may be due to the fact that board member composition is somewhat different in Japan from many other countries: board members of most public organizations are insiders, i.e., they are corporate executives, and the number of board members tends to be far more numerous than in other parts of the world. Although this situation may be slowly changing, many Japanese organizations still have boards comprised of insiders.

Respondents from Japan state that they have a documented and approved information security strategy, at 65%, slightly higher than the global average (60%), higher even than the United States and Canada (55% and 56%, respectively) and a big leap from last year.

But here is where similarity to other regions ends. Survey participants from Japan appear to have no commitment to the information security strategy and therefore little funding. In fact, responses to questions regarding budgets are mystifying: only 16% indicate that their information security budget has increased, a number that falls woefully short of the global average of 56% and the general trend of budget increases given the environment. They are the lowest of all regions in believing that their staff has required competencies (20%). Only 35% train employees to identify and report suspicious activities (versus the global average of 64% and much lower than APAC at 83%).

Japan's bright spot is privacy. They are far and away the leaders in the area of privacy: 100% have an executive responsible for privacy (versus the global average of 53%) and 95% have a program for managing privacy compliance (versus the global average of 50%). Japan is also the region most confident about third party security practices. Even though they do not adhere to information security practices that some consider to be most effective, Japan apparently had an uneventful year with no major scandals or data losses. This may simply be luck or it could be influenced by culture and language: integrity and honour are revered and celebrated attributes in Japan and the language barrier may also be an issue as most attacks on Japanese organizations have originated from outside Japan.

Latin America & Caribbean (LACRO)

LACRO had an impressive showing last year, leading the pack in many areas. This year, however, they have fallen to the middle of the pack in areas they led last year. In LACRO, as in other regions, the majority of respondents indicate that their executive responsible for information security reports to the CIO. LACRO is close to the global average (60%) in having a documented and approved security strategy (54%) but this is a surprising finding given that they led in this area last year. In addition, LACRO's lack of commitment and funding, at 48%, is second only to Japan's and much lower than the global average of 62%. LACRO ranks among the lowest regions who feel that information security and business initiatives are appropriately aligned, and this finding is consistent with their lack of commitment and funding.

Japan's bright spot is privacy: 100% of respondents have an executive responsible for privacy and 95% have a program for managing privacy compliance.

As it is in APAC, privacy is an issue for LACRO – which comes as no surprise, given that there is little or no privacy legislation in the countries of the region and a dominant open and welcoming culture; in fact, they fare the worst in having an executive responsible for privacy (30% versus the global average of 53%) and in having a program for managing privacy compliance (24% versus the global average of 50%).

LACRO also scored among the lowest in having encryption for mobile devices (12% versus the global average of 44%) and in having and maintaining a loss event database (43% versus the global average of 54%). Clearly, without a loss event database, it is hard to have an accurate information security perspective.

A bright spot is that LACRO respondents (64%) indicate that their information security budgets have increased. This is higher than the global average of 56% and higher than at least three other regions. So while LACRO respondents are higher only than Japan in feeling that they do not have commitment and funding, it appears that there is an effort to right this issue through increased budgets.

EMEA (excluding U.K.)

As in all other regions, with the exception of Japan, the majority of respondents (26%) indicate that their executive responsible for information security reports to the CIO. The highest of all regions, EMEA respondents (50%) indicate that their security staff has all the required competencies to handle existing and foreseeable security requirements, higher than the global average of 45%. A respectable percentage of respondents (61%) indicate a documented and approved information security strategy, in line with the global average of 60%. EMEA respondents are slightly higher than the global average in having the commitment and funding to address security requirements (64%). While just over half of EMEA respondents (53%) indicate that their information security budget has increased, that number is still second lowest to Japan and below the global average of 56%.

EMEA respondents do not have a great deal of confidence in the security practices of their third parties, although, at 33%, there are still three other regions – U.S., U.K. and APAC – that score lower. EMEA is one of four regions that does not score the lowest of all regions in any one area.

Middle East

This is the first year that the survey includes the Middle East (ME) as a separate region given the tremendous response and interest shown in completing this survey. Overall, we note that ME has more lowest scores than any other region. While other regions across the globe have more robust security and privacy legislation, the ME has yet to implement comprehensive security regulations. For example, the region has yet to have any formal privacy regulation, thus the low score with regard to managing privacy; only 11% have one or more executive(s) responsible for privacy and only 17% have a program for managing compliance with privacy requirements.

In addition, responses from the ME indicated that the region is in fifth place, after the U.S., APAC, Canada, and overall EMEA, in feeling that they have both the commitment and funding to address regulatory security requirements. The ME also lags behind other regions in terms of having a formally documented and approved information security strategy (47%).

Deloitte believes that ME is the region where a lot is likely to happen in a short time – the UAE has recently established a Computer Emergency Response Team (aeCERT) and Saudi Arabia is investing heavily in security technology. Similarly, Central Banks in Qatar and Lebanon have issued circulars and directives on various security-related matters. Jobs for information security professionals in the ME abound on the internet and the region hosts various conferences and events featuring information security.

United Kingdom (U.K.)

For the most part, the U.K. looks a lot like EMEA in many areas. However, only 15% of U.K. respondents (the lowest number of all regions with the exception of Japan) indicate that their executive responsible for information security reports to the CIO. The majority of U.K. respondents state that the most common reporting line (20%) is to the Chief Operations Officer. There is an increasing trend in the U.K. of re-organizing security as part of a combined security/fraud/financial crime/physical security function reporting to a COO.

This would indicate a higher profile for the information security function, which seems to be at odds with the fact that the U.K. scores the lowest of all the regions in having a documented and approved information security strategy (50%) and below the global average of 60%. Surprisingly, however, even with the low numbers concerning the strategy, U.K. organizations indicate that they have had their information security budgets increased (70%), the second highest behind Canada at 76%.

The U.K. has always had enthusiastic and knowledgeable consumers of technology (they lead the world in the number of cellular phones per capita) so it is not surprising that they excel (and lead the pack) in fully implemented encryption for mobile devices (80% versus the global average of only 44%). The U.K. also leads the rest in having and maintaining a loss event database (79% versus a global average of 53%). This is not surprising since banks, under the operational risk requirements for Basel II, are required to systematically collect loss event data. Basel affects all banks and financial institutions whose regulating authorities adopt the standards and methods. Even financial institutions that are not subject to Basel often follow the banks' lead since Basel is seen as the ultimate standard.

U.K. respondents are in line with the global average (both 45%) in believing that they have the required competencies to handle existing and foreseeable security requirements.

But the survey findings reveal an interesting dichotomy about U.K. organizations. While they excel in encryption and risk management (loss event database), they pay little attention to IAM and, in fact, rank lowest of all regions (35%) and far below the U.S. (67%) in making IAM a top security initiative. All other regions indicate that IAM is either the top or in the top three of their security initiatives for 2010. Another interesting finding is that only 15% of U.K. organizations are confident in their third parties security practices, second lowest only to the U.S. at 6%, yet they excel in maintaining a loss event database.

United States (U.S.)

The majority of the U.S. respondents report having an executive responsible for information security, and this is the highest response among all regions at 91%.

The United States is the region where the greatest number of executives responsible for security report to the CIO, 45% compared to the global average of 24%. This finding cements the fact that the security function in U.S. organizations is considered hugely a technical function. U.S. respondents are the middle of the pack (55%) when it comes to having a documented and approved information security strategy. However, they score the lowest of all regions (33%) when it comes to the alignment of security and business initiatives, not surprising since many of their information security functions are considered part of IT. When information security is considered mostly a technical function within a centralized security model, there may be no representatives in the lines of business and therefore not enough interaction between security and the business.

While U.S. respondents indicate that they have the commitment and funding to address regulatory security requirements (74% and on par with APAC, the highest of all regions) the responses would appear to apply more to commitment than funding since, when asked to characterize their expenditures on information security, the highest number of U.S. respondents indicate that they are merely "catching up" as opposed to the highest number of other respondents who state that they are "on plan".

With increased regulatory expectations, "catching up" may indicate a problem for U.S. organizations in responding to regulatory pressures.

Many consider the United States, the home of Wall Street and the most powerful capital markets system in the world, to be the country most beset by financial scandals. Understandably, IAM is high on U.S. respondents list of priorities; at 67%, it is the highest of any region. This may partially explain why respondents say they are "catching up" in information security expenditures since IAM is expensive.

The U.S., the U.K. and Canada customarily rely on outsourcers to perform at least some of their internal functions but the U.S., of all respondents, has the lowest level of confidence (6% compared to a global average of 36%) in their third parties' security practices. That begs the question as to why they outsource to the degree that they do, particularly when they indicate that they have the required competencies to handle existing and foreseeable security requirements.

Understandably, given the terrorist attacks of 9/11 and subsequent thwarted attacks and threats, respondents from the United States were more likely to choose state or industrial espionage as a high threat (21%) compared, for example, to their close neighbor, Canada, where respondents rate this same category as 0%.

Canada

The country with a banking system that is often held up as an example of stability to the rest of the world has made significant security improvements over last year, with no lowest scores in any area. Canada is similar to all other regions (with the exception of Japan) in having its CISO report to the CIO. But despite the appearance of information security being a technical function, Canada reported the second highest number of respondents (71%) who believe that they have the commitment and funding to address security regulatory requirements. Canada is middle of the pack (56%) in having a documented and approved information security strategy but has improved in a number of areas over last year: security and business initiatives are more aligned (35% this year versus 28% last year); required competencies are increasing (44% this year versus 33% last year); and Canadian respondents must be celebrating the end of the recession: of respondents who indicate that their information security budgets have increased, Canada leads the pack with 76%. In addition, there is a huge improvement over last year in expenditures being on plan or ahead of requirements – 53% this year versus only 26% last year.

But despite these improvements, Canadian organizations need to improve in some areas. They are below the global average in training employees to identify and report suspicious practices (62% versus 64%) and below the global average in maintaining a loss event database (44% versus 54%). Without such a risk management process, Canadian financial services organizations will find it difficult to be in compliance with increasing regulatory and industry requirements.

An area that is likely to become an issue for Canadian organizations is industrial espionage. Compared to U.S. respondents, who rated this threat as high, not one Canadian respondent felt it was a concern (0%). However, this may simply be a case of overconfidence or lack of visibility of the real threat. Some in the information security industry generally accept that the next major terrorist attack is likely to begin with a blackout and not with a bang. Despite its relatively benign profile on the world stage, Canada is inextricably linked with the U.S., its closest neighbor and greatest trading partner, and the Canadian government has not done nearly as much as the U.S. and U.K. governments in this area. This may be the "sleeper" threat of the decade and it is, in Deloitte's view, one that probably deserves far more attention.

Size as a factor in security practices

		Global	Employees		
			<1,000	1,000-10,000	>10,000
Governance and funding	Respondents where security executive has information in physical form included into mandate	59%	50%	63%	72%
	Respondents including disaster recovery planning into the list of functions of the executive responsible for security	49%	60%	46%	29%
	Respondents who have gone through a process of structural convergence between information and technology risk	25%	21%	25%	33%
	Respondents who have documented and approved information security strategy	60%	53%	61%	72%
	Respondents engaging both lines of business and technology executives in defining information security requirements	65%	60%	63%	81%
	Respondents who have established information security metrics aligned to business value and report on a scheduled basis	19%	16%	17%	28%
	Respondents indicating lack of sufficient budget as one of their major barriers	36%	36%	41%	29%
	Respondents who feel they have both commitment and funding to address regulatory security requirements	62%	57%	67%	64%
Threats, risks and mitigation activities	Respondents having excessive access rights in the top list of their audit findings	38%	32%	34%	56%
	Respondents who included Identity and Access Management into the list of their priority initiatives for 2010	44%	35%	44%	63%
	Respondents indicating increasing sophistication of threats as one of their major barriers	31%	31%	27%	41%
	Respondents who have fully implemented the following:				
	• File encryption for mobile devices	44%	36%	48%	57%
	• Vulnerability management	58%	53%	58%	72%
	• Federated identity management	16%	10%	20%	24%
	Respondents who are piloting data loss prevention technology	17%	13%	14%	29%
	Respondents who are planning to pilot or implement data loss prevention technology	26%	22%	34%	24%
	Respondents who train employees to identify and report suspicious activities	64%	53%	67%	79%
	Respondents who indicate that they have and maintain a loss event database	54%	48%	50%	78%

Highest score Lowest score

Not surprisingly, large organizations are much more advanced in their security practices than medium or small organizations and the size of the security function is directly dependent on the size of the organization. However, there are some surprises in the size discussion and observations do not always follow a predictable pattern. For the purposes of this discussion, organizations with fewer than 1,000 employees are considered small; organizations with 1,000-10,000 employees are considered medium; and organizations with more than 10,000 employees are considered large.

The information security executive is more likely to report to the CIO in large organizations than small, probably because small organizations are less likely to have a CIO or the person who performs an information security role is likely to do the job of the CIO as well. There is evidence of strong information security practices in larger organizations.

Information in physical form, i.e., paper, is included in the information security executive's mandate of both large (72%) and medium (63%) organizations. This may well be attributable to the fact that, given recent breaches and incidents, large organizations realized they needed to adopt stronger security practices and went through revisions of their information security mandate, part of which involved assigning responsibility for data in various forms. Additionally, in small organizations, Disaster Recovery Planning functions – and we observe the same pattern for business continuity – are often included as part of the mandate of the information security executive (60%) versus for medium (46%) or large (29%), where this is handled by separate individuals. In small organizations, by necessity, the security function is more likely to take on additional responsibilities.

Organizations of all sizes are beginning to realize the need for a security strategy. The increasing sophistication and frequency of threats, the current environment of huge failures and restructurings, increasing regulation that is going to require the existence of a strategy are all factors that have induced large (72%), medium (61%) and small (53%) organizations to have a documented and approved security strategy. In addition, as organizations are adopting more technology, affecting functions outside security, e.g., IAM, they recognize that a security strategy ties everything together. As expected, large organizations (81%) feel the need to engage both lines of business and technology executives in defining information security requirements. This makes sense since they are engaging in large projects across functions. But small (60%) and medium (63%) organizations, where one would think the environment would make communicating and sharing information more conducive, tend to remain siloed when it comes to engaging business and technology.

Regardless of size, less than a third of organizations have established information security metrics aligned to business value and report on a scheduled basis, an area that last year's survey highlighted as needing attention as well. Large organizations (28%) are understandably ahead of medium (17%) and small (16%) organizations but the numbers for all are much lower than they should be. Clearly, measuring security is still an issue for all organizations. All of the organizations report excessive access rights as top audit findings (large: 56%; medium 34%; small: 32%), and it is especially true for large organizations with more people. As a result, large organizations (63%) are looking at IAM as a priority in 2010 but medium (44%) and small (35%) organizations are understandably restricted due to the cost of IAM.

Increasing regulation puts pressure on all organizations, particularly medium and small, because they need the resources to be able to respond to regulatory requirements. Large organizations obviously have more executive commitment but funding is likely to be tight because of the scale and type of projects that have to be implemented is greater than for small and medium. However, respondents in medium-sized organizations are most likely to indicate that lack of sufficient budget is one of their major barriers (41%) versus small organizations (36%) and large (29%).

When it comes to feeling they have both commitment and funding to address regulatory security requirements, medium-sized organizations, at 67%, are more confident than both small organizations (57%) who likely lack resources, and large organizations (64%) who are subject to more regulation. Medium sized organizations may be in the best situation: they have capabilities and resources but are not as heavily regulated as large ones and can escape the focus of attention.

The bad guys are very adaptable. In the earlier years, their targets were large banks and other financial institutions, the theory being that when they scored, they would score big. Now the fraudsters have changed their strategy since they are being thwarted more and more by large financial institutions with their new technology and savvier employees. Fraudsters appear now to forgo the big victory for a series of smaller ones and what better targets than small and medium organizations. They are even targeting functions and people, particularly within financial institutions, because they know they are less protected than those in the larger organizations. As a result, there is not a huge spread when respondents were asked to rate increasing sophistication of threats as one of their major barriers: large (41%); medium (27%); and small (31%).

When it comes to implementing technology, responses follow a predictable pattern: small organizations, who lack the required resources, score lowest and large organizations, with greater resources, score highest. But there are some interesting findings within the data. At 57%, large organizations score higher on implementing file encryption for mobile devices (versus 36% for small and 48% for medium). Understandably, large organizations have greater risk of information leakage through mobile devices because they have more of them. The response is also fueled by regulation; breach notification laws typically state that if the device lost is encrypted, there is no need to report the loss.

Questions regarding data loss prevention reveal some interesting findings. Predictably, organizations that are most likely to be piloting DLP are the ones with the larger workforce, greater volume of data, and typically more valuable data (29%) versus small (13%) and medium (14%) organizations. However, when it comes to planning to pilot or implement DLP, respondents who indicate the highest response are from medium-sized organizations (34%). This may well be because medium-sized organizations, without the budget flexibility, are waiting to see if the technology is mature and effective enough for their needs.

With a close to 80% response rate, large organizations are better than small (53%) and medium-sized (67%) organizations at training their workforce to identify and report suspicious activities. Obviously, the larger the workforce the greater the vigilance required. Larger workforces typically depend upon information security stewards to be able to prevent breaches, and detect and report them when they are happening.

When it comes to the issue of having and maintaining a loss event database, the responses are predictable: 78% for large organizations; 50% for medium organizations and 48% for small organizations. However, as we observed earlier, small to medium-sized organizations are increasingly the target of fraudsters. Recording and retaining internal risk data through a data base helps an organization to identify trends and continuously improve processes. Large organizations also need to be concerned with external risk data to understand and control their exposure and comply with regulation. For financial institutions, a formal program for managing risk data can drive growth through superior service delivery and improved decision making that is dependent on having the right data at the right place at the right time.

This is the first time Deloitte has included size-based comparisons in the study. The points made are ones Deloitte believes to be most interesting to readers. Additional data is available. Please contact a Deloitte member firm professional in your region for further insights.

Sector as a factor in security practices

	Global	Banking institutions	Insurance	Investments and securities	Payments and processors
Respondents where security executive reports to:					
• Chief Information Officer (CIO)	24%	21%	35%	24%	25%
• Board of Directors	10%	14%	8%	2%	5%
• Chief Executive Officer (CEO)	11%	11%	11%	10%	15%
Respondents who indicated that they have a documented and approved information security governance structure	76%	82%	76%	54%	86%
Respondents who have a centralized information security model	76%	79%	65%	76%	81%
Respondents who indicated that they have a documented and approved information security strategy	60%	70%	54%	46%	48%
Respondents who indicated that they experienced partial or full convergence between information and technology risk functions	76%	82%	76%	54%	86%
Respondents who included in their top security initiatives for 2010:					
• Information security governance	29%	28%	19%	41%	33%
• Identity and access management	44%	44%	51%	37%	38%
Respondents who indicated the following major barriers their organization face:					
• Lack of support from lines of business	19%	15%	32%	17%	24%
• Lack of sufficient budget	36%	32%	46%	39%	29%
Respondents who indicated that they have established metrics for information security function that have been aligned to business value and report on a scheduled basis	19%	24%	14%	13%	14%
Respondents who fully implemented file encryption for mobile devices	44%	42%	54%	46%	38%
Respondents who plan to implement data loss prevention technology	26%	25%	32%	29%	19%
Respondents who indicated that their organization trains employees to identify and report suspicious activities	64%	65%	74%	51%	57%
Respondents who identified risks related to third parties as part of information risk assessments	39%	37%	53%	27%	33%
Respondents who included third parties in the mandate and scope of security executive responsibilities	53%	53%	65%	46%	43%

Highest score Lowest score

In Deloitte's "Banking and Securities Outlook 2010"* DTT member firms subject matter specialists named five major trends that they believe will dominate the financial services industry in 2010. Three out of five of these trends relate to topics discussed in this report. They are as follows:

- The extent to which new regulations may impact financial firm's business models.
- The call for continued efforts to improve governance and risk oversight, especially at the board level.
- Meeting the challenge of core IT systems and data aggregation.

The specialists note that banks are cooperating with regulators and are trying to anticipate the direction in which the new rules might go. This is supported by the survey findings: while the CIO remains the primary reporting relationship for banks (21%), the secondary one is the Board of Directors (14%). This is in sharp contrast to the other sectors – Insurance, Investments and Securities, and Payment & Processors – where Boards play a less significant role in security governance.

Banks dominate the other sectors in having a documented and approved information security strategy as well as an information security governance structure (70% and 82%, respectively).

While 86% of the Payments & Processors sector respondents have an approved and documented information security governance structure, that high number is not due to their anticipation of increased regulation but rather to their compliance with Payment Card Industry (PCI) Data Security Standards (DSS) requirements. Banks' increased focus on governance is also reflected in their response to the question on information security function effectiveness measurement: 24% of banks have established metrics that have been aligned to business value and report on a scheduled basis, while Insurance, Investment and Payments & Processors are well below Banks with 14%, 13%, and 14% respectively.

Top security initiatives for 2010 provide an interesting perspective on the differences in security governance between sectors. Organizations in the Investment sector state that they are planning to work on establishing information security governance (41%) – a finding that is supported by the low number of Investment organizations (54%) who have a documented and approved governance structure. Insurance organizations report a low 19% for this particular initiative. However, this is likely not because insurance organizations are so advanced on the security front but rather because they are the lowest of all sectors to have a centralized security model adoption (65%). Strong security governance reporting vertical becomes less important when security is governed in a decentralized fashion. The fact that insurance organizations seem to see nothing wrong with this would indicated that they are experiencing less pressure from regulators or standards bodies.

Banks and insurance organizations are relatively close in their approach to risk function convergence: 82% and 76% respectively have experienced at least partial convergence between information and technology risk functions. Investment organizations are well behind at 54%. Increased convergence was predicted in Deloitte's "Banking and Securities Outlook 2010"; however, this means increased oversight: "It is expected that more boards may introduce explicit charters setting up risk committees (or adding risk to the Audit Committee's responsibilities) and reporting structures to strengthen board oversight and make sure this is communicated to shareholders."*

Increased support for risk-related initiatives in banks is evident in the responses to the question on barriers to information security. Banking respondents who choose "Lack of support from lines of business" and "Lack of sufficient budget" are significantly lower than those of the other sectors, particularly insurance organizations. Payments and Processors are somewhere in the middle; most likely because data security is key to their core business and most of them are already operating under strict PCI DSS requirements.

The insurance industry's focus on third parties is reflected in their answers to third party-related questions: 65% of insurance organizations, the highest across all sectors of financial services, include third parties within the mandate and scope of the information security executive's responsibilities. Additionally, 53% of insurance organizations identify risks related to third parties as part of information risk assessments (banks are second with only 37% who do so). The focus of insurance organizations on third parties extends to suspicious behavior identification: 74% of insurance organizations train their employees to identify and report suspicious behaviors; banks follow with 65% whereas investment organizations and Payments & Processors trail significantly. One would think that banks would lead on most fronts, given that they, of all the sectors, are perceived to have the most liquid assets on hand. However, it is becoming clear that insurance organizations have the strongest practices around third parties of all financial institutions. One of the reasons is that they are compelled to address risks resulting from their diverse and mobile army of insurance representatives: 54% of insurance organizations have fully implemented file encryption for mobile devices versus only 42% of banks who do so. Another reason is that insurance companies hold, and their representatives transmit, confidential personal information about their clients. It seems to be less catastrophic to an organization's reputation to lose millions of dollars than it is to expose personal information.

Deloitte's "Banking and Securities Outlook 2010"* also predicted that "banks are likely to begin a phase of heavy new investment in their technology infrastructure". This fresh appetite for new technology and infrastructure is reflected in banking respondents' answers to technology- and budget-related questions. But yet again, the appetite of insurance organizations is even higher (but this may be because they have much further to come: insurance organizations are ahead of banks with plans to implement data loss prevention technologies (32% versus 25% of banks and 29% of investment organizations). The same trend is apparent when it comes to top initiatives: identity and access management is stated as a priority by 51% of insurance organizations, 44% of banks, 37% of investment organizations and 38% of payments & processors.

* http://www.deloitte.com/view/en_US/us/Industries/ Banking-Securities-Financial-Services/article/05ff8971f7a75210VgnVCM200000bb42f00aRCRD.htm

While this may indicate that insurance organizations are eager to catch up with banks in the level of protection of their information assets, these numbers may provide some insights for technology and solution vendors: second- and third-tier vendors are likely to have greater success and return on their effort in the insurance sector.

Overall, while banks appear to have a stronger security posture than other financial services institutions, insurance organizations are catching up fast and have an edge in dealing with third-party risks. Payments & Processors are strong in technology and areas that fall under PCI DSS but sometimes lack in other areas. Investments and securities organizations appear to be trailing across multiple domains.

This is the first time Deloitte has included sector-based comparisons in the study. The points made are ones Deloitte believes to be most interesting to readers. Additional data is available. Please contact a Deloitte member firm professional in your region for further insights.

Strong security governance reporting vertical becomes less important when security is governed in a decentralized fashion.

Security issues of 2010

Security management

The economic downturn and the resulting increased risk environment have turned out to be a boon for the profile of the information security function. Its importance to the organization is reflected in a number of areas such as reporting relationships, mandates, budgets, convergence of information and technology risk functions and is driven by factors we will discuss later on in the study. The survey results show that, while there is still a long way to go, organizations are starting to sit up and take notice and recognize the importance of the information security function to the business.

Overall, 80% of organizations in the survey have an executive responsible for information security, the same percentage as last year. What's different this year is the reporting relationship.

While the most common reporting relationship for executives responsible for information security remains to the CIO, at 24%, the response to the same question last year was 33%. So although the role still reports into the IT function (and therefore continues to be viewed as technical), it is clear that there is a marked decrease in this reporting relationship over last year. The next most common reporting relationship for the CISO is to the CEO (11%), and 10% of the respondents indicate that CISOs in their organizations report to the Board of Directors. Overall, with a decrease in reporting to the CIO and a slight increase over last year in reporting both to the CEO and the CFO, the information security function appear to be moving in the right direction in the organization.

The most prevalent mandate of the CISO is information security governance at 85%. A very good sign is that that CISOs' focus continues to be on strategy and planning (75%) versus operations although there is a slight drop in strategy and planning this year over last year (80%). Overall, the services delivered by the CISO continue to be geared towards strategy and governance rather than operations.

Chart 1. Reporting relationship of executive responsible for information security

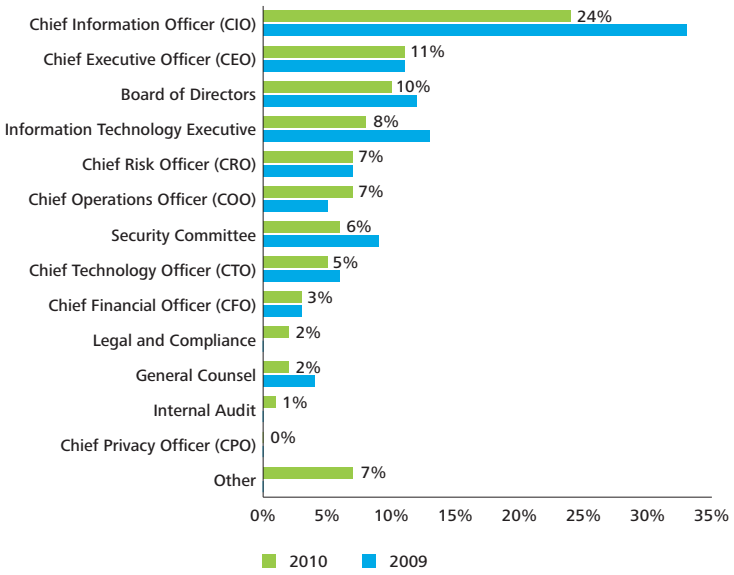


Chart 2. Functions within the scope of the executive responsible for information security

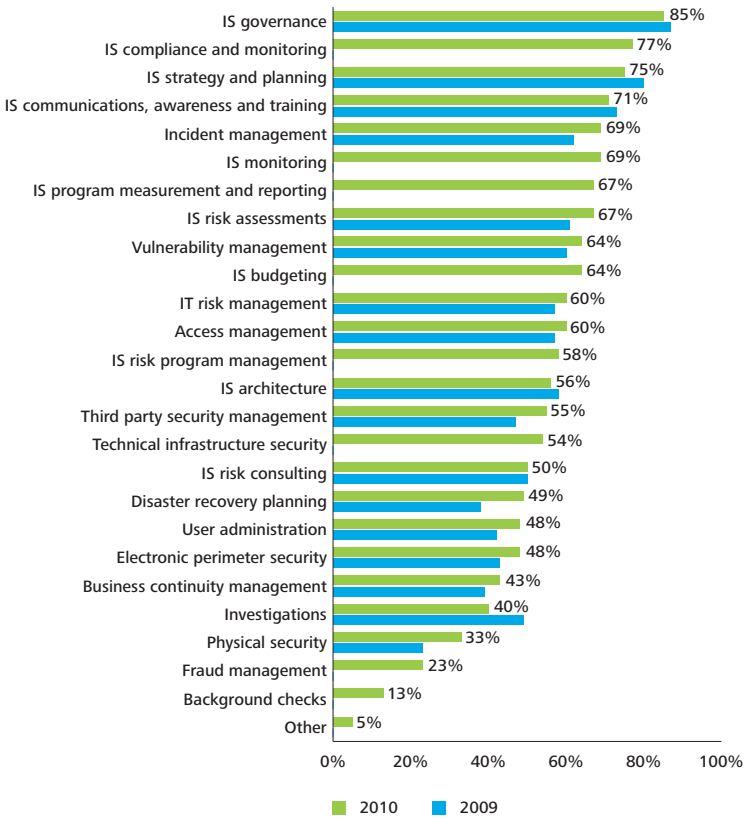


Chart 3. Assets included within the scope and mandate of the executive responsible for information security

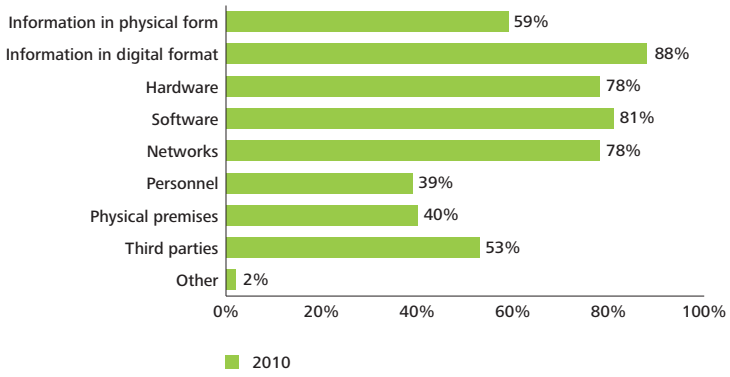
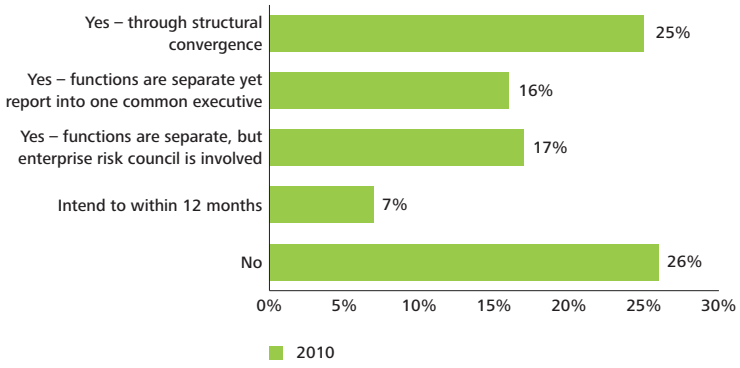


Chart 4. Organizations that have undergone a process of convergence of information and technology risk functions



A breakthrough was revealed in this year's survey. When respondents were asked to rank assets within the scope of the executive responsible for information security, it was no surprise that information in digital format was the primary responsibility, at 88%. And while physical assets, such as paper are still only at 59%, the breakthrough is that this is now indicated by more than half of respondents, a marked increase from 45% last year (the U.S. leads the pack this year with 70%). This is evidence not only of the expanding role of the CISO but also the move towards convergence between risk functions in the organization. However, there is clearly still a security gap around paper assets.

The new decade marks the first time that observers of the industry can truly say that convergence is happening. More than 58% of organizations have undergone some process towards convergence, whether through enterprise risk councils, structural convergence or with separate functions reporting to one common executive. Convergence of information and technology risk is highest in UK (75%) and in the U.S. (67%). Large organizations are more likely to experience convergence and small and medium-sized organizations have higher responses to no convergence: 31% and 25%, respectively.

Only 26% have not undergone any process towards convergence. Since having a total understanding of an organization's exposure to risk is so crucial these days and it is simply too expensive to have groups related to security working in silos, it appears that many organizations see convergence as a way to get a total security picture and save money in the process. Given the current threat environment and legislative requirements, convergence of risk functions may simply turn out to be the natural and logical state over time, like the globalization of the world.

As security functions mature and their mandates grow, there is evidence of convergence in a number of areas: the CISO's responsibility for physical security surging from 23% last year to 33% this year and physical assets such as paper increasingly part of the mandate of the CISO. However, one role that seems to maintain distance is that of the CRO. This link may become stronger in the coming years.

As in previous years, lack of sufficient budget is perceived as the primary barrier to ensuring information security.

But this year there is a difference. While 36% of respondents state this as a factor in 2010, that percentage has dropped considerably from last year (56%). It would appear that budgets are becoming less of a barrier as organizations recognize that they have to spend money to protect their information, evidenced by the increased interest in expensive projects such as IAM. The second most reported barrier is increasing sophistication of threats at 31% (last year 38%). For the first time, organizations appear eager to embrace emerging technologies to combat threats, previously avoided because of lack of maturity and expense. It may be an overstatement to say that information security budgets are recession-proof but they appear to be headed in that direction.

A documented and approved governance structure for information security is clearly not a barrier to ensuring information security. Only 7% of respondents do not have a documented and approved governance structure. The remainder either have one documented or approved (76%), intend to have one documented and approved in the next 12 months (11%) or have one documented but not approved (5%).

Chart 5. Major barriers faced in ensuring information security

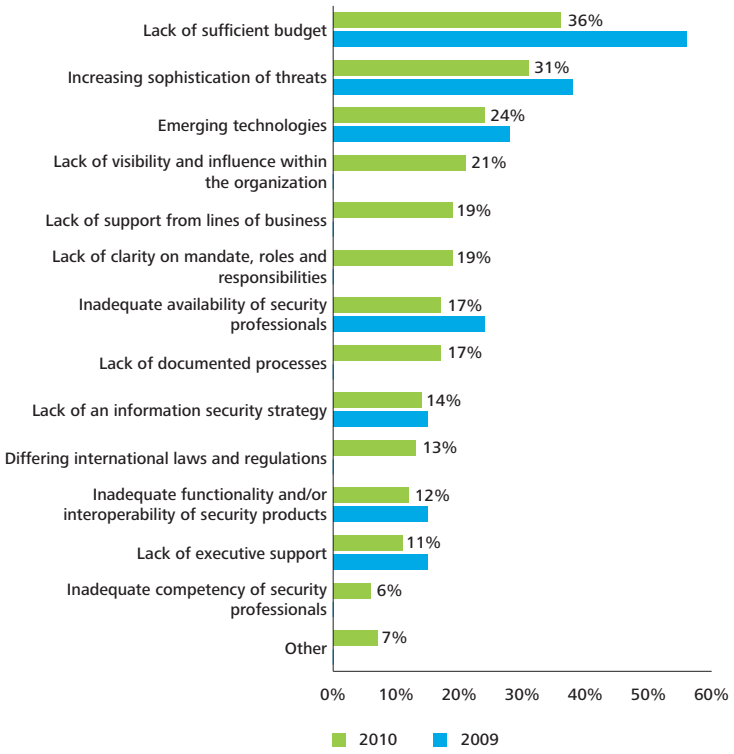


Chart 6. Existence of a documented and approved governance structure for information security

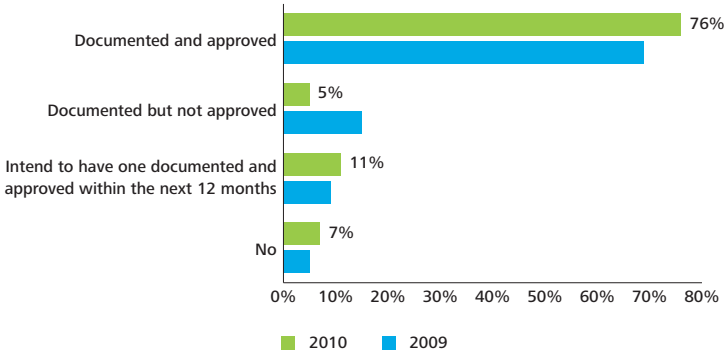
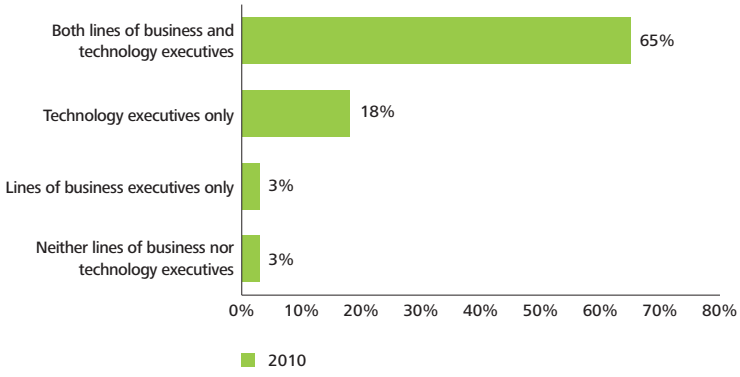


Chart 7. Frequency of reporting on the information security status of the organization to various groups

	Monthly	Quarterly	Semi-annually	Annually	Ad hoc	Never
Board of Directors	11%	18%	8%	18%	25%	9%
CEO	22%	18%	7%	11%	28%	5%
Senior and executive management	38%	23%	4%	5%	19%	2%

Chart 8. Who is engaged in identifying requirements for the information security strategy



A security strategy that starts out with input and buy-in from the lines of business means that, ideally, information security projects will map back to the organization's strategic business objectives.

The purpose of reporting by the information security function should be primarily to capture the attention of the business. But this does not appear to be happening.

For the Board of Directors, the most common frequency of reporting is ad hoc at 25% and quarterly at 18%. For the CEO, the most common frequency is ad hoc at 28%, and monthly at 22%. For senior and executive management, the most common frequency is monthly at 38%, with ad hoc at 19%. For both the Board of Directors and the CEO, reporting is more ad hoc than scheduled. Even for senior and executive management, 19% of respondents say that their reporting is ad hoc.

Ideally, for reporting to provide the most visibility for the function it should be scheduled, frequent and demonstrate the relationship between information risk and business success, particularly to the Board and C-suite.

The slow but steady progress that is reflected in responses to questions related to security management demonstrate that the information security function is moving towards recognition as a strategic necessity.

Business alignment

Business alignment starts with the basics: a documented and approved information security strategy. A security strategy that starts out with input and buy-in from the lines of business means that, ideally, information security projects will map back to the organization's strategic business objectives. But sticking to this takes determination, consistency and focus on the part of the CISO, who must make tough decisions about the kinds of investments that he or she is willing to support.

More than a half of respondents (60%) have a documented and approved security strategy. But when asked if they engage both lines of business and technology executives in identifying requirements for the strategy, only 65% of respondents state that they do.

If respondents consult only one group with regard to the security strategy, it is far more likely to be technology executives (18%) than lines of business executives (3%). Without the right level of involvement from the lines of business, security goals cannot be aligned with those of the business.

When asked how their organization's information security model is structured, respondents indicate that the most prevalent is centralized (76%).

A centralized security function is an effective means of enforcing security and protecting the organization at all levels, so the growth of centralized security model adoption may be a welcome change. However, being the sole source of security guidelines may also encourage security executives to limit the amount of feedback they collect from the lines of business. As a result, security function effectiveness may suffer due to lack of visibility and lack of alignment with business units' priorities and goals; this will also negatively affect the security function's ability to secure funding for critical projects. Even with a centralized security model, the leading practice is to have security resources embedded into or attached to the lines of business and geographic units to translate their requirements back to information security leadership.

Although it was mentioned previously that fewer respondents state that budgets are a barrier this year (36%) versus last year (56%), projects that adhere to the strategy approved by the lines of business (i.e., those that support the strategic business objectives) are far more likely to receive funding than those that do not appear to further business objectives.

It was stated earlier that more than half of respondents have a security strategy. But establishing strategic objectives, while an important step, is only part of the exercise. Performance against those objectives must be measured and the results used to demonstrate how well the function is doing in pursuing the strategy.

But only 19% of respondents state that they have established metrics aligned to business value and report on them on a scheduled basis; 33% are working on establishing metrics and aligning them to business value. However, nearly 20% either have no measurement or very little and another 21% have established metrics that are technical but not well understood by functions outside information security and IT (which may as well be no measurement in terms of visibility in the organization). In the absence of clear metrics that can be understood by the lines of business, the security function cannot demonstrate its value and consequently, its visibility suffers.

Chart 9. Information security model structure

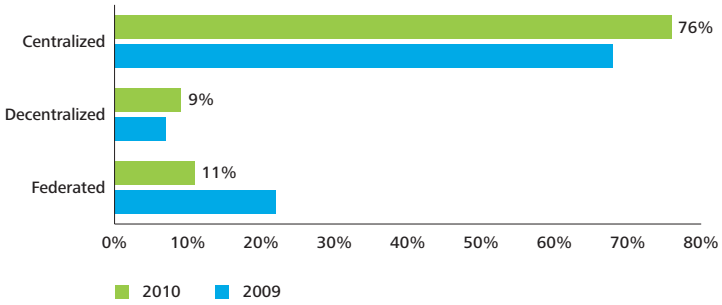


Chart 10. Measuring and demonstrating the value and effectiveness of the information security function's activities

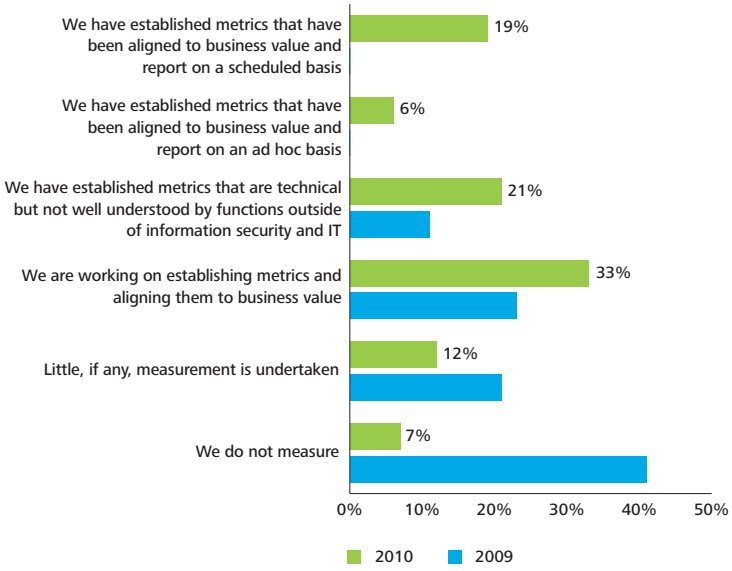


Chart 11. Effectiveness of information security function at meeting the needs and expectations of the organization

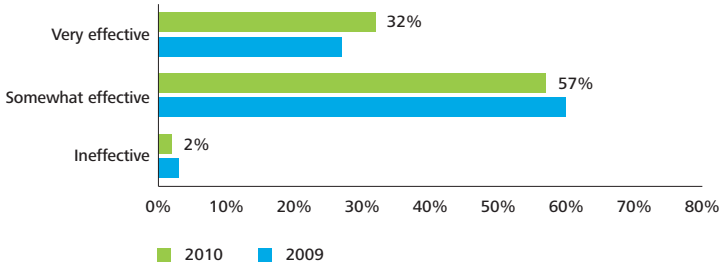


Chart 12. Extent to which business and information security initiatives are aligned with each other

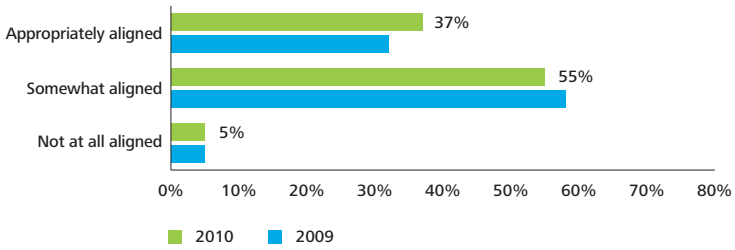


Chart 13. Year-over-year trending in the information security budget

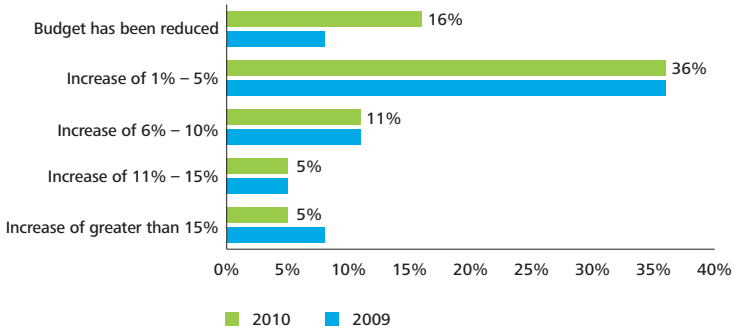
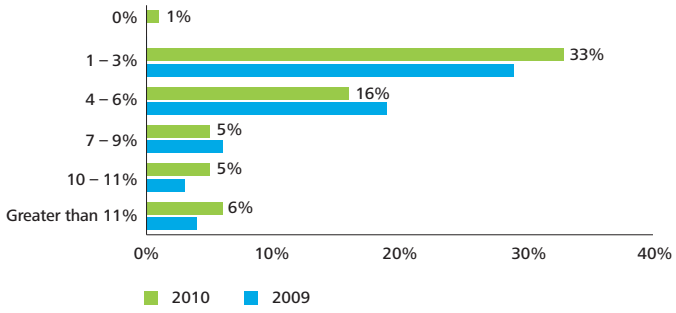


Chart 14. Percentage of organization's overall IT budget dedicated to information security



* A Tale of Two Cities, Charles Dickens, English Novelist (1812-1870)

When respondents were asked to rate feedback from the lines of business and other internal sources as to how effective the information security function is at meeting the needs and expectations of the organization, the majority responded "somewhat effective", 57%, approximately the same percentage as last year. Only 32% could state "very effective".

When asked how their organization's business and information security initiatives align with each other, the majority of respondents (55%) indicate "somewhat aligned". Only 37% state that they are "appropriately aligned".

This gets back to one of the greatest challenges facing the information security function: demonstrating value to the business. The business is on the front lines, acting with competitive urgency. The information security function needs to demonstrate that it is aligned with the needs of the business, not sheltered from the marketplace doing its own thing.

Security budgets/economy

A quote from Charles Dickens might best describe security budgets and the economy: "It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness…"* Despite the worst economy in decades and a lot of budgets being reduced in all areas, the information security function appears to be flying under the cost cutters' radar, a fact that may speak to a new regard for the value of the function.

Only 16% of respondents state that their information security budgets have been reduced while 36% indicate an increase of between 1% to 5%. While this is not a large increase, it is still an increase in a time when most budgets are being cut.

When asked what percentage of their organization's overall IT budget is dedicated to information security, 33% indicated 1%-3%.

When asked how they would characterize their organization's expenditures on information security, the greatest percentage of respondents state that they are on plan (41%), a slight increase over last year. "Catching up" was indicated by 32% of respondents.

When asked whether information security professionals have the required competencies to handle existing and foreseeable security requirements, 45% of respondents indicate that they do; 24% of respondents indicate that their staff is missing some competencies but adequately closing the gap through training and development.

That means that nearly 70% of respondents feel that their security requirements can be handled in-house. However, when asked about their major expenditures covered under the information security budget, respondents indicate that software, hardware and consultants/contractors are their greatest expenditures (66%, 62% and 61%, respectively).

One might wonder, since most respondents say their people are skilled enough, why contractors would be a major expense, not to mention the level of risk that they might add. But it is possible to have a full complement of required competencies, especially for day-to-day security operations and still use consultants for specific projects.

The information security function needs to demonstrate that it is aligned with the needs of the business, not sheltered from the marketplace, doing its own thing.

Chart 15. State of expenditures on information security

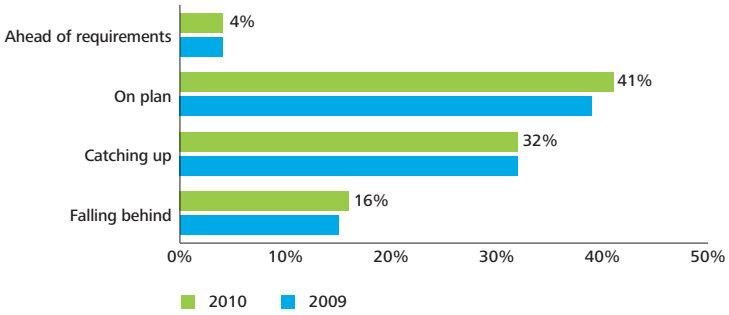


Chart 16. Required competencies to handle existing and foreseeable security requirements

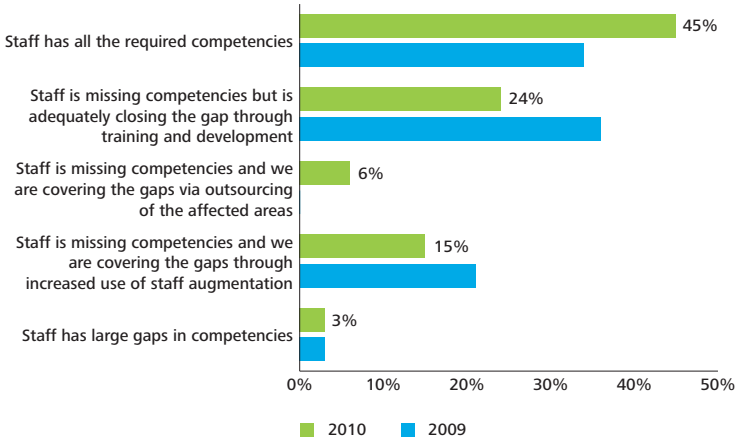
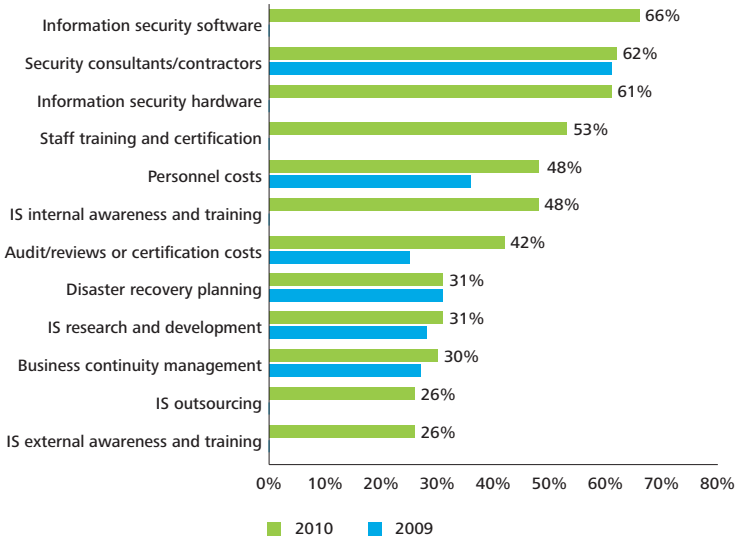


Chart 17. What is covered under the information security budget



Threat landscape/cybersecurity

In 2010, the threat landscape is more dangerous and more threatening than it has ever been before. For the most part, the children are gone and the big guns (government, organized crime) are in. The battle for your information is now high-stakes cyber warfare played out in every corner of the world. The threat lexicon continues to build at a dizzying rate: botnets, zombies, malicious PDFs, targeted attacks, hacking groups, spear phishing … the list continues. In his speech on May 29, 2009, U.S. President Barack Obama estimated annual world-wide loss from intellectual property theft by cyber criminals alone at $1 trillion.*

As in previous years, people are the organization's greatest worry – the ultimate "can't live with them, can't live without them" scenario.

Chart 18. Confidence that your organization's information assets are protected from internal and external attacks

	Extremely confident	Very confident	Somewhat confident	Not very confident	Not confident at all
Attacks originating internally	5%	34%	42%	16%	2%
Attacks originating externally	15%	56%	25%	3%	1%

When asked to rate their level of confidence that their organization's assets are protected from an attack, the greatest number of respondents (42%) indicate that they are only "somewhat confident" they are protected against internal attacks versus 25% who are "somewhat confident" they are protected against external attacks. Only 34% said they were "very confident" about being protected against internal attacks versus 56% who said they were "very confident" about being protected against external attacks. And this loss of confidence in internal people is a trend; almost 50% in last year's survey indicated that they were only "somewhat confident". Some new scams have appeared on the horizon described by a pair of similar words that have entered the security lexicon: cyber mules and cyber moles. Cyber mules (or money mules) unwittingly carry out illegal acts for hackers.

As an example, a recent story describes how consumers are lured into fake working-at-home scams that require them to receive money transfers and then forward the funds to Eastern Europe, either directly or through other cyber mules.* Cyber moles are internal individuals who steal corporate data. In other words, the illegal actions of cyber mules are inadvertent; the illegal actions of cyber moles are deliberate.

Despite the external environment, and as concerned as organizations are about it, human failings – carelessness, laziness, forgetfulness, fatigue, etc. – are more of a concern. It seems that organizations recognize that, despite the occasional disgruntled or malicious employee or third party, generally, their people are not "out to get them", they are just human. When asked to rate threats, respondents indicate that their highest threats are "non-intentional loss of sensitive information" and "increasing sophistication and proliferation of threats", both at 42%.

Financial institutions are now fighting on both fronts: externally and internally. As the external landscape gets more dangerous and threats get more ingenious and harder to detect, organizations worry more about their employee's inadvertent behaviour. And as individuals communicate and transact with each other more over the internet through emails, instant messaging, internet purchases, etc. there is a greater and greater potential for information to fall into the wrong hands. Deloitte member firms are receiving multiple requests for information on leading practices in content filtering, use of social media, data leakage protection – organizations world-wide are definitely concerned, and are taking steps towards protecting their valuable assets.

But in many cases organizations themselves are the enablers of mistakes on the part of their own people. Excessive access rights was the top internal/external audit finding at 38%. Employees routinely have access to more information and applications than they need to do their job. If an employee is dismissed on Friday, he or she may have access to the organization's information until Monday, when the IT group gets the directive from Human Resources to remove that person's access privileges. A contractor may fulfill a contract within the organization but that person's access rights may linger long after the contract is completed. Organizations tend to be overly generous with access rights so as not to impact employee productivity. But any productivity gains may pale in comparison to the negative consequences of a security breach. The issue of excessive access rights represents a huge gap in the information security for most organizations.

* downloaded from http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/on March 27, 2010

** downloaded from http://voices.washingtonpost.com/securityfix/2009/11/fdic_uptick_in_money_mule_scam.htm downloaded on March 27, 2010

In 2009, it was estimated that there were 30,000 new malware programs detected per day.* Malware is becoming much harder to detect and malware automation is likely to make attacks more frequent. Botnets are considered to be the major security threat on the internet. A botnet is a group of infected machines (also called zombies) that are controlled by the owner or the software source, called the "botmaster". Once the malicious software has been installed in a computer it becomes a zombie, and is totally controlled by the commands of the botmaster. Botnets can bring down servers, infect millions of computers with spyware and other malicious code, be used as agents for identity theft, steal company secrets, send out of spam, and engage in click fraud, blackmail, and extortion. In a recent Fortune 500 attack, criminals placed custom coded malware, that had specific IP address targets, hardcoded and hid the code using "near normal" appearing system file names, dates, and sizes. And botnets aside, attacks against social networking sites were a growing trend last year, as were attacks via peer-to-peer networks. Understandably, IAM and data protection are top security initiatives for 2010 and data loss prevention is the technology that most organizations plan to deploy in the next 12 months.

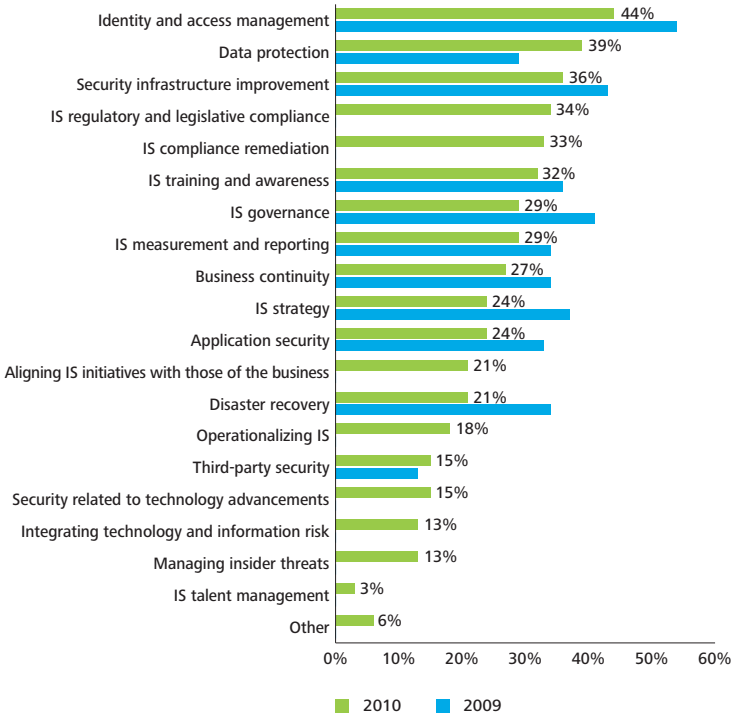
Training is obviously not effective if intent is malicious but it does change behaviour when loss is non-intentional, which is what organizations are most concerned about. Our survey shows that training and awareness are on the rise, especially when combined with enforcement and consequences. Training and awareness in such a context are very effective at changing behaviour and attitudes – one only has to look at the progress of recycling programs in North America, so successful so quickly that some cities experienced sharp budget shortfalls due to a decline in refuse revenues.

Data protection is a top security initiative with information security awareness and training rounding out the top six.

Chart 19. Threat perception

	Low	Medium	High
Increasing sophistication and proliferation of threats	9%	46%	42%
Non-intentional loss of sensitive information	14%	40%	42%
Phishing, pharming and other related variants	14%	49%	35%
Employee abuse of IT systems and information	16%	48%	33%
External financial fraud involving information systems	27%	38%	33%
Exploits of vulnerabilities in emerging technologies	20%	44%	32%
Attacks exploiting vulnerabilities of end point devices	18%	47%	32%
Attacks exploiting vulnerabilities due to unsecured code	19%	47%	31%
Social engineering	18%	49%	30%
Employee errors and omissions	11%	56%	30%
Security breaches involving third party organizations	21%	49%	27%
Zombie networks	22%	49%	25%
Attacks exploiting vulnerabilities due to unsecured code	27%	48%	22%
Differing cultural interpretations of security positive behavior	26%	49%	22%
Insider and rogue trading	28%	52%	15%
State or industrial espionage	55%	33%	10%

Chart 20. Top security initiatives



* Downloaded from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1420681,00.html on March 14, 2010

Chart 21. Training for employees to identify and report suspicious activities

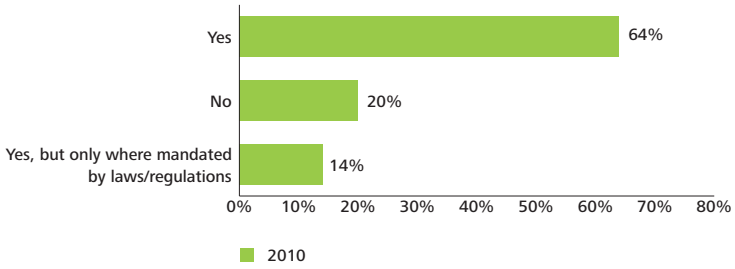


Chart 22. Customized IS training by job role and function

Customized training provided	Yes	No
Executives	32%	58%
People handling sensitive information	48%	45%
IT application developers and programmers	54%	38%
Systems administrators	56%	36%
Third party contractors	21%	60%

Chart 23. External breaches experienced in the last 12 months

	One occurrence	Repeated occurrences
Malicious software originating from outside the organization	14%	20%
Loss of information originating from a physical attack outside the organization	10%	10%
External financial fraud involving information systems	5%	9%
Breach of information originating from outside organization	7%	4%
Breach of information originating from a third party vendor	6%	4%
Theft of information resulting from state or industrial espionage	2%	1%
Website defacement	4%	1%
Mobile network breach originating from outside the organization	1%	1%
Other form of external breach	5%	4%

When asked if their organizations provide training to employees to identify and report suspicious activities, 64% responded that they did. Respondents are also focused on targeted training.

IT application developers and programmers are most likely to receive targeted training (54%) followed by people handling sensitive information (48%). Least likely to receive targeted training are executives at 32%.

When asked about external breaches experienced in the past 12 months, respondents cite repeated occurrences of "malicious software originating outside the organization" most often (20%).

Training and awareness are very effective at changing behaviour and attitudes – one only has to look at the progress of recycling programs in North America, so successful so quickly that some cities experienced sharp budget shortfalls due to a decline in refuse revenues.

Despite the ominous and dangerous external landscape, organizations that have sustained a breach report that losses are minimal.

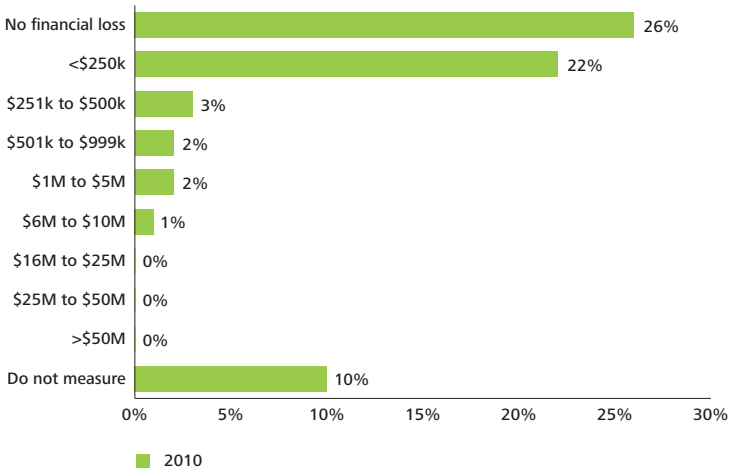
However, while 26% of respondents report no financial loss and 22% report a loss of $250,000 or less, the largest number of respondents (34%) chose the category "Not applicable/do not know". Organizations may simply not know what they don't know: only 54% maintain a loss event database and, of those respondents who answered the question about a loss event database, 41% comprise the two categories "do not have" or "not applicable/do not know."

The U.S. Identity Theft Research Center's 2007 Data Breach Statistics indicated that well over 127,000,000 records were exposed in 446 data breach incidents in 2007, and the Open Security Foundation reported that well over 83 million more were compromised in 2008.* When asked which attributes were included to determine the monetary damages suffered as a result of breaches in the last 12 months, 15% of respondents chose "internal investigation and forensic costs".

Chart 24. Internal breaches experienced in the last 12 months

	One occurrence	Repeated occurrences
Accidental breach of information originating from inside the organization	8%	11%
Malicious software originating from inside the organization	9%	10%
Breach of information originating from inside the organization conducted by an employee	11%	8%
Internal financial fraud involving information systems	7%	4%
Breach of information originating from inside the organization conducted by a non-employee	3%	2%
Breach of information originating from a third party vendor	3%	2%
Mobile network breach originating from inside the organization	1%	1%
Insider and rogue trading	2%	0%
Other form of internal breach	3%	3%

Chart 25. Estimated total monetary damages resulting from breaches over the last 12 months



* Downloaded from https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&srctype=smi&srcid=3B15&doctype=cite&docid=4+ISJLP+661&key=e6edb7eff741987c9ffcd1c5499c79d4 on March 14, 2010

Chart 26. Attributes included in the calculation to determine monetary damages as a result of breaches in the last 12 months

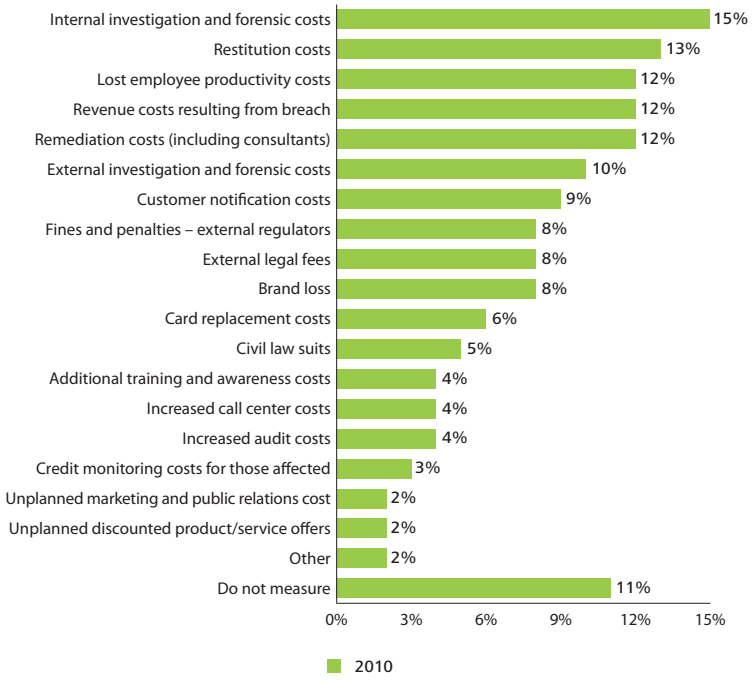


Chart 27. Frequency with which organization conducts specific testing or review

	Quarterly	Semi-annually	Annually	Adhoc	Never
Vulnerability scanning	40%	12%	14%	23%	6%
Internal penetration testing	15%	11%	21%	28%	19%
External penetration testing	16%	13%	31%	21%	14%
Penetration testing conducted by third party	13%	12%	38%	22%	10%
Application security code review	6%	3%	9%	46%	23%

Chart 28. Top security initiatives by sector

Global	Banking institutions, insurance companies	Investment	Payments & processors
Identity and access management	Identity and access management	Informantion security governance	Informantion security compliance remediation
Data protection	Data protection	Identity and access management	Data protection
Security infrastructure improvement	Security infrastructure improvement	Data protection	Business continuity

When asked how often their organizations conduct testing or review, the top response was vulnerability scanning conducted on a quarterly basis (40%). Penetration testing conducted by a third party annually was the next most popular response (38%).

However, responses to this question revealed a gaping security hole: 46% of respondents state that their application security code review is conducted only on an ad hoc basis. If the frequency is ad hoc the processes are likely to be informal or inconsistent. Since applications are not ignored by the hackers they should not be ignored by the organization.

Identity and Access Management (IAM)

Respondents indicate that identity and access management and data protection are their top two security initiatives for 2010.

The two go hand in hand: with strong IAM, data protection is more assured because the organization's people, without excessive access to information they do not need to do their jobs, are less likely to cause the "non-intentional loss of sensitive information" which organizations state is one of their greatest threats. Excessive access rights was the top internal/external audit finding this year and last year as well. Data loss prevention technologies were cited as the top technologies that organizations plan to fully deploy or pilot within the next 12 months.

The truth is that completely eliminating excessive access rights is almost impossible. However, that is no excuse not to have reasonable targets. Allowing an employee who leaves the organization to have access to the network two weeks later is not reasonable. Nor is allowing a junior Human Resources assistant to have access to payroll information about employees, including executives. But setting reasonable targets and sticking to them is difficult because the workforce is not static. Employees are hired, promoted (sometimes doing both jobs for a period of time) and fired; job requirements change; contractors come and go; off-site consultants (often in an unsecure environment) need access to documents and applications; mergers and acquisitions mean restructuring. The financial services industry is particularly hard hit: banks have failed and merged resulting in thousands of employees being laid off and those left behind taking on more work and heightened levels of stress. It's a lot to keep up with.

But IAM solutions are costly, particularly so for small and medium-sized organizations. "Lack of sufficient budget" is chosen by respondents as the top barrier to ensuring information security. But as long as the information security function does not learn how to sell itself, it will be difficult for it to get the budgets it needs. IAM is primarily a line of business project. But when asked how many actively involve both lines of business and IT decision makers in identifying requirements for the security strategy, only 65% do so.

When asked how effective the information security function is at meeting the needs and expectations of the organization based on feedback from the lines of business, only 32% of respondents state "very effective" with the greatest percentage, 57%, stating "somewhat effective". The word "somewhat" can cover a multitude of ills and that category likely includes some for whom the next choice, "ineffective", is simply too difficult to admit.

In addition, when respondents are asked to what extent business and information security are aligned with each other, only 37% state that they are "appropriately aligned". In order for projects such as IAM to get approved and underway, the lines of business need to have a vested interest in them.

Many financial institutions, particularly banks, continue to use user name and password for customers' authentication or password and "secret question", both of which are now considered weak.

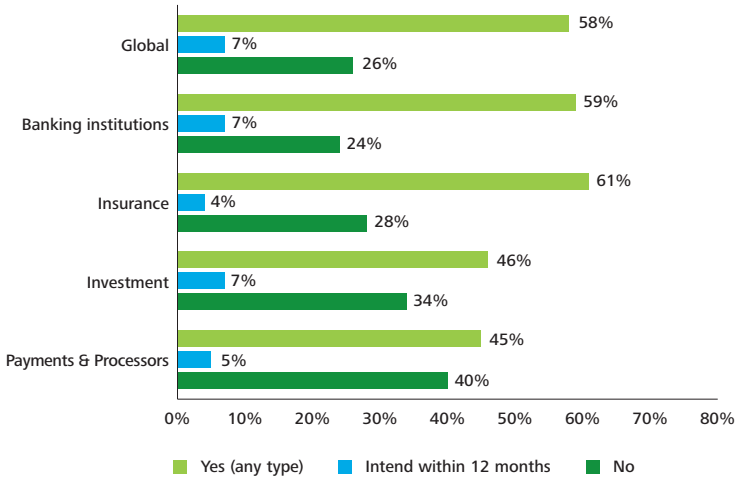
Chart 29. Top audit findings by sector

Global	Banking institutions	Insurance	Investment	Payments & processors
Excessive access rights	Excessive access rights	Excessive access rights	Excessive access rights	Lack of sufficient segregation of duties
Excessive developers' access to production systems and data	Lack of sufficient segregation of duties	Excessive developers' access to production systems and data	Lack of sufficient segregation of duties	Audit trails/logging issues
Lack of sufficient segregation of duties	Audit trails/ logging issues	Lack of clean up of access rules following a transfer or termination	Excessive developers' access to production systems and data	Lack of clean up of access rules following a transfer or termination

More and more financial institutions are looking into 2-factor authentication, which requires not only the user name and password but also another method of authentication such as a smart card in the user's possession or something unique to the user, such as a fingerprint. For those organizations who have customer-facing applications, the fine line they need to tread is how to convert to stronger authentication without inconveniencing and turning customers off. Since IAM is complex and expensive, there are those who suggest that the future of IAM might be in SaaS (Software as a Service) delivery, essentially outsourcing to save money (like computing power through mainframes in the 70s and 80s). However, while outsourcing might relieve the organization of responsibility for IAM, it does not relieve the organization of the duty to protect its data and stay compliant. Trying to comply with audits conducted off-site could add a whole new dimension of difficulty.

What is interesting is that respondents state that emerging technologies are the third most identified barrier to information security, after lack of sufficient budget and increasing sophistication of threats. However, when asked to identify their organization's top five security initiatives, respondents rank "security related to technology advancement" a low 14%.

Chart 30. Sector convergence



The world has changed and the stakes are higher in 2010. Organizations now need a holistic security solution capable of 360 degrees of protection.

Convergence

The question about convergence in this year's survey differs from those of previous years. In 2009, respondents were asked about the convergence of physical and logical security. This year, respondents were asked about convergence between functions mandated with technology risk and information risk responsibilities.

The question of convergence was introduced into the survey in 2006. Back then, the idea of convergence did not resonate with a lot of people. That may have been primarily because convergence was misunderstood. Many people saw it simply as putting together physical and logical technologies but could not understand how that was going to help productivity or business gains. In addition, convergence was considered an all or nothing undertaking: you either converged completely or you didn't at all. There was nothing in between.

But that was back when threats were perpetrated by teenagers and organizations were confident that they could handle what was out there. The world has changed and the stakes are higher in 2010. Organizations now need a holistic security solution capable of 360 degrees of protection. Security threats need to be addressed in tandem. People understand convergence better now. They understand that when it comes to security, the silo approach cannot be a good thing because that means that one group doesn't know what the other is doing or how things are going.

When asked if they had undergone a process of convergence ("Has your organization undergone a process of convergence between functions mandated with Technology Risk and Information Risk responsibilities?"), 58% of respondents indicated that they have, either through enterprise risk councils, through having separate functions report into one common executive or through structural convergence. Only 26% have not undergone a process towards convergence. Clearly, the responses to this question are very much dependent upon the size of the organization; this is an issue that is not likely to be relevant to an organization of 1000 people or less and the same would apply to many of the medium sized organizations as well.

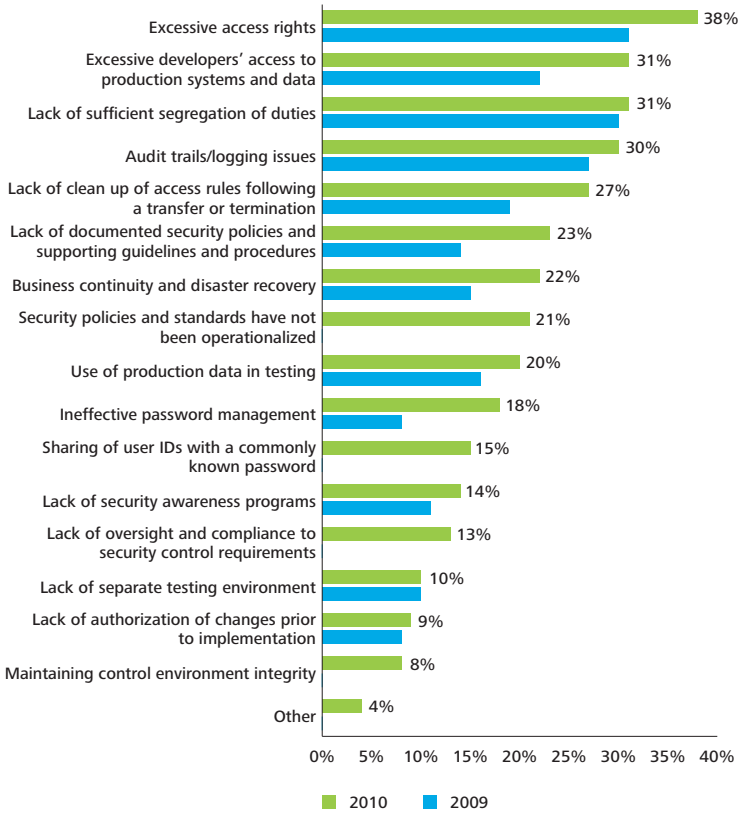
Data protection

Data makes the world go round. The most valuable asset of any organization, after its people, is its data. Data loss prevention is the hottest topic in 2010. Data loss prevention technology is the number one security technology that organizations plan to fully deploy or pilot within the next 12 months. All of respondents' top internal/external audit findings have to do with protecting data: excessive access rights, lack of sufficient segregation of duties, excessive developers' access to production, and audit trails/logging issues. And these findings are similar to last year's.

Respondents indicate that their organizations' security initiatives for 2010 are aligned with these issues (a finding that was not always the case in previous years' surveys): IAM (44%); data protection (39%); security infrastructure improvement (36%); information security regulatory and legislative compliance (34%) and information security compliance (internal/external audit) remediation (33%). Just outside the top five is information security training and awareness (32%) (see chart 20). The number five initiative, internal and external audit remediation, which has never been cited as a top five priority in previous surveys, demonstrates that financial organizations are gearing up for increased regulation and legislative compliance.

Organizations are recognizing that awareness and training programs can be very effective. There is evidence in many aspects of daily life that awareness and training change attitudes: smoking, littering, recycling, etc. Where organizations might have considered training and awareness too "fluffy" in the past, they are now recognizing that, since their workforce is subject to human failings, a combination of effective controls and training and awareness programs can go a long way toward protecting data. Most organizations (64%) train their employees to identify and report suspicious activities. There is also an interest in targeted training, particularly for IT application developers, system administrators and people handling sensitive information.

Chart 31. Top internal/external audit findings



Organizations are recognizing that awareness and training programs can be very effective.

Chart 32. Confidence in the information security practices of third parties

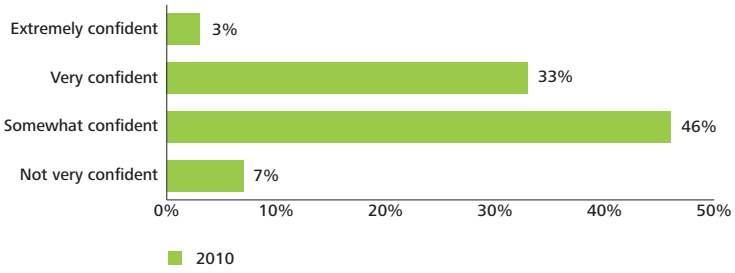
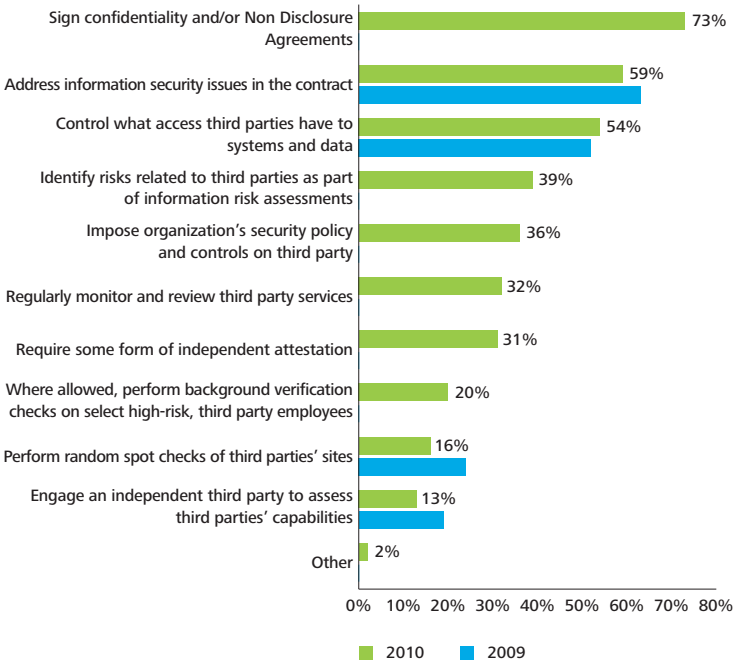


Chart 33. Ensuring the security practices of third parties



Given the risk landscape and the increasing sophistication of threats, organizations are no longer content to adopt only when the mainstream does.

Third parties are still an issue when it comes to data protection, as they have been in previous years.

Third parties are least likely to receive information security training (21% compared to 56% for system administrators), perhaps because they are typically removed from the organization and therefore out of sight and out of mind. But there is still insufficient attention paid to the security practices of third parties.

Despite their best intentions and their vested interest in being as accommodating as possible to their host organization, third parties are just as vulnerable to the same "non-intentional data loss". When asked how confident they are in the in the information security practices of their third parties, the majority of respondents (46%) indicate that they are "somewhat confident" while 33% indicate that they are "very confident". Altogether, 82% of respondents have some level of confidence in the security of their third parties. Perhaps organizations perceive that if third parties want to continue to be in business they will ensure that their security practices are above reproach. The most effective means to ensure that the level of security of third parties is aligned to your own organization is through a combination of explicit terms, conditions and expectations, as well as continuous audits, examinations and assessments. Only 7% of respondents are not "very confident" about their third parties which begs the question as to why these people are allowed to continue as third parties.

When asked how organizations ensure the security practices of their third parties, respondents state that they address information security requirements in a contract with third parties (59%) and control what access third parties have to their systems (54%).

A single control is not enough; rather, a series of controls must be in place. To ensure the security practices of their third parties, organizations must apply due diligence during and after selection process:

- review third parties' security policies and controls;
- regularly monitor and review their third parties' services;
- require some form of independent assessment;
- where allowed, perform background verification checks on select high-risk, third party employees; and
- perform random spot checks of third parties' sites.

Emerging technologies

One of the most exciting trends uncovered by the survey is in the area of emerging technologies. Emerging technologies bring new opportunities but greater risks as well. But organizations now seem willing to take more risks to be able to capitalize on opportunities.

For the first time in the history of the survey, "early majority" was chosen by the greatest number of respondents (nearly 40%). Early majority adopters are not willing to take the same risks as innovators or early adopters, but, while thoughtful in deployment, they adopt faster than the mainstream (late majority). This indicates a major breakthrough in the thinking of financial institutions as they move from reactive towards proactive. Given the risk landscape and the increasing sophistication of threats, organizations are no longer content to adopt only when the mainstream does. While this may not be true in other industries, financial institutions have to take this stance for survival – because they have the money, they are more likely to be targets. Even the "early adopters" category (thought leaders who try out new technologies carefully, having learned from the innovators) shows an increase this year (20%) over last year (15%).

Chart 34. Organization's adoption of security technology

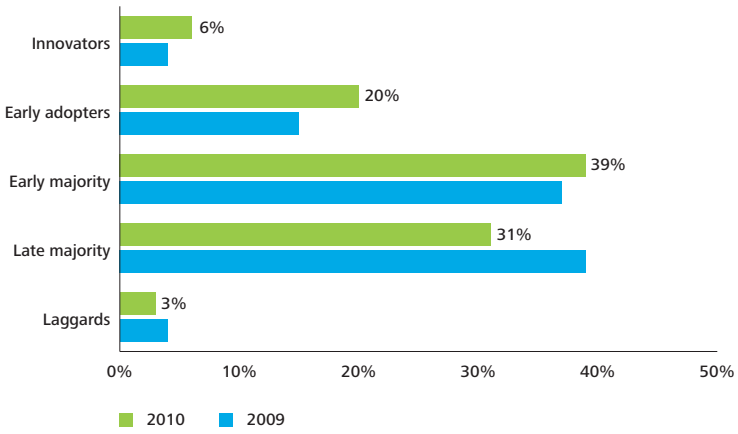


Chart 35. Types of technologies deployed, piloted or planned

	Full	Pilot	Plan
Data loss prevention technology	32%	17%	26%
Federated identity management	16%	11%	21%
Encrypted storage devices	33%	17%	20%
Enterprise Single Sign On	21%	14%	19%
File encryption for mobile devices	44%	13%	18%
Network access control	43%	13%	18%
Security compliance tools	30%	13%	18%
Email encryption	38%	17%	18%
Biometric technologies for user authentication	13%	7%	18%
Security log and event management systems	50%	19%	17%
Data at rest security/encryption	32%	14%	15%
Incident management workflow tools	38%	13%	13%
Email authentication	39%	13%	12%
Network behavior analysis	38%	15%	12%
Web access management systems	44%	10%	12%
Wireless security solutions	34%	11%	11%
Web services security	39%	12%	11%
Vulnerability management	58%	12%	10%
Intrusion Detection and/or Prevention Systems (IDS/IPS)	78%	7%	7%
Anti phishing solutions	63%	8%	5%
Content filtering/monitoring	82%	5%	4%
Anti spyware software	84%	4%	3%
Spam filtering solutions	93%	0%	1%
Antivirus	97%	1%	0%
Firewalls	97%	1%	0%

More than 70% of organizations indicate that they are planning to implement at least one new information security-related technology in the next 12 months; this is an exciting time for vendors, who have huge opportunities to demonstrate the effectiveness of their products in a receptive atmosphere. The greatest number of respondents indicates that data loss prevention is the technology that their organizations are planning to adopt.

Despite recent high-profile security breaches that have succeeded due, in part to, the absence of encryption, when it comes to the "fully deployed" category, only 38% of organizations have email encryption, only 33% have encrypted storage devices, only 44% have file encryption for mobile devices, and only 32% have data at rest security/encryption. There are major regional differences. U.K. respondents indicate 80% for file encryption of mobile devices, well above the global average. And the U.S. (67%) differs hugely from APAC (22%) when it comes to email encryption. In some areas, encryption is a relatively easy and very effective security measure and yet surprisingly under-utilized. For example, only 12% of respondents from LACRO indicate that they have "fully deployed" file encryption for mobile devices but only 26% indicate that it is "planned" or being "piloted" (34%).

Data at rest encryption appears to be a largely ignored area. Although many successful breaches have occurred by intercepting data in transit, the majority of information (e.g., medical records, insurance information, personal financial information, etc.) is data at rest. Only 32% of respondents have data at rest security/encryption fully deployed and the numbers are low for "piloting" (14%) or "planned" (15%).

Along with encryption technologies and security log and event management systems, data loss prevention technologies are those most likely to be piloted or planned. Federated identity management technologies are close behind as well as enterprise single sign on of technologies that are planned.

How DTT's GFSI Group designed, implemented and evaluated the survey

The 2010 Financial Services Industry Global Security Study reports on the outcome of focused discussions between Deloitte member firm Information & Technology Risk Services professionals and Information Technology executives of top global FSIs – a sub-set of participants from 7 industries, which were part of 2010 Global Security Study (financial services; consumer business; technology, media, and telecommunications; energy, resources & utilities; life sciences and healthcare; public sector; manufacturing).

Discussions with representatives of these organizations were designed to identify, record, and present the state of the practice of information security in the financial services industry with a particular emphasis on identifying levels of perceived risks, the types of risks with which FSIs are concerned, and the resources being used to mitigate these risks. The survey also identifies technologies that are being implemented to improve security and the value FSIs are gaining from their security and privacy investments.

To fulfill this objective, senior Deloitte member firm professionals designed a questionnaire that probed key aspects of strategic and operational areas of security and privacy across all industries and in financial services industry in particular. Responses of participants were subsequently analyzed and consolidated and are presented herein in both qualitative and quantitative formats.

Size and structure

The overall number of questions was reduced compared to previous year to reduce the burden on participants. However, new questions were also added to reflect topics being asked about by Deloitte member firm clients and raised by the media.

The 2010 Global Security Study questionnaire had 3 distinct parts: core part – which applied to all industries, industry part – targeted industry-specific questions, and business continuity management part – in-depth questions on business continuity and disaster recovery processes (previously, a separate survey – its results are not included in this publication).

Questions were selected based on their global suitability, added value, and for the financial industry part – also based on their potential to reflect the most important operating dimensions of a financial institution's processes or systems in relation to security and privacy.

The collection process

Once the questionnaire was finalized and agreed upon by the survey team, questionnaires were distributed to the participating regions electronically. Data collection involved gathering both quantitative and qualitative data related to the identified areas. Each participating region assigned responsibility to senior member firm professionals within their firms' Information & Technology Risk practices and those people obtained answers from various financial institutions with which they had a relationship.

Most of the data collection process took place through face-to-face interviews with the CISO/Chief Security Officer or designate, and in some instances, with the security management team. Deloitte member firm professionals also offered preselected financial institutions the ability to submit answers online using an online questionnaire managed by DeloitteDEX Advisory Services.

Data analysis and validation

Results of the survey have been analyzed according to industry leading practices and reviewed by senior members of Deloitte's Information & Technology Risk Services. Some basic measures of dispersion were calculated from the data sets. Some answers to specific questions were not used in calculations to keep the analysis simple and straightforward. Results in some charts may not total 100% as the study team was reporting selected information only; responses from those who decline to answer may not be included in the reported data.

Item# 100046

Designed and produced by The Creative Studio at Deloitte, London. 3434A

2009 Annual Study: Cost of a Data Breach

Understanding Financial Impact, Customer Turnover, and Preventive Solutions

Executive Summary:

This 2009 Ponemon Institute benchmark study, sponsored by PGP Corporation, examines the cost incurred by 45 organizations after experiencing a data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. This is the fifth annual survey of this issue.

Breaches included in the survey ranged from approximately 5,000 records to more than 101,000 records from 15 different industry sectors.

Benchmark research conducted by

Ponemon Institute, LLC

January 2010

Table of Contents

Executive Summary

PGP Corporation and Ponemon Institute are pleased to report the results of our fifth annual study concerning the cost of data breach incidents for U.S.-based companies. Ponemon Institute research indicates that data breaches continue to have serious financial consequences on organizations. This year's report, entitled *2009 U.S. Cost of a Data Breach Study*, found that for the first time, U.S. companies are spending more on technologies to prevent and remediate breaches.

First conducted over five years ago, our initial study established objective methods for quantifying specific activities that result in direct, indirect and opportunity costs from the loss or theft of personal information, thus requiring notification to breach victims as required by law. To maintain consistency from prior years, our methods for quantifying data breach costs has remained relatively constant.[1]

Our current analysis of the actual data breach experiences of 45 U.S. companies from 15 different industry sectors takes into account a wide range of business costs, including expense outlays for detection, escalation, notification, and after-the-fact (ex-post) response. We also analyze the economic impact of lost or diminished customer trust and confidence as measured by customer turnover, or churn, rates.

Utilizing activity-based costing, our methods capture information about direct expenses such as engaging forensic experts, outsourced hotline support, free credit monitoring subscriptions, and discounts for future products and services. We also capture indirect costs such as in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished acquisition rates.

The following are some of the top findings from the 2009 U.S. study:

- **U.S. organizations continue to experience an increased cost of data breaches,** which includes activities intended to prevent a loss of customer or consumer trust. This rise in expense occurs despite a decline in major media or press coverage of this topic. Overall cost is not declining despite the perception that data breaches are becoming a more mundane issue. This viewpoint may be tied to stabilizing costs of detection, escalation and notification as well as our first-ever observation of a decrease in lost business. The average organizational cost of a data breach increased nearly 2 percent, from to $6.65 million in our 2008 study to $6.75 million in 2009. The average cost per compromised record per breach rose only $2, from $202 to $204. The most expensive data breach event included in this year's study cost one organization nearly $31 million to resolve.

- **Although most U.S. companies still prefer manual and policy solutions as post-breach remediation measures, for the first time, many companies are starting to use enabling prevention and remediation technologies more often and effectively.** While the findings suggest that remediation measures after breach incidents in all categories increased from 2008, most organizations aim to prevent future breaches through training and awareness programs (67 percent) and additional manual procedures and controls (58 percent). Automated IT security solutions that saw modest to marked increases in use included: expanded use of encryption (58 percent), identity and access management solutions (49 percent), data loss prevention solutions (42 percent), and endpoint security solutions (36 percent).

- **Data breaches from malicious attacks and botnets doubled from 2008 to 2009 and cost substantially more than those caused by human negligence or IT system glitches.** The incidence of malicious attacks rose from 12 percent to 24 percent. In addition, the 2009 cost per compromised record of data breaches involving a malicious or criminal act averaged $215, 40 percent higher than breaches involving a negligent insider ($154) and 30 percent higher than breaches from system glitches ($166). For the first time,

[1] Our 2006 study involved one very large (catastrophic) data breach that represented an outlier cost event. Hence, it was removed from the total for comparison purposes.

companies participating in the study reported that data-stealing malware caused their breaches. These findings suggest that organizations must start protecting themselves more proactively from increasingly aggressive malicious outsiders.

- **The leadership of a CISO or equivalent position substantially reduces the overall cost of data breaches.** Specifically, companies with a CISO (or equivalent title) who managed data breach incidents experienced an average cost per compromised record of $157, versus $236 – a whopping 50 percent increase – for companies without such leadership.

- **Companies that notify victims too quickly may fact incur higher costs.** About 36 percent of participating organizations notified victims within one month, but these "quick responders" ended up paying more than their slower peers ($219 versus $196, a 12 percent difference). Moving too quickly through the data breach process -- especially during the detection, escalation and notification phases -- may cause inefficiencies that raise total costs.

2009 Annual Study: Cost of a Data Breach

This 2009 Ponemon Institute benchmark study, sponsored by PGP Corporation, examines the costs incurred by 45 organizations after experiencing a data breach. Results were not hypothetical responses; they represent cost estimates for activities resulting from actual data loss incidents. This is the fifth annual survey of this issue.

Breaches included in the survey ranged from roughly 5,000 records to more than 101,000 records from 15 different industry sectors.

What we learned from the 2009 Results:

The total cost of a data breach rose slightly to $204 from $202 per compromised record. According to participants in the 2009 study, data breaches cost their companies an average of $204 per compromised record – of which $144 pertains to indirect cost including abnormal turnover or churn of existing and future customers.[2] Last year's average per victim cost was $202 with an average indirect cost at $152 per breach victim. This year direct costs rose to $60 from $50 in 2008.

The cost of lost business decreased slightly but ex-post response increased. In a dramatic reversal, ex-post response represented the largest increase in total cost. Last year, this cost category represented the largest decrease. One of the main reasons for an increase in ex-post response costs is due to the increase in legal defense cost mentioned above.

Once again, our research finds organizations in highly trusted industries such as financial services and healthcare are more likely to experience a data breach with high abnormal churn rates. In contrast, retailers and companies with less direct consumer contact seem to experience a lower overall data breach cost. Other cost components of a data breach appear to have stabilized.

Data breach continues to be a very costly event for organizations. The average organizational cost of a data breach increased from to $6.65 million in our 2008 study to $6.75 million in 2009. The most expensive data breach event included in this year's study cost a company nearly $31 million to resolve. The least expensive total cost of data breach for a company included in our study was $750,000. The magnitude of the breach event ranged from approximately 5,000 to approximately 101,000 lost or stolen records. As in prior years, data breach cost appears to be linearly related to the size or magnitude of the breach event.

[2] For purposes of comparability across different breach incidents, we measure data breach cost on a *per victim* compromised record, basis.

Abnormal churn or turnover of customers resulting directly from the data breach incident appears to the main driver for data breach cost. In this year's study, average abnormal churn rates across all 45 incidents is slightly higher than last year (from 3.6 percent in 2008 to 3.7 percent in 2009), which was measured by the loss of customers who were directly affected by the data breach event (i.e., typically those receiving notification). The industries with the highest churn rate are pharmaceuticals, communications and healthcare (all at 6 percent), followed by financial services and services (both at 5 percent). The industries with the lowest abnormal churn rates are manufacturing, energy and media (all at or below 1 percent), followed by technology and retail (both at 2 percent).

Forty-two percent of all cases in this year's study involved third-party mistakes or flubs. Data breaches involving outsourced data to third parties, especially when the third party is offshore, were most costly. This could be due to additional investigation and consulting fees. The cost per compromised record for data breaches involving third parties was $217 versus $194, more than a $21 difference.

Twenty-four percent of all cases in this year's study involved a malicious or criminal attack that resulted in the loss or theft of personal information. Our research shows data breaches involving malicious or criminal acts are much more expensive than incidents resulting from negligence. Accordingly, in 2009 the cost per compromised record of a data breach involving a malicious or criminal act averaged $215. In contrast, the cost per compromised record of a data breach involving a negligent insider or a systems glitch averaged $154 and $166, respectively.

Thirty-six percent of all cases in this year's study involved lost or stolen laptop computers or other mobile data-bearing devices. Data breaches concerning lost, missing or stolen laptop computers are more expensive than other incidents. Specifically, in this year's study the per victim cost for a data breach involving a lost or stolen laptop was $225.

More than 82 percent of all cases in this year's study involved organizations that had more than one data breach involving the loss or theft of more than 1,000 records containing personal information. Data breaches experienced by "first timers" are more expensive than those experienced by organizations that have had previous data breaches. The per victim cost for a first time data breach was $228 versus $198 for companies experiencing two or more incidents. This finding suggests companies that experience data breaches become more efficient at managing costs over time.

Training and awareness programs lead companies' efforts to prevent future breaches, according to 67 percent of respondents. Other notable remediation procedures following the breach incident include: additional manual procedures and controls (58 percent), expanded use of encryption (58 percent), identity and access management solutions (49 percent), data loss prevention solutions (42 percent), and endpoint security solutions (36 percent). The presented 2009 findings suggest that remediation measures after the breach incident in all categories increased from 2008.

In approximately 40 percent of participating companies, the CISO was in charge of managing the data breach incident. While other senior IT officials within an organization are typically involved in crisis management activities surrounding data breach response, our results suggest CISO leadership substantially reduces the overall cost of data breach. Specifically, companies that had a CISO (or equivalent title) who managed the data breach incident experienced an average cost per compromised record of $157, versus $236 for companies without CISO leadership.

About 36 percent of participating companies notified victims within one month of discovering the data breach (a.k.a. quick responders). Surprisingly, our findings suggest that companies that execute notification quickly experience a higher average cost per compromised record than companies that move more slowly ($219 versus $196). Our results suggest that moving too quickly through the data breach process may cause cost inefficiencies for the organization, especially during the detection, escalation and notification phases.

More than 42 percent of participating companies achieved a Security Effectiveness Score (SES) that was above the median value determined from benchmark results.[3] As expected, those organizations with a more favorable security posture (SES above the median) experienced a lower average cost per compromised record than organizations with an SES below the median. Accordingly, organizations with a favorable security posture had an average cost per compromised record of $202, versus $207 for those with an unfavorable security posture.

About 44 percent of participating companies engaged an outside consultant to assist them over the course of the data breach incident. Our findings suggest that engaging a consultant or other third-party expert to assist in the data breach incident results in a lower average cost per compromised record. Specifically, those organizations that engaged a consultant experienced, on average, a per victim cost of $170, as opposed to $231 for companies that decided to go it alone.

In conclusion, our 2009 research once again suggests that U.S. organizations by and large take their stewardship of sensitive personal data seriously and are taking greater steps to ensure its protection from breaches. Despite its limitations, the research reinforces best practices for IT security and privacy and arguments that those practices provide a positive return on investment. Our research also supports statements by leading industry and government experts who advocate proactive, automated data protection in addition to written policies, procedures and training.

Preventive Solutions

Especially given the rise in data-stealing malicious attacks, organizations should strongly consider a holistic approach to protecting data wherever it is – at rest, in motion and in use. While manual and policy approaches may come first to mind for many companies, those approaches by themselves are not as effective as a multi-pronged approach that includes automated IT security solutions.

Many kinds of automated, cost-effective enterprise data protection solutions are now available to secure data both within an organization and among business partners. Some of the most popular and effective of these technologies currently available include:

- Encryption (including whole disk encryption and for mobile devices/smartphones)
- Data loss prevention (DLP) solutions
- Identity and access management solutions
- Endpoint security solutions and other anti-malware tools

Companies should also look for centralized management of IT security solutions so they can automatically enforce IT security best practices throughout their organizations. Such capability also enables enterprises to align information protection with corporate security policies and regulatory or business-partner mandates.

[3] The SES is a methodology developed by Ponemon Institute and PGP Corporation in 2005 for its annual encryption trends study. The SES measures the effectiveness of an organization's security posture. Since its inception five years ago, this proprietary security scoring method has been used in more than 80 studies involving information security practitioners in organizations throughout the world.

Next Steps

This fifth annual report enables organizations to forecast in detail the specific actions and costs required to recover from a customer data security breach. This report can be used as a guideline to conduct an internal audit and to create breach response cost estimates. These estimates may then be compared with the technology and other costs of preventing data breaches.

Companies should also consider following industry best practices, including:

- Companies should ensure that portable data-bearing devices – such as laptops, smart phones and USB memory sticks – are encrypted, especially for people who travel extensively for business.
- Companies should establish an organizational structure that allows the CISO or other security/privacy leaders to take charge and ensure the detection and notification process is handled appropriately.
- When in doubt about requirements, companies should seek the counsel of consultants and legal experts to ensure the notification process complies with the plethora of state data breach notification laws, as well as related federal laws.
- To minimize customer churn (turnover), companies should draft communications that clearly define the issue and root cause of the breach incident. Whenever feasible, the company should take steps that minimize potential harm to data breach victims – for instance, the company may consider providing free identity protection services when the root cause of a breach is likely to be a theft or criminal attack.

Introduction

Government, industry and the American public in 2009 understood more than ever the damage that data breaches can do. High-profile data breaches continued to occur in both the public and private sectors. In December, the Transportation Security Administration, part of the U.S. Department of Homeland Security, accidentally published its passenger screening criteria online, embarrassing an already hard-hit agency and industry. Heartland Payment Systems, which processes 100 million transactions per month for more than 250,000 businesses, announced in January that malicious hackers may have compromised 130 million of its transactions, causing the potentially biggest data breach ever.

In response to longstanding industry and government concerns that cyberthreats – including data breaches – pose some of the greatest economic, homeland and national security challenges of the 21st century, the Obama Administration made improving cybersecurity, and particularly protection of the nation's cyberinfrastructure and sensitive data, a presidential priority. The White House ordered a 60-day federal cybersecurity review, which recommended urgent action and suggested that "increased liability for the consequences of poor security" might improve the situation – a recommendation that resonates with the findings in this report.

The White House also filled the long-vacant position of White House Cybersecurity Coordinator and created the first-ever federal CIO and CTO positions, long recommended by experts as essential to raising federal IT to an appropriate level of importance in the federal government.

Increased public and government attention to cybersecurity drove Congress to make progress on a national data breach notification law that would standardize data breach protections nationwide.

In February, the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the federal economic stimulus package, included the first federally mandated data breach notification requirements. It mandated periodic audits to ensure that covered entities and – for the first time – their business associates comply with security and privacy requirements or face civil and criminal penalties.

In November, the U.S. Senate Judiciary Committee approved two bills concerning data breach notification. The Personal Data Privacy and Security Act would set standards for protecting sensitive personally identifying information and impose civil penalties for those caught violating them. The second bill, the Data Breach Notification Act, would require entities engaged in interstate commerce to notify victims whose personal information is compromised in a breach — unless disclosure would harm national security or in some way hinder a law-enforcement investigation.

In December, the U.S. House of Representatives for the first time passed a data breach notification bill, the Data Accountability and Trust Act (DATA). The bill would require any organization experiencing a breach to notify the Federal Trade Commission and notify all affected U.S. individuals. Organizations would also have to designate an information security officer and establish data security policies for data collection and retention as well as finding and fixing system vulnerabilities. The bill includes a safe harbor provision for organizations that protect data with encryption.

Despite progress overall, some controversy remained. A data breach notification rule that the U.S. Department of Health and Human Services (HHS) implemented in September drew widespread criticism from both Congress and industry experts. The rule required healthcare entities to publicly disclose breaches only if they think the breach would do financial, reputational or other harm to victims – a position thought to encourage those entities not to report, and therefore suffer the consequences, of data breaches.

Lawmakers in at least 21 states introduced security breach legislation in 2009[4], and since 2004 45 states[5] have passed laws requiring organizations and government agencies to notify customers, employees, and other affected individuals when a breach of protected personal information occurs due to human error, technology problems, or malicious acts.

Although the specific conditions for notification vary by state, organizations may not be required to notify individuals when:

- The breached data is protected by at least 128-bit encryption
- The breached data elements are not considered "protected"
- The breach was stopped before information was wrongfully acquired
- Other special circumstances (such as national security or law enforcement investigations) exist

Responding to a data breach incident includes activities intended to prevent losing customers or consumer trust and help preserve an organization's reputation. But when organizations experience data breaches and must notify customers or clients, what costs do they encounter as they attempt to recover?

The Ponemon Institute and PGP Corporation are pleased to offer the fifth annual survey that quantifies the actual costs incurred by 45 organizations compelled to notify individuals of data privacy breaches. Summarized in this document, the study provides detailed information from responses to questions organizations face when responding to a data breach:

- What are the potential legal costs?
- What are industry-average costs resulting from a breach, including the detection, investigation, notification, and possible services offered to affected individuals?
- What are the costs of lost customers and brand damage?
- What are the key trends?
- What measures are taken following a breach that could have been implemented to avert it?

[4] National Conference of State Legislatures, Security Breach Legislation 2009: http://www.ncsl.org/default.aspx?tabid=18325

[5] National Conference of State Legislatures, State Security Breach Notification Laws as of December 9, 2009: http://www.ncsl.org/Default.aspx?TabId=13489

Study Overview & Methodology

The Ponemon Institute's annual benchmark study, begun in 2005, examines the costs organizations incur when responding to data breach incidents resulting in the loss or theft of protected personal information.

- To complete the study, benchmark surveys were sent to 126 organizations known to have experienced a breach involving the loss or theft of personal customer, consumer or student data during the past year.
- Of that group, 45 companies agreed to participate by completing the survey. Results were not hypothetical responses to possible situations; they represent cost estimates for activities resulting from an actual data loss incident.
- The reported number of individual records breached ranged from approximately 5,000 to more than 101,000 records from companies in 15 different industry sectors.
- The 2009 survey shows that 42% percent of breaches occurred due to external causes, a decrease from 44 percent in 2008. A third-party breach is defined as a case where a third party (such as professional services, outsourcers, vendors, business partners) was in the possession of the data and responsible for its protection. In comparison, an in-house breach is defined as a case where the protection of data was the responsibility of the organization itself (by an employee or for data on the corporate network, for example).

Table 1 summarizes the 45 study participants by industry and source of data breach:

Industry	Total	Internal Breaches	Third-Party Breaches
Communications	1	1	0
Consumer	3	2	1
Education	3	2	1
Energy	1	0	1
Financial	8	3	5
Healthcare	5	2	3
Hotel & Leisure	1	1	0
Manufacturing	1	1	0
Media	1	1	0
Pharmaceutical	1	0	1
Research	1	1	0
Retail	8	6	2
Services	5	2	3
Technology	4	2	2
Transportation	2	2	0
Totals	**45**	**26**	**19**

Table 1: Study participant sectors and data breach source

Study Methodology

Our study addresses core process-related activities that drive a range of expenditures associated with a company's data breach detection and response. The four cost centers are:

- Detection or discovery: Activities that enable a company to reasonably detect the breach of personal data either at risk in storage or in motion.
- Escalation: Activities necessary to report the breach of protected information to appropriate personnel within a specified time period.
- Notification: Activities that enable the company to notify data subjects with a letter, outbound telephone call, e-mail or general notice that personal information was lost or stolen.
- Ex-post response: Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations in order to minimize potential harm. Redress activities also include ex-post response such as credit report monitoring or the reissuing of a new account or credit card.

In addition to the above process-related activities, most companies experience opportunity costs associated with a breach incident, which results from diminished trust or confidence by present and future customers. Accordingly, our Institute's research shows that the negative publicity associated with a data breach incident can often damage companies' reputations and may lead to abnormal turnover, or churn, rates and a diminished rate for new customer acquisitions.

To extrapolate these opportunity costs, we used a shadow costing method that relies on the "lifetime value" of an average customer as defined for each participating organization.

- Turnover intentions of existing customers: The estimated number of customers who will most likely terminate their relationship as a result of the breach incident. The incremental loss is abnormal turnover attributable to the breach incident. This number is an annual percentage, which is based on estimates provided by management during the benchmark interview process.
- Diminished new customer acquisition: The estimated number of target customers who will not have a relationship with the organization as a consequence of the breach. This number is provided as an annual percentage.

It is important to note, however, that the loss of non-customer data, such as employee records, may not impact an organization's churn or turnover rates directly.

Key Report Findings

The Ponemon Institute's annual benchmark study, begun in 2005, examines the costs organizations incur when responding to data breach incidents resulting in the loss or theft of protected personal information.

Data breach costs continue to increase: According to participants in the 2009 study, data breaches cost their companies an average of $204 per compromised record – of which $144 pertained to indirect cost, including abnormal turnover or churn of existing and future customers.[6] Last year's average per victim cost was $202 with an average indirect cost at $152 per breach victim. This year, direct costs rose to $60 from $50 in 2008. Total cost rose only 1 percent, while indirect costs dropped 5 percent and direct costs soared by 20 percent due to increased legal defense costs.

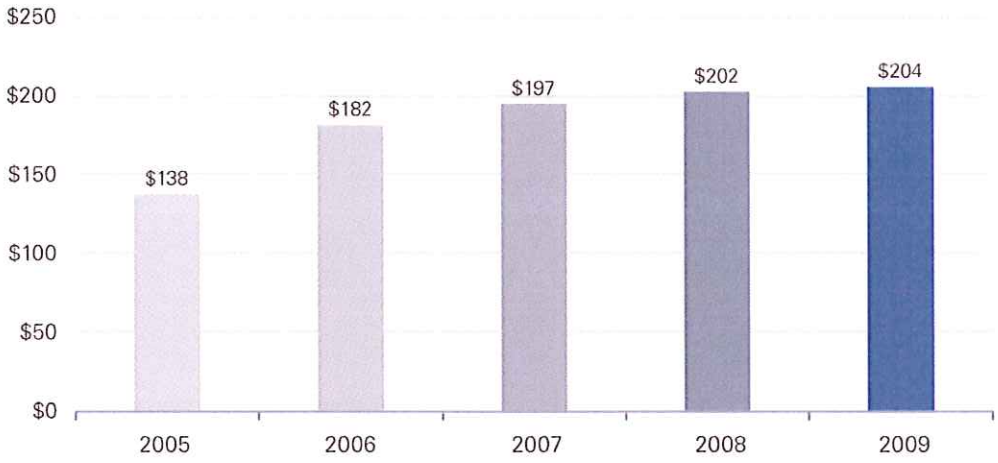


Figure 1: Average per-record cost of a data breach, 2005–2009

[6] For purposes of comparability across different breach incidents, we measure data breach cost on a *per victim* compromised record basis.

Direct vs. indirect costs of a data breach:

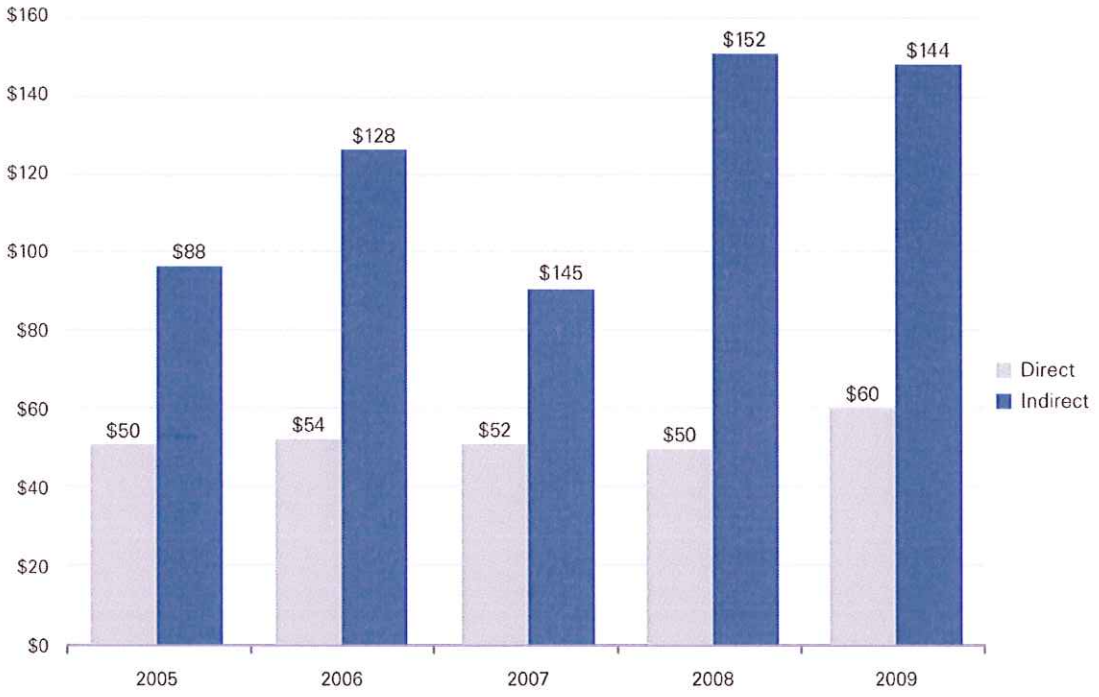


Figure 2: Direct vs. Indirect cost – 2008

Total cost average continues to increase: Data breaches continue to be very costly for organizations. The average organizational cost of a data breach increased from to $6.65 million in our 2008 study to $6.75 million in 2009. The most expensive data breach event included in this year's study cost a company nearly $31 million to resolve. The least expensive total cost of data breach for a company included in our study was $750,000. The magnitude of the breach event ranged from approximately 5,000 to approximately 101,000 lost or stolen records. As in prior years, data breach cost appears to be linearly related to the size or magnitude of the breach event.

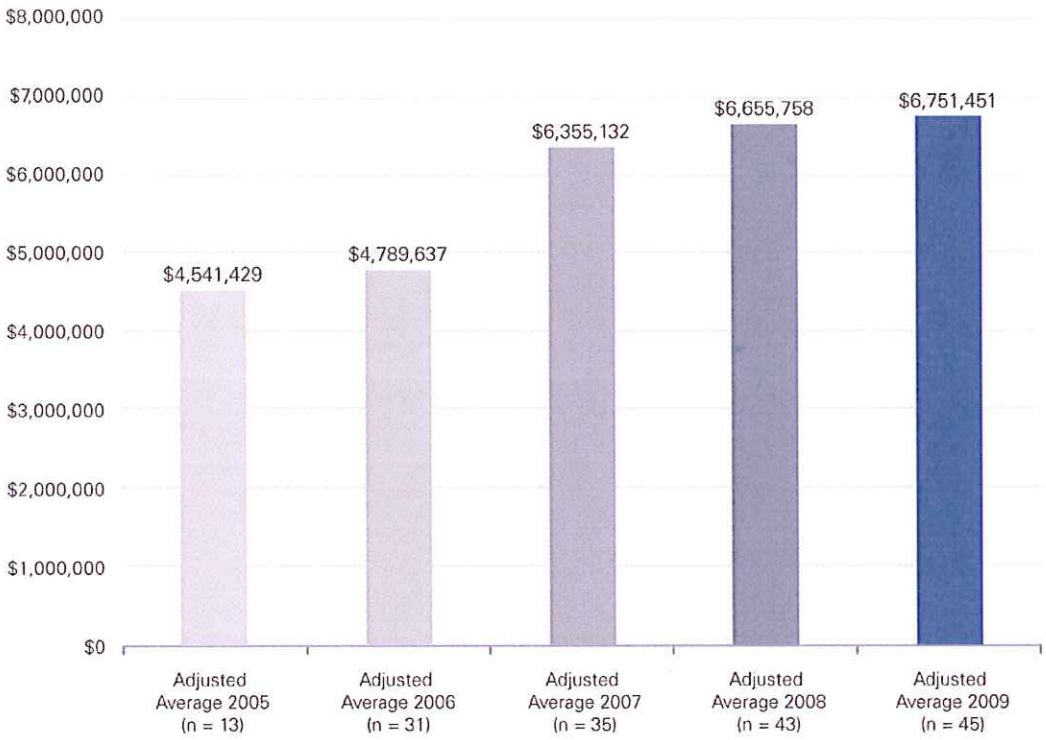


Figure 3: Average organizational costs of a data breach, 2005–2009

The cost of lost business decreased slightly but ex-post response increased: In a dramatic reversal, ex-post response represented the largest increase in total cost. Last year, this cost category represented the largest decrease. One of the main reasons for an increase in ex-post response costs is due to the increase in legal defense costs. This can be attributed to increasing fears of successful class actions resulting from customer, consumer or employee data loss.

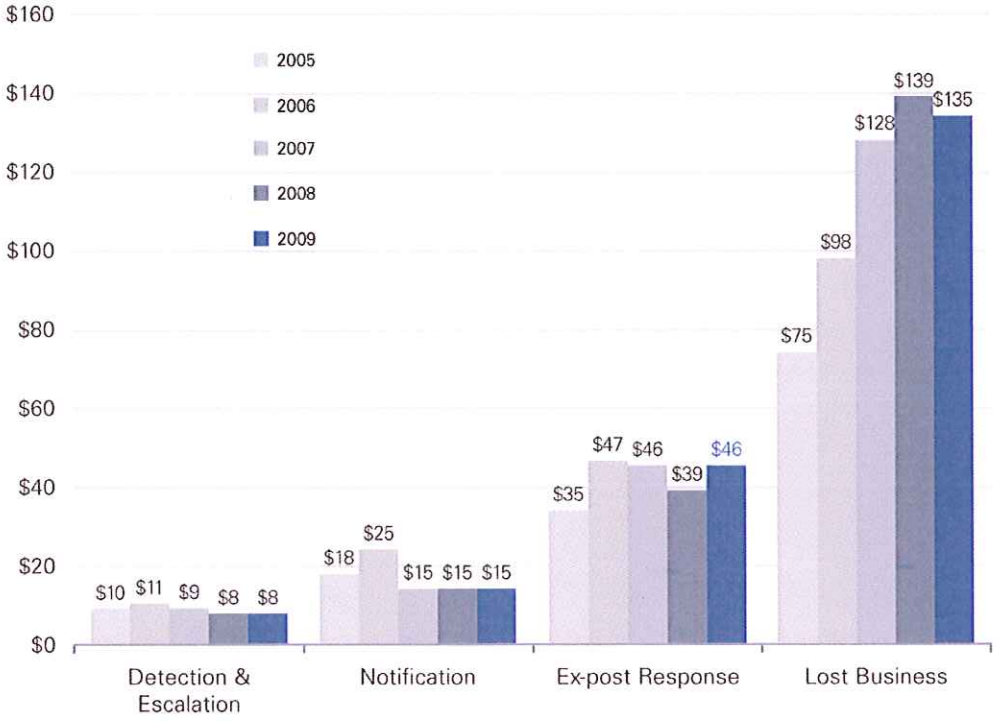


Figure 4: Average cost of data breach on a per-victim basis, 2005–2009

Malicious or criminal attacks growing costs: Twenty-four percent of all cases in this year's study involved a malicious or criminal attack that resulted in the loss or theft of personal information. Our research shows data breaches involving malicious or criminal acts are much more expensive than incidents resulting from negligence. Accordingly, in 2009 the cost per compromised record of a data breach involving a malicious or criminal act averaged $215. In contrast, the cost per compromised record of a data breach involving a negligent insider or a systems glitch averaged $154 and $166, respectively.

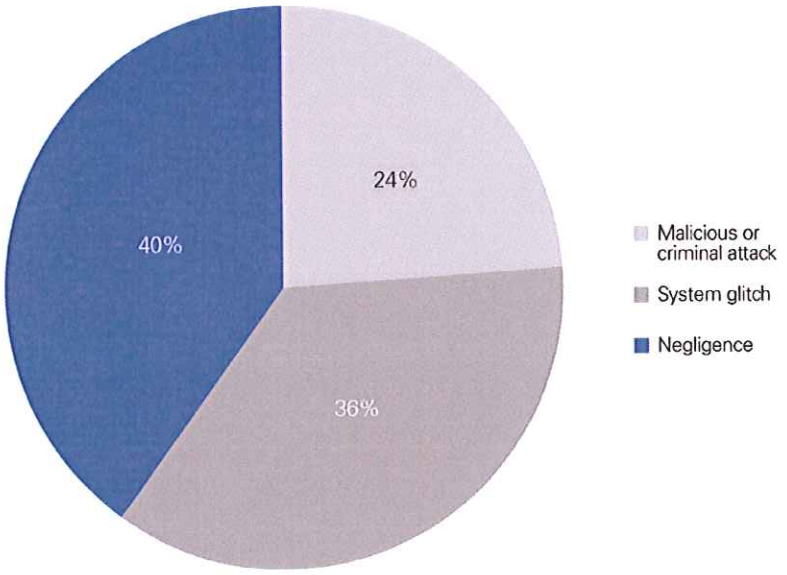


Figure 5: Malicious or criminal attacks

Figure 6: Malicious or criminal attacks cost of a breach per record, 2009

"First timers" cost more, repeat breaches continue: More than 82 percent of all cases in this year's study involved organizations that have had more than one data breach involving the loss or theft of more than 1,000 records containing personal information. Data breaches experienced by "first timers" are more expensive than those experienced by organizations that have had previous data breaches. The per victim cost for a first-time data breach was $228, versus $198 for companies that have experienced two or more incidents. This finding suggests companies that experience data breaches become more efficient at managing costs over time.

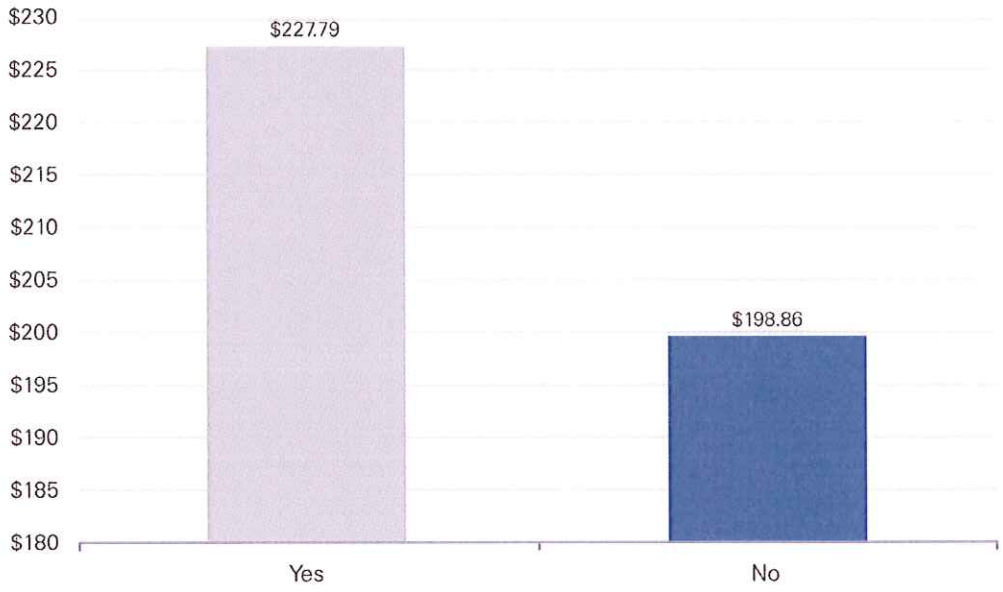


Figure 7: Cost of first time and subsequent data breaches, 2009

Measures implemented following a breach: As the result of a data breach, organizations often consider a number of possible remedies. Encryption is the most popular technology chosen to protect confidential and sensitive data as part of an enterprise data protection strategy.

What preventive measures have been implemented?	FY 2008	FY 2009
Training and awareness programs	53%	67%
Additional manual procedures and controls	49%	58%
Expanded use of encryption	44%	58%
Identity and access management solutions	37%	49%
Data loss prevention (DLP) solutions	26%	42%
Other system control practices	40%	40%
Endpoint security solutions	19%	36%
Security certification or audit	30%	33%
Security event management systems	21%	22%
Strengthening of perimeter controls	16%	20%

Table 2: Measures implemented as a result of a data breach

Increased churn rates following a breach: Abnormal churn or turnover of customers resulting directly from a data breach incident appears to the main driver of data breach cost. In this year's study, average abnormal churn rates across all 45 incidents was slightly higher than last year (from 3.6 percent in 2008 to 3.7 percent in 2009), which was measured by the loss of customers who were directly affected by the data breach event (i.e., typically those receiving notification). The industries with the highest churn rate were pharmaceuticals, communications and healthcare (all at 6 percent), followed by financial services and services (both at 5 percent). The industries with the lowest abnormal churn rates were manufacturing, energy and media (all at or below 1 percent), followed by technology and retail (both at 2 percent).

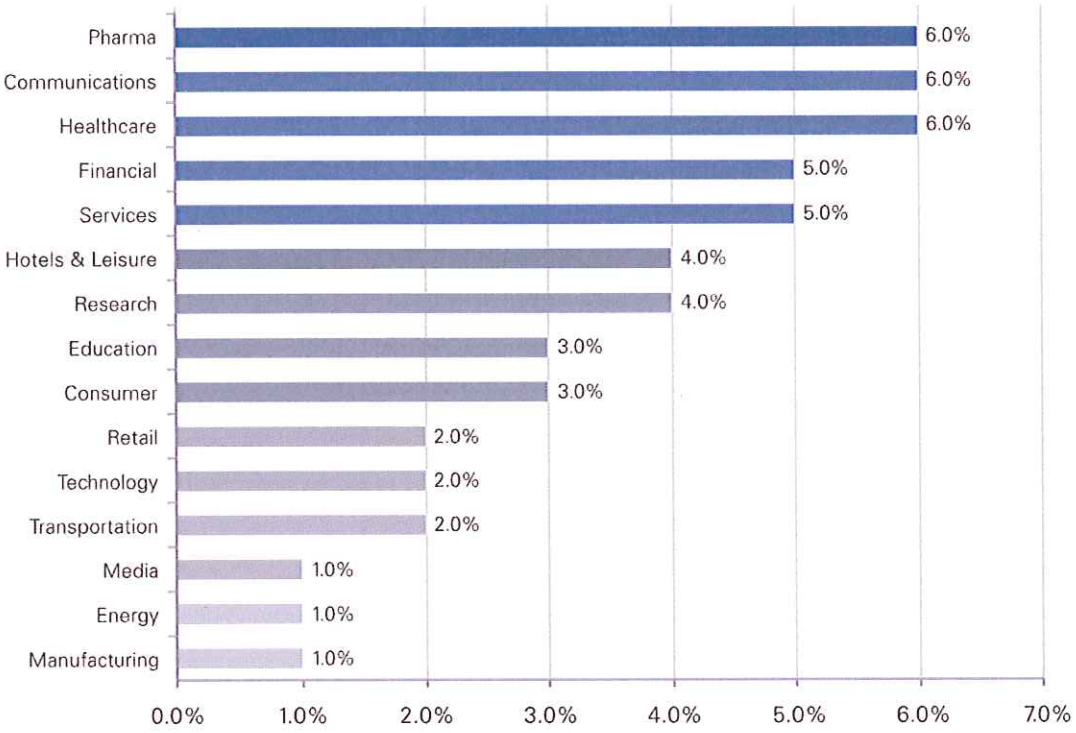


Figure 8: Abnormal churn rates following a data breach incident by industry classification, 2009

Expectations of trust and privacy drive data breach costs higher: Once again, our research finds organizations in highly trusted industries such as financial services and healthcare were more likely to experience a data breach with high abnormal churn rates. In contrast, retailers and companies with less direct consumer contact seem to experience a lower overall data breach cost.

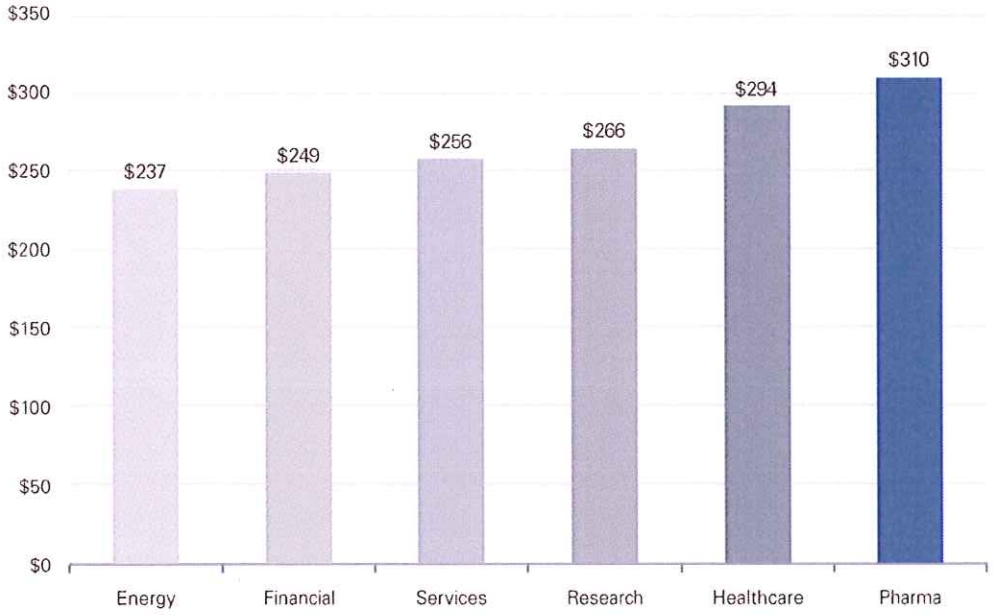


Figure 9: Cost per compromised records of a breach compared by industry classification, 2009

Costs of breach by activity, indirect vs. direct: When the survey first started in 2005, the indirect cost of lost business due to churn accounted for 55 percent of total breach costs. While cost of lost business has remained relatively stable over the last five years, organizations are spending more on legal defense costs - a direct cost. Other direct costs that have increased over the last five years include audit and consulting services.

Cost changes over five years	2005	2006	2007	2008	2009	Net change
Investigations & forensics	8%	8%	8%	9%	8%	stable
Audit and consulting services	8%	10%	10%	11%	12%	increase
Outbound contact costs	13%	9%	7%	6%	6%	decrease
Inbound contact costs	15%	10%	8%	6%	5%	decrease
Public relations/communications	0%	1%	3%	1%	1%	decrease
Legal services - defense	5%	6%	8%	9%	14%	increase
Legal services - compliance	3%	3%	3%	1%	2%	stable
Free or discounted services	4%	2%	1%	2%	1%	decrease
Identity protection services	3%	3%	2%	2%	2%	stable
Lost customer business (due to churn)	35%	39%	41%	43%	40%	stable
Customer acquisition cost	6%	8%	9%	9%	9%	stable

Table 3: Percent of breach costs by activity, 2005-2009

Note: The cost of lost business includes both lost business due to churn and increased customer acquisition costs.

2009 Annual Study: U.S. Cost of a Data Breach

Cause of a data breach: Forty-two percent all cases in this year's study involved third-party mistakes or flubs. Data breaches involving outsourced data to third parties, especially when the third party is offshore, were most costly. This could be due to additional investigation and consulting fees. The cost per compromised record for data breaches involving third parties was $217 versus $194, more than a $21 difference.

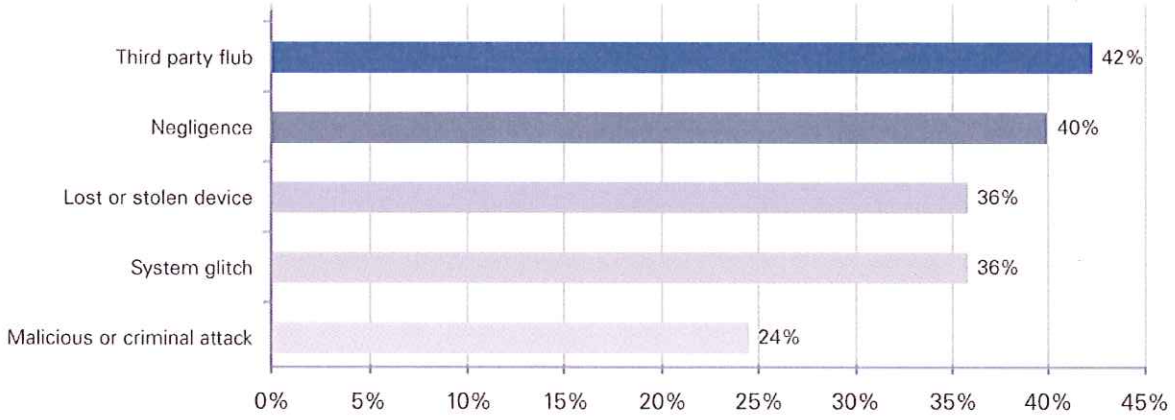


Figure 10: Primary cause of a data breach, 2009

Thirty-six percent of all cases in this year's study involved lost or stolen laptop computers or other mobile data-bearing devices. Data breaches concerning lost, missing or stolen laptop computers are more expensive than other incidents. Specifically, in this year's study the per victim cost for a data breach involving a lost or stolen laptop was just under $225, over $30 more than if a laptop or mobile device was not involved.

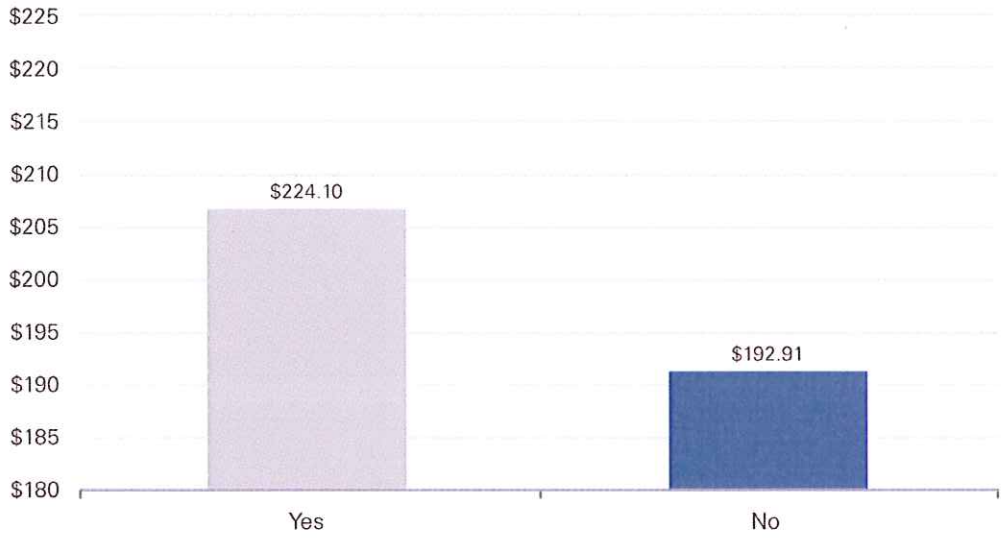


Figure 11: Cost involving lost or stolen laptop, 2009

CISO leadership in breach response: In approximately 40 percent of participating companies, the CISO was in charge of managing the data breach incident. While other senior IT officials within an organization are typically involved in crisis management activities surrounding data breach response, our results suggest CISO leadership substantially reduces the overall cost of data breaches. This is likely due to the strategic role CISOs play in ensuring security and privacy measures are effectively implemented. Specifically, companies that had a CISO (or equivalent title) who managed the data breach incident experienced an average cost per compromised record of $157, versus $236 for companies without CISO leadership.

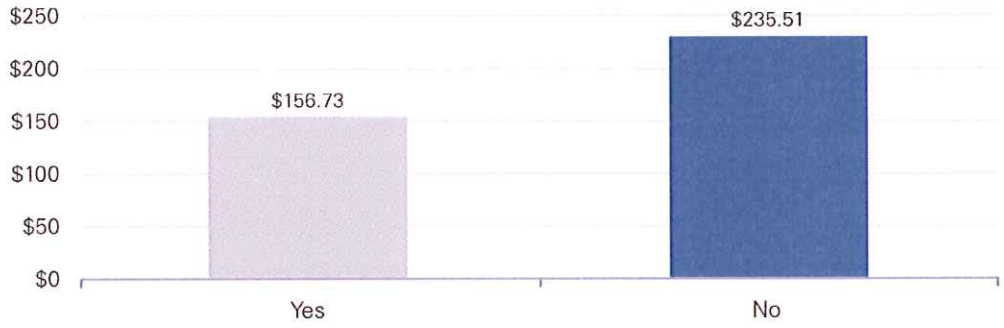


Figure 12: Cost of a data breach when CISO is in charge, 2009

About 36 percent of participating companies notified victims within one month of discovering the data breach (a.k.a. quick responders). Surprisingly, our findings suggest that companies that notify victims quickly experienced a higher average cost per compromised record of a data breach than companies that moved more slowly ($219 versus $196). Our results suggest that moving too quickly through the data breach process may cause cost inefficiencies for the organization, especially during the detection, escalation and notification phases.

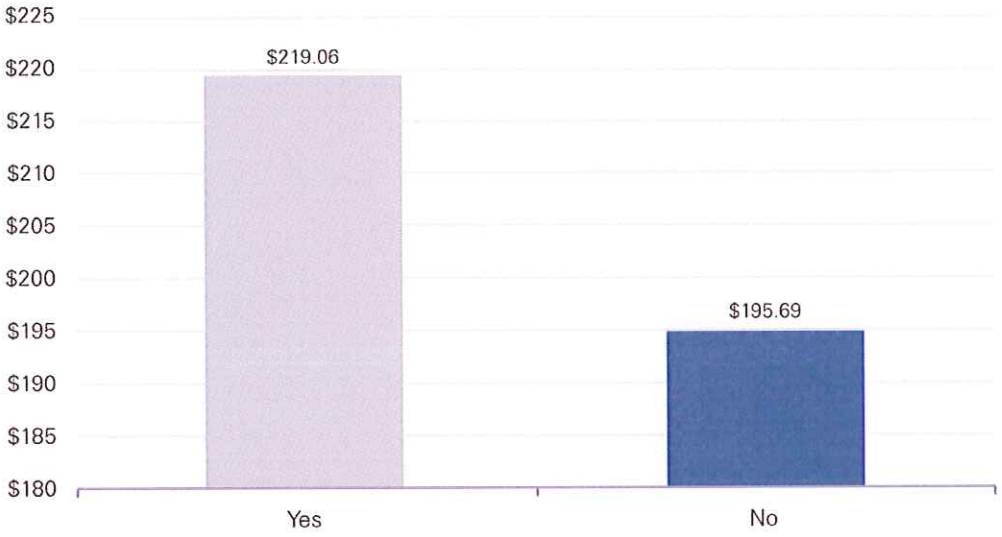


Figure 13: Cost of a data breach for quick responders, 2009

More than 42 percent of participating companies achieved a Security Effectiveness Score (SES) that was above the median value determined from benchmark results.[7] As expected, those organizations with a more favorable security posture (SES above the median) experienced a lower average cost per compromised record than organizations with an SES below the median. Accordingly, organizations with a favorable security posture had an average cost per compromised record of $202, versus $207 for those with an unfavorable security posture.

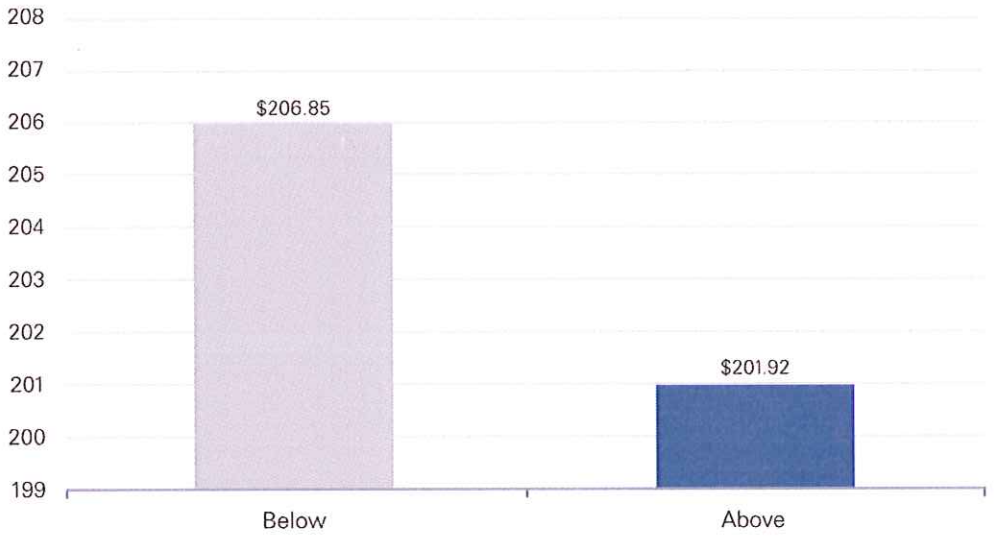


Figure 14: Cost of a data breach when company has a favorable security posture, 2009

[7] The SES is a methodology developed by Ponemon Institute and PGP Corporation in 2005 for its annual encryption trends study. The SES measures the effectiveness of an organization's security posture. Since its inception five years ago, this proprietary security scoring method has been used in more than 80 studies involving information security practitioners in organizations throughout the world.

About 44 percent of participating companies engaged an outside consultant to assist them over the course of the data breach incident. Our findings suggest that engaging a consultant or other third-party expert to assist in data breach response results in a lower average cost per compromised record. Specifically, those organizations that engaged a consultant experienced, on average, a per victim cost of $170, as opposed to $231 for companies that decided to go it alone. Our research indicates that organizations that engage outside consultants may have more resources and be more responsive overall to IT security issues than those that do not.

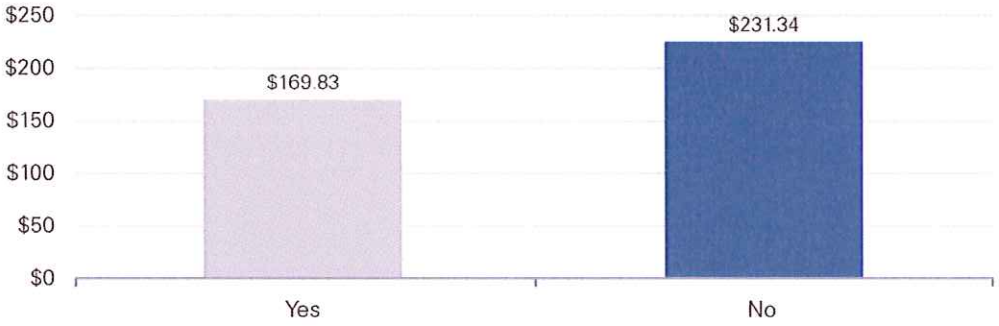


Figure 15: Cost of a data breach when outside consultant is involved with response, 2009

Report Conclusions

The findings of this benchmark study suggest U.S. companies that have a loss or theft of personal information requiring notification do incur significant direct and indirect expenses. The most negative cost impact results from the diminishment of confidence and trust in the company, which translates into abnormal or unexpected customer turnover.

The top five sectors represented among 2009 study participants were retail and financial (18 percent each), consumer and healthcare (12 percent each) and technology (9 percent). Some industries with higher customer churn rates, such as healthcare (6 percent) and financial services (5 percent), also happen to be those that handle more sensitive personal information and must meet data breach notification mandates. They also often receive the most media attention when a large breach occurs.

Data breaches are becoming a fact of life, which may be causing fewer people to end or diminish their relationships with breached organizations. More products and services become available to meet the demand, bringing down costs, and increasing mandates and regulations may push more organizations to clean up after the fact. Time will tell whether the data breach notification legislation and other government action that occurred in 2009 will create the desired long-term reductions of the incidence and severity of data breaches for U.S. organizations.

In addition to major findings mentioned above, other key takeaways from the report include:

- **Hiring outside IT security consultants is common and can greatly lower data breach costs.** More than 4 out of 10 participating organizations engaged outside consultants or experts to assist in data breach response, and those that did had lower average data breach costs per capita ($170 with consultants versus $231 without, a 26 percent difference). This figure is more likely an indication of certain organizational having more resources and responsiveness to data breach issues in general than a statement on the quality of consulting work itself.

- **Data breaches involving outsourced data to third parties, especially when the third party is offshore, are common and more costly.** Forty-two percent of all cases in this year's study involved third-party mistakes or flubs. The cost per compromised record for data breaches involving third parties was $217, versus $194 for cases that did not, a 12 percent difference. This could be due to additional investigation and consulting fees.

- **More than 1 in 3 data breaches concerned lost, missing or stolen laptop computers and those incidents are more expensive** -- $225 per victim, 10 percent higher than the average total cost and 5 percent higher than malicious attacks.

- **Data breaches experienced by "first timers" are more expensive than those encountered by organizations that have had previous data breaches.** The per victim cost for a first-time data breach is $228, versus $198 – 13 percent less – for companies that have experienced two or more incidents. For better or worse, fewer and fewer companies fall into the first-time category: more than 82 percent of 2009 survey participants have had more than one breach.

- **Negligent insider breaches have decreased in number and cost.** One explanation is that training and awareness programs may be having a positive effect on employees' sensitivity and awareness about the protection of personal information.

- **Organizations are spending more on legal defense costs, leading to a dramatic reversal in ex-post response spending.** Ex-post response represented the largest increase in total cost in 2009, while in 2008, this cost category represented the largest decrease. This can be attributed to increasing fears of successful class actions resulting from customer, consumer or employee data loss.

Preventive Solutions

Especially given the rise in data-stealing malicious attacks, organizations should strongly consider a holistic approach to protecting data wherever it is – at rest, in motion and in use. While manual and policy approaches may come first to mind for many companies, those approaches by themselves are not as effective as a multi-pronged approach that includes automated IT security solutions.

Many kinds of automated, cost-effective enterprise data protection solutions are now available to secure data both within an organization and among business partners. Some of the most popular and effective of these technologies currently available include:

- Encryption (including whole disk encryption and for mobile devices/smartphones)
- Data loss prevention (DLP) solutions
- Identity and access management solutions
- Endpoint security solutions and other anti-malware tools

Companies should also look for centralized management of IT security solutions so they can automatically enforce IT security best practices throughout their organizations. Such capability enables enterprises to align information protection with corporate security policies and regulatory or business-partner mandates. It also enables organizations to implement technology with minimal or no user disruption, encouraging user compliance and acceptance.

Next Steps

This fifth annual report enables organizations to forecast in detail the specific actions and costs required to recover from a customer data security breach. This report can be used as a guideline to conduct an internal audit and to create breach response cost estimates. These estimates may then be compared with the technology and other costs of preventing data breaches.

Companies should also consider the following best practices:

- Companies should ensure that portable data-bearing devices – such as laptops, smart phones and USB memory sticks – are encrypted, especially for people who travel extensively for business.

- Companies should vet and evaluate the security posture of third parties before sharing confidential or sensitive information.

- Companies should have a crisis management plan that clearly defines roles, responsibilities, procedures and timelines.

- Companies should establish an organizational structure that allows the CISO or other security/privacy leaders to take charge and ensure the detection and notification process is handled appropriately.

- When in doubt about requirements, companies should seek the counsel of consultants and legal experts to ensure the notification process complies with the plethora of state data breach notification laws, as well as related federal laws.

- To minimize customer turnover (churn), companies should draft communications that clearly define the issue and root cause of the breach incident. Whenever feasible, the company should take steps that minimize potential harm to data breach victims. For instance, the company may consider providing free identity protection services when the root cause of a breach is likely to be a theft or criminal attack.

- Finally, companies should perform a post-mortem a few months after the incident to objectively evaluate the adequacy and effectiveness of the overall response. At this point, it may make good sense to consider buying insurance products to defray future data breach costs.

About The Ponemon Institute

The Ponemon Institute© is dedicated to advancing ethical information and privacy management practices in business and government. The Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations in a variety of industries.

Dr. Larry Ponemon is the chairman and founder of the Ponemon Institute. He is also a founding member of the Unisys Security Leadership Institute and an Adjunct Professor of Ethics & Privacy at Carnegie Mellon University's CIO Institute. Dr. Ponemon is a critically acclaimed author, lecturer, spokesman, and pioneer in the development of privacy auditing, privacy risk management, and the ethical information management process.

Previously, Dr. Ponemon was the CEO of the Privacy Council and the Global Managing Partner for Compliance Risk Management at PricewaterhouseCoopers (where he founded the privacy practice). Prior to joining PricewaterhouseCoopers, Dr. Ponemon served as the National Director of Business Ethics Services for KPMG and as the Executive Director of the KPMG Business Ethics Institute. Dr. Ponemon holds a Ph.D. from Union College, attended the Doctoral Program in System Sciences at Carnegie-Mellon University, and has a Masters degree from Harvard University as well as a Bachelors degree from the University of Arizona. Contact The Ponemon Institute at www.ponemon.org or +1 800 887 3118.

About PGP Corporation

PGP Corporation is a global leader in email and data encryption software for enterprise data protection. Based on a unified key management and policy infrastructure, the PGP® Encryption Platform offers the broadest set of integrated applications for enterprise data security. PGP® platform-enabled applications allow organizations to meet current needs and expand as security requirements evolve for email, laptops, desktops, instant messaging, PDAs, network storage, file transfers, automated processes, and backups.

PGP® solutions are used by more than 100,000 enterprises, businesses, and governments worldwide, including 95 percent of the Fortune® 100, 75 percent of the Fortune® Global 100, 87 percent of the German DAX index, and 51 percent of the U.K. FTSE 100 Index. As a result, PGP Corporation has earned a global reputation for innovative, standards-based, and trusted solutions. PGP solutions help protect confidential information, secure customer data, achieve regulatory and audit compliance, and safeguard companies' brands and reputations. Contact PGP Corporation at www.pgp.com or +1 650 319 9000.

Appendix A – Survey Methodology

Our study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

- Non-statistical sample: The purpose of this study is descriptive inquiry rather than normative inference. This research draws upon a representative, but non-statistical sample of U.S. organizations experiencing a breach involving the loss or theft of customer or consumer data over the past 12 month period.

  For consistency purposes, our study does not include data breaches resulting from missing or stolen employee records. In addition, we deliberately excluded data breaches considered to be catastrophic (as defined by an event involving the loss or theft of more than 150,000 records). Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the judgmental nature of our company recruitment process.

- Non-response: The current findings are based on a small representative sample of completed benchmark surveys. An initial invitation was sent to a targeted group of 126 organizations, all known to have experienced a breach involving the lost or theft of customer or consumer data sometime over the past year. Forty-five US companies completed all parts of the benchmark survey. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the methods used to manage the data breach process, as well as the underlying costs associated with information loss.

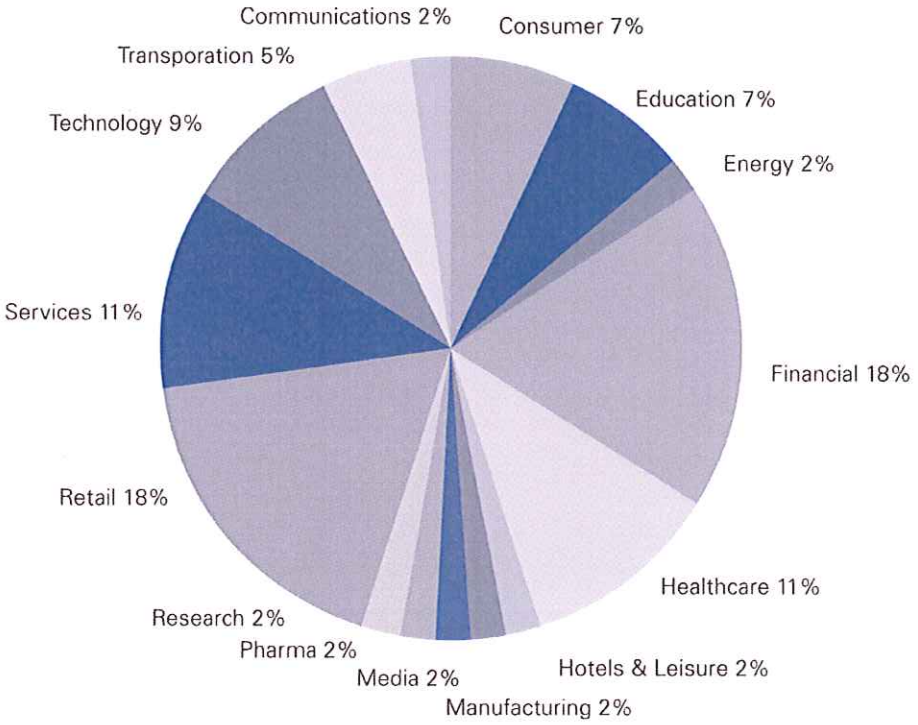
- Sampling-frame bias: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.

- Company-specific information: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.

- Unmeasured factors: To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.

- Estimated cost results. The quality of survey research is based on the integrity of confidential responses received from companies. While reliability checks were incorporated into the benchmark survey process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique rather than the company's detailed actual cost data could create significant bias in presented results.

2009 Annual Study: U.S. Cost of a Data Breach



Industry Classification	Frequency
Financial	8
Retail	8
Healthcare	5
Services	5
Technology	4
Consumer	3
Education	3
Transportation	2
Communications	1
Pharma	1
Hotel & leisure	1
Manufacturing	1
Media	1
Energy	1
Research	1

Figure 16 and Table 4: Sample composition by industry vertical

Benchmark Methods

The benchmark survey instrument was designed to collect descriptive information about the costs incurred either directly or indirectly concerning the breach event. Typically, the point-person for each survey was privacy, data protection or compliance professionals responsible for managing the data breach incident. The survey required these practitioners to estimate the opportunity cost associated with different program activities. Data was collected on a structured survey form. The researcher conducted a follow-up interview to obtain additional facts, including estimated abnormal churn rates that resulted from the breach event.

The survey design relied upon a shadow costing method used in applied economic research. This method doesn't require subjects to provide actual accounting results, but instead relies on broad estimates based on the experience of the subject.

Within each category, cost estimation was a two-stage process. First, the survey required individuals to provide direct cost estimates for each privacy cost category by checking a range variable. A range variable was used rather than a point estimate to preserve confidentiality (to ensure a higher response rate). Second, the survey required participants to provide a second estimate for both indirect cost and opportunity cost, separately. These estimates were calculated based on the relative magnitude of these costs in comparison to direct cost within a given category.

The size and scope of survey items was limited to known cost categories that cut across different industry sectors. We believed that a survey focusing on process (and not areas of compliance) would yield a higher response rate and better quality of results. We also used a paper instrument, rather than electronic survey, to provide greater assurances of confidentiality.

The diagram below illustrates the activity-based costing schema used in the current benchmark study. The study examined the above-mentioned cost centers. The arrows suggest that these cost centers are sequentially aligned, starting with incident discovery and proceeding to escalation, notification, ex-post response, and culminating in lost business. The cost driver of ex-post response and lost business opportunities is the public disclosure or notice of the event.

2009 Annual Study: U.S. Cost of a Data Breach

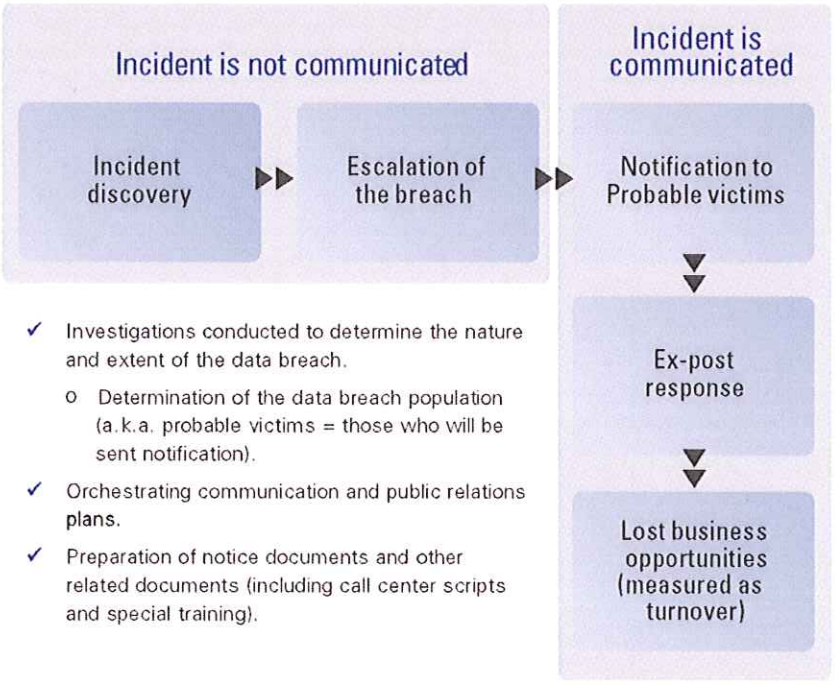


Figure 16: Visual representation of benchmark cost categories

2010 Data Breach Investigations Report

AUTHORS:

Wade Baker
Mark Goudie
Alexander Hutton
C. David Hylender
Jelle Niemantsverdriet
Christopher Novak
David Ostertag
Christopher Porter
Mike Rosen
Bryan Sartin
Peter Tippett, M.D., Ph.D
Men and women of the United States Secret Service

CONTRIBUTORS:

Thijs Bosschert
Eric Brohm
Calvin Chang
Michael Dahn
Ron Dormido
Ben van Erck
Kylee Evans
Eric Gentry
John Grim
Clarence Hill
Adam Kunsemiller
Kenny Lee
Wayne Lee
Kevin Long
Raphael Perelstein
Enrico Telemaque
Denson Todd
Yuichi Uzawa
J. Andrew Valentine
Nicolas Villatte
Matthijs van der Wel
Paul Wright

SPECIAL THANKS TO:

Tracey Beeferman
Carl Dismukes
Paul Goulding
Carole Neal

TABLE OF CONTENTS

For additional updates and commentary, please visit http://securityblog.verizonbusiness.com.

For inquiries directed to the United States Secret Service, contact databreachstudy@usss.dhs.gov.

2010 Data Breach Investigations Report

A study conducted by the Verizon Business RISK team in cooperation with the United States Secret Service.

Executive Summary

In some ways, data breaches have a lot in common with fingerprints. Each is unique and we learn a great deal by analyzing the various patterns, lines, and contours that comprise each one. The main value of fingerprints, however, lies in their ability to identify a particular individual in particular circumstances. In this sense, studying them in bulk offers little additional benefit. On the other hand, the analysis of breaches in aggregate can be of great benefit; the more we study, the more prepared we are to stop them.

Not surprisingly, the United States Secret Service (USSS) is also interested in studying and stopping data breaches. This was a driving force in their decision to join us in this 2010 Data Breach Investigations Report. They've increased the scope of what we're able to study dramatically by including a few hundred of their own cases to the mix. Also included are two appendices from the USSS. One delves into online criminal communities and the other focuses on prosecuting cybercrime. We're grateful for their contributions and believe organizations and individuals around the world will benefit from their efforts.

With the addition of Verizon's 2009 caseload and data contributed from the USSS, the DBIR series now spans six years, 900+ breaches, and over 900 million compromised records. We've learned a great deal from this journey and we're glad to have the opportunity to share these findings with you. As always, our goal is that the data and analysis presented in this report proves helpful to the planning and security efforts of our readers. We begin with a few highlights below.

WHO IS BEHIND DATA BREACHES?	
70% resulted from external agents (-9%)	Including the USSS cases in this year's report shook things up a bit but didn't shake our worldview. Driven largely by organized groups, the majority of breaches and almost all data stolen (98%) in 2009 was still the work of criminals outside the victim organization. Insiders, however, were more common in cases worked by the USSS, which boosted this figure in the joint dataset considerably. This year's study has by far improved our visibility into internal crime over any other year. Breaches linked to business partners continued the decline observed in our last report and reached the lowest level since 2004.
48% were caused by insiders (+26%)	
11% implicated business partners (-23%)	
27% involved multiple parties (-12%)	

	HOW DO BREACHES OCCUR?
Related to the larger proportion of insiders, Misuse sits atop the list of threat actions leading to breaches in 2009. That's not to say that Hacking and Malware have gone the way of the dinosaurs; they ranked #2 and #3 and were responsible for over 95% of all data comprised. Weak or stolen credentials, SQL injection, and data-capturing, customized malware continue to plague organizations trying to protect information assets. Cases involving the use of social tactics more than doubled and physical attacks like theft, tampering, and surveillance ticked up several notches.	**48%** involved privilege misuse (+26%)
	40% resulted from hacking (-24%)
	38% utilized malware (<>)
	28% employed social tactics (+16%)
	15% comprised physical attacks (+6%)

WHAT COMMONALITIES EXIST?

98% of all data breached came from servers (-1%)

85% of attacks were not considered highly difficult (+2%)

61% were discovered by a third party (-8%)

86% of victims had evidence of the breach in their log files

96% of breaches were avoidable through simple or intermediate controls (+9%)

79% of victims subject to PCI DSS had not achieved compliance

As in previous years, nearly all data were breached from servers and applications. This continues to be a defining characteristic between data-at-risk incidents and those involving actual compromise. The proportion of breaches stemming from highly sophisticated attacks remained rather low yet once again accounted for roughly nine out of ten records lost. In keeping with this finding, we assessed that most breaches could have been avoided without difficult or expensive controls. Yes, hindsight is 20/20 but the lesson holds true; the criminals are not hopelessly ahead in this game. The more we know, the better we can prepare. Speaking of being prepared, organizations remain sluggish in detecting and responding to incidents. Most breaches are discovered by external parties and only then after a considerable amount of time.

While we've added some new suggestions to the Conclusions and Recommendations section of this report, what you see to the right is similar to the message we've been preaching from the beginning. That's not because we don't feel like writing another sermon; it's simply that, based on the data before us, all the points in this one still apply.

This study always reminds us that our profession has the necessary tools to get the job done. The challenge for us lies in selecting the right tools for the job at hand and then not letting them get dull and rusty over time. Evidence shows when that happens, our adversaries are quick to take advantage of it.

The amount of breaches that exploit authentication in some manner is a problem. In our last report it was default credentials; this year it's stolen and/or weak credentials. Perhaps this is because attackers know most users are over-privileged. Perhaps it's because they know we don't monitor user activity very well. Perhaps it's just the easiest way in the door. Whatever the reason, we have some work to do here. It doesn't matter how hardened our defenses are if we can't distinguish the good guys from the bad guys.

Malware gets increasingly difficult to detect and prevent (especially once the attacker owns the system). Therefore, protect against the damage malware does after infection, much of which can be mitigated if outbound traffic is restricted.

Finally, the value of monitoring (perhaps we should say "mining") logs cannot be overstated. The signs are there; we just need to get better at recognizing them.

WHERE SHOULD MITIGATION EFFORTS BE FOCUSED?

- ✔ Eliminate unnecessary data; keep tabs on what's left
- ✔ Ensure essential controls are met
- ✔ Check the above again
- ✔ Test and review web applications
- ✔ Audit user accounts and monitor privileged activity
- ✔ Filter outbound traffic
- ✔ Monitor and mine event logs

Methodology

It is often said that the role of science is to explain the "how" of things in the natural world. We find it a fitting description and applaud all who study the intricacies of our field in pursuit of greater understanding. In that vein, the 2010 Data Breach Investigations Report (DBIR) marks the third installment (fifth if you count supplemental reports) in our continuing effort to shed light on the "how" of things in the world of computer crime.

The collection of data through rigorous observation is, of course, one of the cornerstones of any scientific endeavor. While we like to think our methodology has been rigorous, it cannot be said that it has been entirely consistent. The 2008 DBIR was a retrospective covering four years (2004-2007) of Verizon's caseload in one massive data collection effort. The scope was large but the level of analysis was somewhat limited due to the passage of time. The shift from historic to ongoing collection for the 2009 DBIR opened the door to more active observation, greater detail, and new areas of study. This approach certainly would have worked again for this year's report and would have maintained a state of consistency, which is a good trait to have in a methodology. Our ultimate goal, however, is not a state of consistency; our ultimate goal is a state of knowledge. It is to understand and explain the "how."

Not only does this increase the size of the window of visibility we have into the world of data breaches but also grants a new perspective into that world. As will be seen, our caseloads share many similarities, but there are some key differences as well.

For this reason, we are shaking things up again by including a completely foreign and very different (yet still very reliable) dataset in the 2010 DBIR. We're thrilled to welcome the contributions (in data and expertise) of the United States Secret Service (USSS) to this year's report. Not only does this increase the size of the window of visibility we have into the world of data breaches but also grants a new perspective into that world. As will be seen, our caseloads share many similarities, but there are some key differences as well. Both are instructive and we firmly believe this joint effort will lead us closer to the goal described above.

Pulling the two datasets together was quite an undertaking for both parties and the rest of this section will explain how it was accomplished.

Verizon Data Collection Methodology

The underlying methodology used by Verizon remains unchanged from that of previous years. All results are based on firsthand evidence collected during paid forensic investigations conducted by Verizon from 2004 to 2009. The 2009 caseload is the primary analytical focus of the report, but the entire range of data is referenced extensively throughout. Though the Investigative Response (IR) team works a variety of engagements, only those involving a confirmed breach are included in this data set. To help ensure reliable and consistent input, all investigators use the Verizon Enterprise Risk and Incident Sharing (VERIS) framework to record case data and other relevant details. The information collected using VERIS is then submitted to members of the RISK Intelligence team for further validation and analysis. The aggregate repository of case data is sanitized and contains no information that would enable one to ascertain a client's identity.

USSS Data Collection Methodology

With all the talk of "shaking things up" above, one might conclude that consistency was tossed out the window in this year's report. This is not the case. In terms of data collection, the USSS methodology differs little from that of Verizon. For the purposes of this study, the USSS created an internal application based on the VERIS framework. From the thousands of cases worked by the USSS during 2008 and 2009[1], the scope was narrowed to only those involving confirmed organizational data breaches[2] in alignment with the focus of the DBIR. The scope was further narrowed to include only cases for which Verizon did not conduct the forensic investigation[3]. Of these cases, a sample was taken and requests to input data were sent to USSS agents who worked each case. In doing so, these agents utilized investigative notes, reports provided by the victim or other forensic firms, and their own experience gained in handling the case. This yielded 257 qualifying cases for which data were collected within the time frame set for this report. The resulting dataset was purged of any information that might identify organizations or individuals involved in the case and then provided to Verizon's RISK Intelligence team for analysis.

In conclusion, we would like to reiterate that we make no claim that the findings of this report are representative of all data breaches in all organizations at all times. Even though the merged Verizon-USSS dataset (presumably) more closely reflects reality than either in isolation, it is still a sample. Although we believe many of the findings presented in this report to be appropriate for generalization (and our confidence in this grows over time), bias undoubtedly exists. Even so, there is a wealth of information here and no shortage of valid and clear takeaways. As with any study, readers will ultimately decide which findings are applicable within their organization.

A BRIEF PRIMER ON VERIS

VERIS is a framework designed to provide a common language for describing security incidents in a structured and repeatable manner. It takes the narrative of "who did what to what or whom with what result" and translates it into the kind of data you see presented in this report. Because many readers asked about the methodology behind the DBIR and because we hope to facilitate more information sharing on security incidents, we released VERIS earlier this year for free public use. A brief overview of VERIS is available on our website[4] and the complete framework can be obtained from the VERIS community wiki[5]. Both are good companion references to this report for understanding terminology and context.

1 The scope of data collection for the USSS was 2008 and 2009. However, over 70 cases worked in 2008 pertained to breaches that occurred in 2007. Because this is a large enough sample and allows for three-year trend analysis, we show them separate from 2008 breaches.

2 The USSS works many cases related to theft and fraud that are not included in this report. For instance, crimes committed against consumers that do not involve an organization or its assets are not included. Criminal activities that occur after data are stolen (i.e., "white plastic fraud" and identity theft) are also not within the scope of this study.

3 The USSS is often involved in one manner or another with cases worked by Verizon (especially the larger ones). To eliminate redundancy, these cases were removed from the USSS sample. Where both Verizon and the USSS worked a case, Verizon-contributed data were used.

4 http://www.verizonbusiness.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_en_xg.pdf

5 https://verisframework.wiki.zoho.com/

Cybercrime Year in Review, 2009

2009 was, in many ways, a transformational year in the trenches. As attackers and defenders vied for advantage, there were numerous developments on many fronts around the world. It's difficult to measure who's winning with any certainty but there are, at least, some measurements available. One of them, public breach disclosures, fell noticeably in 2009. Organizations that track disclosed breaches like DataLossDB[6] and the Identity Theft Resource Center[7] reported figures that were well off 2008 totals. Private presentations and hallway conversations with many in the know suggested similar findings. Our own caseload reveals this as well. In a report dedicated to the analysis of annual breach trends, it seems wholly appropriate to reflect on why. It also provides a fitting backdrop for discussing some key 2009 milestones.

In our last report, we observed that massive exposures of payment card data in recent years have effectively flooded the market and driven down the prices criminals can get for their stolen wares. 2009, then, may simply be the trough in a natural supply and demand cycle. If supply has outpaced demand, why release more product? Perhaps cybercriminals are directing their resources elsewhere until market conditions improve. It is also possible that breaches are occurring at the same rate but the criminals are sitting on stolen data until demand picks up. Because fraud alerts are the leading method of discovering breaches, it stands to reason that many breaches could occur without anyone being the wiser if the criminal decided it was in his best interest to be patient.

Perhaps cybercriminals are directing their resources elsewhere until market conditions improve. It is also possible that breaches are occurring at the same rate but the criminals are sitting on stolen data until demand picks up.

Another possible reason for this decline is law enforcement's effectiveness in capturing the criminals. The prosecution of Albert Gonzalez was a major event in 2009. He and his accomplices were responsible for some of the largest data breaches ever reported. Taking them off the streets, so to speak, may have caused a temporary (but we can hope for permanent) dip in breaches. It is also possible that their prosecution made other cybercriminals take some time off to reevaluate their priorities in life.

2009 witnessed much discussion and consideration around the world about breach disclosure laws. As seen in the U.S., the creation of these laws can have a huge effect on breach statistics. So can the administration of them. Depending on how the legal environment evolves in this area, it could have a significant impact on the number of known breaches worldwide.

While it's highly unlikely that cloud computing or virtualization had anything to do with breach disclosure rates, they were no doubt hot topics in 2009. We continue to search for a link between data breaches and cloud-based or virtualized infrastructure but continue to find none.

Finally, we would be remiss if we did not touch on the subject of the hour, Advanced Persistent Threats (APTs). Yes, APTs are real but they are not new. Although the hype has grown exponentially, the post-2010 threat of APTs to your organization is more or less the same as pre-2010 levels. While we do appreciate the business, we would like to save you some expense and heartache: APTs are not the source of all malware infections and suspicious traffic on your network. Don't get caught up in the hype. Manage your defenses based on reality, not on publicity. We hope this report helps with that.

6 http://datalossdb.org/
7 http://www.idtheftcenter.org/index.html

Results and Analysis

The Verizon IR team worked over 100 cases in 2009; 57 of them were confirmed breaches. While lower than typical for our caseload, many of these breaches were quite large and complex, often involving numerous parties, interrelated incidents, multiple countries, and many affected assets. The 257 qualified cases in the USSS dataset[8] included 84 cases from 2009, 102 from 2008, and 71 from 2007.

The primary dataset analyzed in this report contains the 141 (57 + 84) confirmed breach cases worked by Verizon and the USSS in 2009. The total number of data records compromised across these cases exceeds 143 million. In several places throughout the text, we show and discuss the entire range of data for both organizations (2004-2009 for Verizon, 2007-2009 for the USSS). No small amount of internal discussion took place regarding how best to present statistics on the combined Verizon-USSS dataset. In the end, we decided that its most compelling feature was not simply the ability to compare and contrast Verizon's cases with those of the USSS but rather the opportunity to study a more representative sample. Therefore, the chosen approach is to present the combined dataset intact and highlight interesting differences (or similarities) within the text where appropriate. There are, however, certain data points that were collected by Verizon but not the USSS; these are identified in the text/figures.

As was the case in our last report, about two-thirds of the breaches covered herein have either not yet been disclosed or never will be. Many were related in some manner (i.e., same perpetrators or source IP). So far, almost 15% of Verizon's 2009 cases led to known arrests while 66% of USSS cases resulted in the arrest of a suspect. Even more impressive is that most of those ended in a conviction.

With the addition of Verizon's 2009 caseload and data contributed from the USSS, the DBIR series now spans six years, 900+ breaches, and over 900 million compromised records.

The figures in this report utilize a consistent format. Values shown in **dark gray** pertain to breaches while values in red pertain to data records. The "breach" is the incident under investigation in a case and "records" refer to the amount of data units (files, card numbers, etc.) compromised in the breach. Figures and tables do not always contain all possible options but only those having a value greater than 0. If you are interested in seeing all options for any particular figure, these can be found in the VERIS framework.

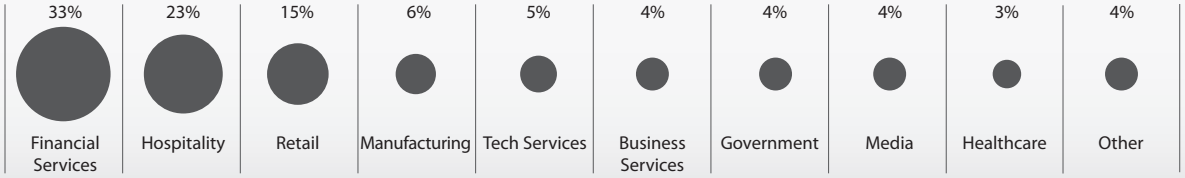
Without further delay, we present the investigative findings and analysis of Verizon and the USSS.

8 Refer to the Methodology section for an explanation of the qualification process.

Demographics

Of all sections in this report, demographics always present the greatest challenge for drawing out deeper meaning behind the numbers. While attack trends, incident response metrics, and other results are certainly dependent upon a given year's caseload, demographic data seem particularly so. Does the fact that we have more/less of a particular industry or region mean it is under increased attack? Is it more vulnerable? Did laws or other environmental factors change? Sheer coincidence? Obviously, it's difficult to know for certain. Demographic information is helpful, though, in establishing the context for other results. Thus, in this section we will relay the statistics, infer what we can, and let you do the rest.

Figure 1. Industry groups represented by percent of breaches



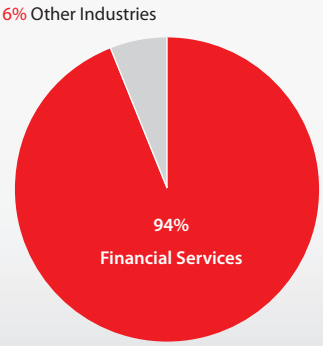
Data breaches continue to occur (in our caseload and elsewhere) within all types of organizations. These are categorized as they have been in previous reports according to the industry groups represented in Figure 1[9]. Financial Services, Hospitality, and Retail still comprise the "Big Three" of industries affected (33%, 23%, and 15% respectively) in the merged Verizon-USSS dataset, though Tech Services edged out Retail in Verizon's caseload. That this is consistently true of both the Verizon and USSS caseloads does seem to carry some significance.

The targeting of financial organizations is hardly shocking; stealing digital money from information systems rather than vaults is basically just a less primitive form of bank robbery. It represents the nearest approximation to actual cash for the criminal. Also, and perhaps more importantly, financial firms hold large volumes of sensitive consumer data for long periods of time. For this reason (and others), they fall under more stringent regulation and reporting requirements. This, in turn, increases the likelihood that breaches will require criminal and/or forensic investigation. In short, where other industries might be able to "sweep it under the rug," financial institutions are finding it increasingly difficult to do so. Regardless of the root cause(s), a growing percentage of cases and an astounding 94% of all compromised records in 2009 were attributed to Financial Services.

9 There are some changes in the way we categorize industries in this report. Most notably, "Food and Beverage" has been folded into the "Hospitality" group as this seems to be standard convention. A complete list of industries can be found in the VERIS framework.

The Hospitality and Retail industries exhibit similar trends when it comes to data breaches, which has a lot to do with their acceptance of payment cards and use of Point of Sale (POS) systems. This tends to draw a certain breed of criminal who favors certain ways and means of attack. There were quite a few public breach disclosures within the Hospitality industry in the last year or so and this spilled over into investigations conducted by Verizon and the USSS. Not surprisingly, restaurants and hotels comprise the bulk of cases in this industry group. Retail, which ranked first in total breaches in our last two reports, has fallen to third place and now accounts for less than half of its former glory (31% in '08 down to 14% in '09). This is not simply a by-product of incorporating USSS data (our own percentage for Retail was an even lower 9%) but we find it hard to attribute much more to these numbers than their face value.

Figure 2. Compromised records by industry group

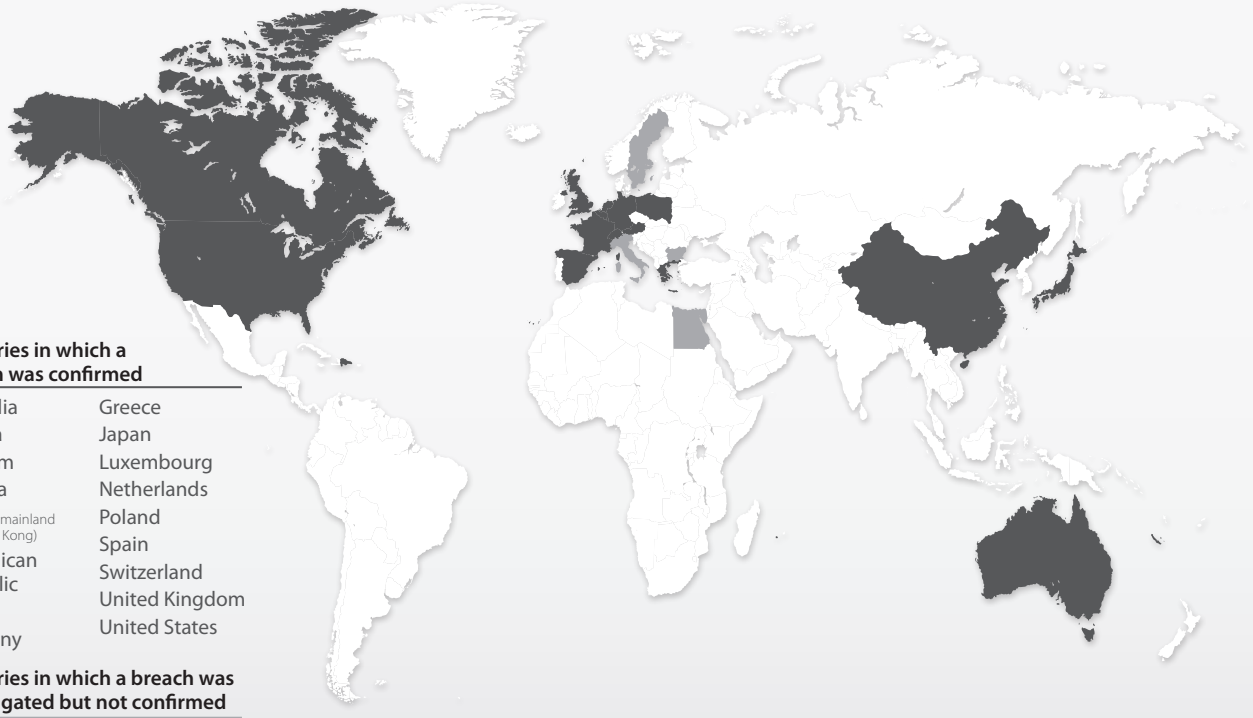


For regional trends, it's worth making a distinction between the USSS and Verizon datasets. The USSS caseload, as one might suspect, is comprised of nearly all breaches that occurred in the United States (though investigating and prosecuting these crimes takes them all around the world). On the other hand, over half of the breaches investigated by Verizon in 2009 occurred outside the U.S. (the "North America" region includes cases from Canada and the Dominican Republic). Countries in which Verizon investigated confirmed and suspected breaches are highlighted in Figure 3. Over the past two years our caseload has consistently grown in Asia-Pacific and Western European countries. It is unclear as to whether our expanded international IR team or changes in global incident trends are most responsible for this but other sources suggest growth in these regions as well.

The targeting of financial organizations is hardly shocking; stealing digital money from information systems rather than vaults is basically just a less primitive form of bank robbery. It represents the nearest approximation to actual cash for the criminal.

The apparent disparity between the number of known data breaches in the United States and other parts of the globe has led some to conclude that other parts of the world are safer environments for electronic business. We do not believe this to be the case. The same basic information and communication technologies are present in homes, businesses, and governments all around the world. Admittedly, there are some differences that have an impact on cybercrime (the Chip and PIN payment infrastructure is a good example) but these differences are not enough to explain the disparity. The primary reason we hear more about data breaches in the U.S. (and in the report) stems from mandatory disclosure laws. Outside the U.S., breach disclosure differs significantly. Some countries are silent on the matter, others encourage it but don't require, and some even discourage disclosure.

Figure 3. Countries represented



Countries in which a breach was confirmed

Australia
Austria
Belgium
Canada
China (mainland and Hong Kong)
Dominican Republic
France
Germany
Greece
Japan
Luxembourg
Netherlands
Poland
Spain
Switzerland
United Kingdom
United States

Countries in which a breach was investigated but not confirmed

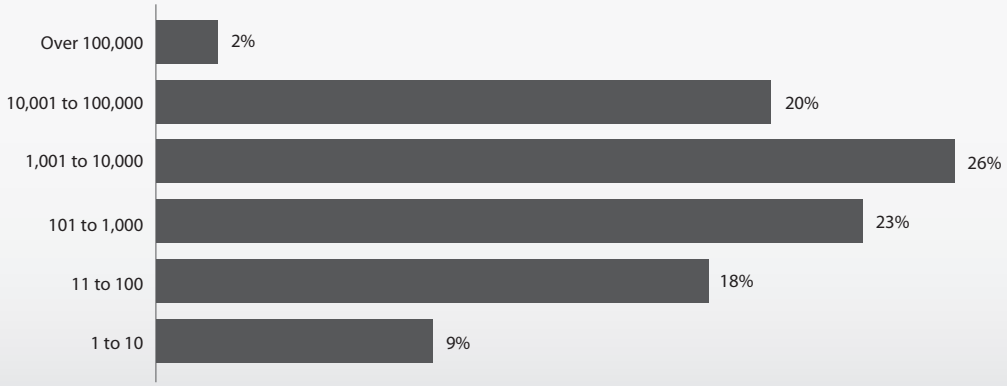
Bulgaria
Egypt
Italy
Singapore
Sweden

The bottom line is that where disclosures occur, they often require investigations, which sometimes require external investigators, which, in turn, means breaches are more likely to show up in this study. As in previous years, the majority of cases investigated by Verizon in 2009 have not yet been disclosed and may never be. Only a handful of breaches outside the U.S. were publicly reported. Of those, two did so because they were regional facilities of U.S.-based organizations.

Figure 4 shows that, once again, a breakdown of organizational size follows a rather normal-looking distribution. It's quite possible (and perhaps logical) that an organization's size matters little in terms of its chances of suffering a data breach. One might speculate that smaller budgets mean less security spending but it probably also means fewer assets to protect and a lower profile. Thieves are more likely to select targets based on the perceived value of the data and cost of attack than victim characteristics such as size.

Over half of the breaches investigated by Verizon in 2009 occurred outside the U.S.

Figure 4. Organizational size by percent of breaches (number of employees)



Many of our customers express concern about the security ramifications of mergers, acquisitions, and other major organizational changes (perhaps even more so than normal given economic conditions in recent years). This is understandable as these changes bring together not only the people and products of separate organizations but their technology environments as well. Seamless integration of technology, process, and mind-set certainly has its fair share of challenges. Last year, we reported that 13% of our caseload involved organizations that had recently been involved in a merger or acquisition. In 2009 that figure was 9% and another 9% had restructured in some significant way. While nothing can be claimed or inferred directly from these findings, we believe it is well worth watching this metric over time.

Threat Agents

Threat agents refer to entities that cause or contribute to an incident. There can be more than one agent involved in any incident and their involvement can be malicious or non-malicious, intentional or accidental, direct or indirect. Identifying those responsible for a breach is critical to any forensic investigation, not only for purposes of response and containment, but also for creating current and future defensive strategies. Verizon recognizes three primary categories of threat agents—External, Internal, and Partner.

External: External threats originate from sources outside the organization and its network of partners. Examples include hackers, organized crime groups, and government entities, as well as environmental events such as weather and earthquakes. Typically, no trust or privilege is implied for external entities.

VERIS Classification Note: If the agent's role in the breach is limited to a contributory error (see note in the Threat Actions section under Error), they would not be included here. For example, if an insider's unintentional misconfiguration of an application left it vulnerable to attack, the insider would not be considered an agent if the application were successfully breached by another agent. An insider who deliberately steals data or whose inappropriate behavior (i.e., policy violations) facilitated the breach would be considered an agent in the breach.

Internal: Internal threats are those originating from within the organization. This encompasses company executives, employees, independent contractors (i.e., 1099 staff), and interns, etc., as well as internal infrastructure. Insiders are trusted and privileged (some more than others).

Partners: Partners include any third party sharing a business relationship with the organization. This includes suppliers, vendors, hosting providers, outsourced IT support, etc. Some level of trust and privilege is usually implied between business partners.

Figure 5. Threat agents (inclusive) by percent of breaches

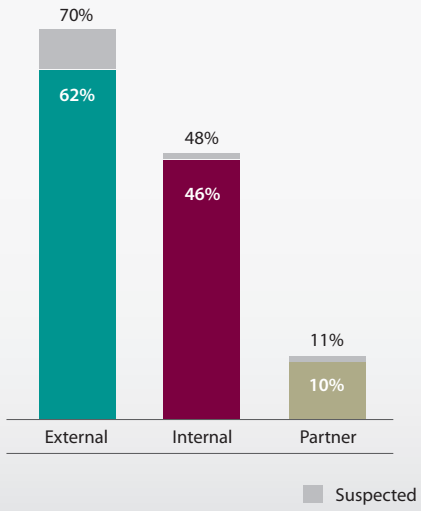


Figure 5 records the distribution of threat agents among breach cases worked by Verizon and the USSS in 2009. Immediately noticeable is a substantial change in the composition of threat agents from previous DBIRs. While these results don't go so far as to justify the "80% Myth[10]" they certainly don't fall in line with the 80/20 external vs. internal ratio that has been a staple of Verizon's caseload. The percentage of breaches attributed to external agents slid 9% (though 70% is not an historical outlier), insiders more than doubled, and partners represent a mere third of their 2008 level. That's a lot of change to digest but this section is dedicated to sorting it all out.

Essentially, there are three possible explanations for these results:

1. They reflect changes in Verizon's caseload
2. They reflect the addition of USSS caseload
3. They are a product of both 1 & 2

We will start with option 1. Figure 6 shows the distribution of threat agents for breaches worked by Verizon over the last five years. From this, it is clear that the lower proportion of external agents is not due to Verizon's caseload, as this statistic hit its highest mark ever in 2009. Neither can it explain the rise for insiders in the merged dataset. The percent of breaches involving partners, however, did drop substantially and for the second year in a row. It is unclear whether this is due to increased awareness of third-party security threats, regulatory guidance focusing on vendor management, a shift in criminal strategy, a change in Verizon's IR clients, all of the above, or none of the above. Whatever the reason(s), we view it as a positive outcome and hope this problem is being reigned in.

The changes evident for threat agents in 2009 stem partially from a drop in partners within Verizon's caseload but mostly from the addition of a materially different USSS dataset.

10 http://taosecurity.blogspot.com/2009/05/insider-threat-myth-documentation.html

Figure 6. Threat agents over time by percent of breaches

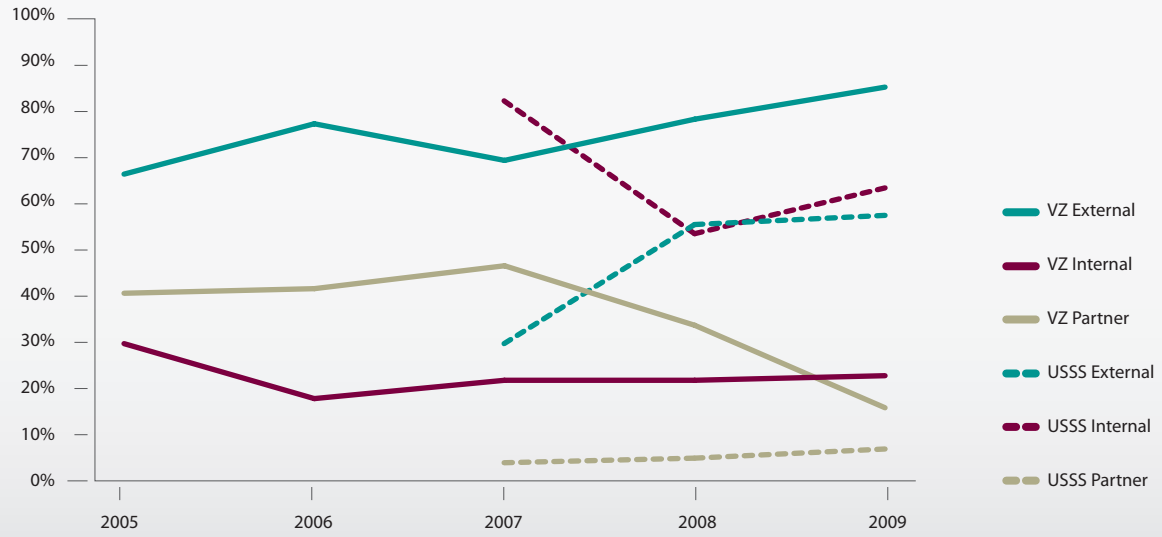
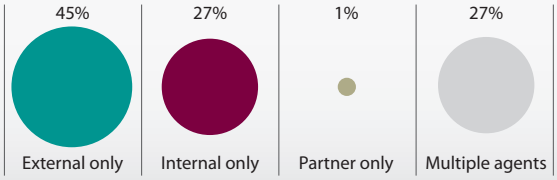


Figure 6 also shows the same information discussed in the preceding paragraph for USSS cases (see dashed lines). Undoubtedly, the changes in Figure 5 are largely due to the inclusion of the USSS caseload, as their results show a strong representation of internal threat agents, comparatively fewer outsiders, and a very low percentage of partner-related breaches. As a law enforcement agency, it would follow that the USSS would have a different perspective on the broader security incident population. For example, an organization suffering a data breach due to the actions of an insider (especially if that insider is part of an easily-identified list of suspects or used simple methods to perpetrate the crime) is more likely to call law enforcement directly. If true, this would reinforce the assertions and findings of some, especially law enforcement agencies, that insiders are a more frequent source of incidents than stats released by external parties like Verizon often show. In addition, it's also important to consider the impact of disclosure laws on the proportions represented in the various datasets.

So, if #1 has some truth to it and #2 is wholly true, then #3 must be the best option. The changes evident for threat agents in 2009 stem partially from a drop in partners within Verizon's caseload but mostly from the addition of a materially different USSS dataset. As stated in the beginning of this report, our motivation in studying a larger sample is to better understand the biases of our own and to gain a more complete and accurate representation of the entire population of breaches. These results are clearly the product of that larger perspective.

Figure 7. Threat agents (exclusive) by percent of breaches



Following this discussion, there are a few observations to note regarding Figure 7 which contrasts single and multi-agent breaches. The 27% of cases involving more than one agent is well below the 2008 level of 39%. Though not apparent from the figure itself, most multi-agent breaches worked by Verizon exhibit an external-partner combination. In most of these, partner assets are compromised by an external agent and used to attack the victim. On the other hand, external-internal is far more common in USSS cases. As will be discussed later in this report, this scenario often involves an outsider soliciting or bribing an employee to embezzle or skim data and/or funds. Partner-internal pairings are rare within both caseloads.

Breach Size by Threat Agents

Though we do not assert that the full impact of a breach is limited to the number of records compromised, it is a measurable indicator of it. Analysis around financial losses incurred by breach victims is probably the most requested addition to the DBIR. For various reasons[11], forensic investigators do not have nearly as much visibility into this as they have into the immediate details surrounding a breach. We do, however, include metrics for collecting impact data within VERIS and refer interested readers there for more information.

Figure 8. Compromised records by threat agent, 2009

Figure 9. Compromised records by threat agent, 2004-2009

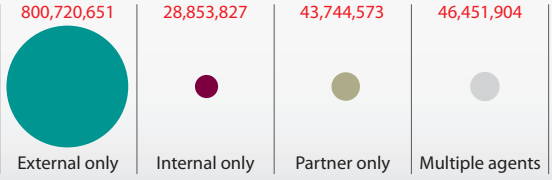


Figure 8 records the distribution of the 143+ million records compromised across the merged 2009 dataset among threat agents. It looks a great deal like it did in our last DBIR. There is not a linear relationship between frequency and impact; harm done by external agents far outweighs that done by insiders and partners. This is true for Verizon and for the USSS and true for this year and in years past. To illustrate this point, we present Figure 9 showing the distribution of the over 900 million compromised records in the merged dataset between 2004 and 2009.

We could provide commentary to Figure 9, but what could it possibly add? If a chart in this report speaks with more clarity and finality we aren't sure what it is.

We could provide commentary to Figure 9, but what could it possibly add? If a chart in this report speaks with more clarity and finality we aren't sure what it is.

11 http://securityblog.verizonbusiness.com/2009/04/16/to-dbir-show-me-the-money/

External Agents (70% of breaches, 98% of records)

Table 1 presents a comparison of the various types of external threat agents identified during 2009 by Verizon and the USSS. The merged results continue to show that external breaches are largely the work of organized criminals. Banding together allows them to pool resources, specialize skills, and distribute the work effort, among other advantages. Figure 10 demonstrates the effectiveness of this approach. Crime has been a business for a very long time. This is just the same old story played out on a different (digital) stage. We refer readers to Appendix A for more information on organized criminal communities.

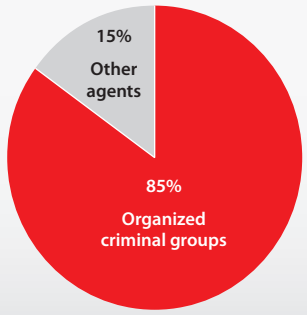
The large proportion of "unknown" in Table 1 is the result of several factors. Sometimes the particular type of agent cannot be determined. Sometimes the victim does not wish to spend time or money toward making this determination. The USSS contains far fewer "unknown" agents due to their role in identifying and prosecuting suspects.

In terms of the role external agents played in 2009 breaches, 84% participated directly in the attack. The rest solicited another agent to perpetrate the attack or supported it in some other manner. Scenarios of this are discussed elsewhere in this report.

Table 1. Types of external agents by percent of breaches within External

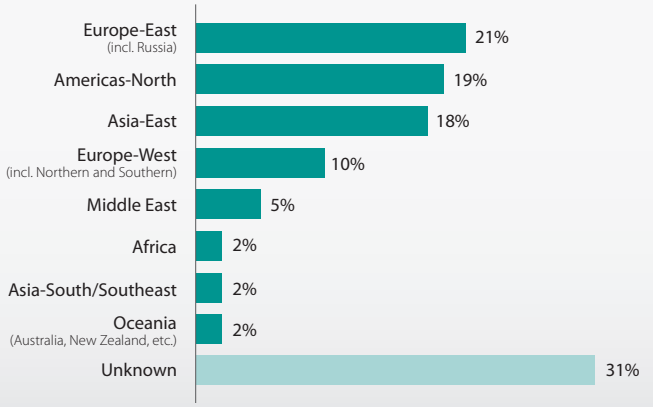
Organized criminal group	24%
Unaffiliated person(s)	21%
External system(s) or site	3%
Activist group	2%
Former employee (no longer had access)	2%
Another organization (not partner or competitor)	1%
Competitor	1%
Customer (B2C)	1%
Unknown	45%

Figure 10. Percent of compromised records attributed to organized crime



Banding together allows criminal groups to pool resources, specialize skills, and distribute the work effort, among other advantages. Crime has been a business for a very long time. This is just the same old story played out on a different (digital) stage.

Figure 11. Origin of external agents by percent of breaches within External



Pinpointing the geographic origin of these attacks can be problematic, especially when it hinges mainly on source IP addresses. Fortunately, forensic investigators—and especially law enforcement agencies—often have much more to go on than that. Even if we accept that the IP address that shows up in log files does not belong to the actual machine of the actual threat agent (i.e., it is a bot controlled by the agent), it is still informative and potentially useful for defensive purposes. Figure 11 shows the regional origin of relevant external attacks.

Once again, more breaches originate from East Europe than any other region (although North America and East Asia remain a close #2 and #3). Comparing "type" and "origin" reveals some interesting findings. For instance, most organized criminal groups hail from East Europe, while unidentified and unaffiliated persons often come from East Asia. Finally, it is worthy of mention that within Verizon's caseload, East Asia rose to the top spot for the first time in 2009.

THERE MUST BE SOME MISTAKE—WHERE'S APT?

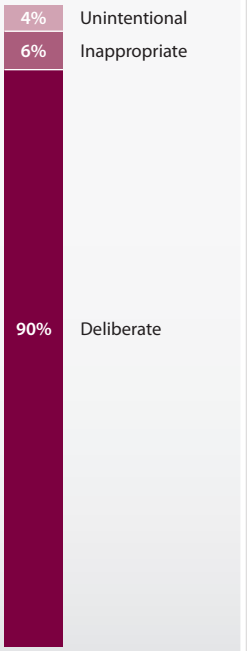
Despite the huge amount of buzz around Advanced Persistent Threats (APT) this year, neither the term nor the concept is new. Due to this attention, we imagine more than one pair of eyes scanned the list of external agent types in search of "APT." One of the difficulties with APT is that, though it may have an official definition, its use in everyday practice varies widely. By it, some refer strictly to nation-states, some to any highly skilled attacker, some to particularly difficult methods of attacks or their unrelenting nature. We're not interested in arguing about the definition. We simply want to explain why it is not listed in any figure or table in this report. Rather than identifying an "APT attack," VERIS classifies threat agents and their actions in a descriptive manner. If interested, you can see glimpses of "APT-ish elements" throughout this report. Look at the types and origins of external agents (note the absence of the "government" category that is an available option in VERIS), examine the types and vectors of threat actions, read our assessments of attack difficulty, notice the length of time that passes from compromise to discovery, and check out the anti-forensics section. These areas might not be stamped with the acronym "APT" but we do believe them to "apt-ly" describe breaches investigated by Verizon and the USSS in 2009.

Internal Agents (48% of breaches, 3% of records)

Of cases involving internal threat agents in 2009, investigators determined 90% were the result of deliberate and malicious activity. This finding does not mean that insiders never unintentionally contribute to breaches; they very often do. As discussed earlier, our method of classification does not consider insiders to be an active part of the event chain if their role is limited to contributory error. Inappropriate actions include policy violations and other questionable behavior that, while not overtly malicious, can still result in harm to information assets. Not only can inappropriate behavior contribute directly to a breach, but it may also be an ill omen of what's to come. Over time investigators have noticed that employees who commit data theft were often cited in the past for other "minor" forms of misuse (or evidence of it was found and brought to light during the investigation).

Recently, many have hypothesized that insider crime would rise due to financial strain imposed by global economic conditions. Hard times breed hard crimes as they say. It is entirely possible that this is occurring, but neither the Verizon nor USSS caseload show evidence of it. As seen back in Figure 6, Verizon shows a flat trend for insiders and the USSS shows a downward trend over the last three years. Nevertheless, it is a logical hypothesis and worthy of further study.

Figure 12. Role of internal agents by percent of breaches within Internal



Analyzing the types of insiders behind breaches yields a great deal of practical information. Each of the types listed in Table 2 represent a certain inherent mix of skills, duties, privileges, etc., all of which speak to the capabilities and resources of that agent and the safeguards most relevant to them. Traditionally, we have seen a large and fairly even proportion of system/network administrators to regular users with a few other types mixed in occasionally. 2009 results are substantially different and, no surprise, this is largely due to USSS data. Specifically, it is related to the types of internal crime investigated by the USSS (see the Misuse section under Threat Actions for a more detailed discussion). As a result, regular employees were responsible for a much larger share (51%) of breaches. These cases typically involved bank tellers, retail cashiers, and other similar personnel taking advantage of their everyday job duties to skim, embezzle, or otherwise steal data from their employers.

Recently, many have hypothesized that insider crime would rise due to financial strain imposed by global economic conditions. Hard times breed hard crimes as they say. It is entirely possible that this is occurring, but neither the Verizon nor USSS caseload show evidence of it.

Finance and accounting staff are similar to regular employees in terms of IT privileges but we differentiate them due to the higher privileges of another sort. Their oversight and management of accounts, records, and finances affords them great propensity for harm. Executives are in a similar position. Though outside the scope of this study, devious acts committed by such employees have caused far more damage to businesses than IT-related incidents.

While it is clear that pulling off an inside job doesn't require elevated privileges, evidence consistently supports that they do facilitate the bigger ones. Overall, insiders were not responsible for a large share of compromised records but system and network administrators nabbed most of those that were. This finding is not surprising since higher privileges offer greater opportunity for abuse. In general, we find that employees are granted more privileges than they need to perform their job duties and the activities of those that do require higher privileges are usually not monitored in any real way.

Table 2. Types of internal agents by percent of breaches within Internal

Regular employee/end-user	51%
Finance/accounting staff	12%
System/network administrator	12%
Executive/upper management	7%
Helpdesk staff	4%
Software developer	3%
Auditor	1%
Unknown	9%

It is worth noting that while executives and upper management were not responsible for many breaches, IP and other sensitive corporate information was usually the intended target when they were. These acts were often committed after their resignation or termination.

Speaking of that, across all types of internal agents and crimes, we found that 24% was perpetrated by employees who recently underwent some kind of job change. Half of those had been fired, some had resigned, some were newly hired, and a few changed roles within the organization. With respect to breaches caused by recently terminated employees, we observed the same scenarios we have in the past: 1) the employee's accounts were not disabled in a timely manner, and 2) the employee was allowed to "finish the day" as usual after being notified of termination. This obviously speaks to the need for termination plans that are timely and encompass all areas of access (decommissioning accounts, disabling privileges, escorting terminated employees, forensic analysis of systems, etc.).

THE SLIPPERY SLOPE OF INSIDER MISCONDUCT

Verizon investigated a case in which a recently terminated system administrator stole sensitive data from his former employer as well as personal information belonging to its customers. He then attempted to blackmail the organization and threatened to go public with the information if they did not meet his demands. Obviously, not a good situation but what makes it worse is that it might have been avoided with a few changes in policy and practice. On several occasions in the past, this employee had been cited for IT policy violations and inappropriate behavior. There were harassment complaints against him filed by other employees. Finally, when he stole a co-worker's password for a popular social networking site and modified it with slanderous content, he was let go. Unfortunately, his generic administrative account was given to his successor with a minor password change (i.e., "Password2" instead of "Password1") and we've already covered what happened after that.

Partner Agents (11% of breaches, 1% of records)

As discussed already, partner-related breaches are down in comparison to previous years. When partners are a factor, the Verizon and USSS cases have differing perspectives as to their role. Verizon's findings continue to show that the majority of breaches involving partners are the result of third-party information assets and accounts being "hijacked" by another agent and then used to attack victims. This frequently involves a remote access connection into the victim's systems. If compromised, the malicious agent's actions would appear to come from a trusted source and therefore be even more difficult to detect and prevent. Poor partner security practices usually allow or worsen these attacks.

Organizations that outsource their IT management and support also outsource a great deal of trust to these partners. In the end, what we said last year remains true; poor governance, lax security, and too much trust is often the rule of the day. Outsourcing should not mean "Out of sight, out of mind."

Figure 13. Role of partner agents by number of breaches within Partner

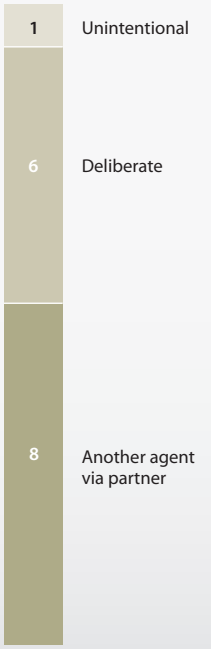


Table 3. Types of partner agents by number of breaches within Partner

Remote IT management/support	7
Data processing and analysis	1
Hosting provider	1
Onsite IT management/support	1
Security services/consulting	1
Shipping/logistics provider	1
Unknown	3

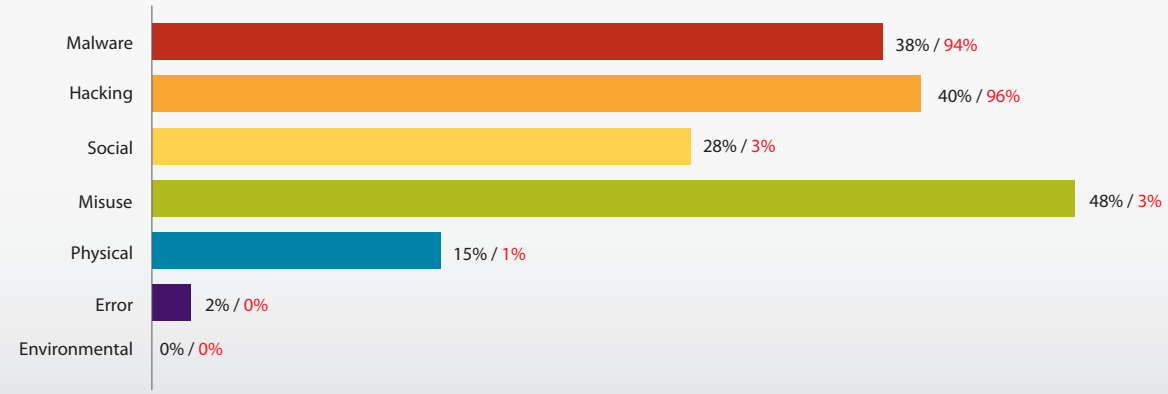
The USSS caseload, on the other hand, shows most partner breaches stem from the deliberate and malicious actions of that partner. An example of this might be a third-party system administrator who maliciously misuses her access to steal data from the victim. We believe that the merged data set balances these two extremes to arrive at the ratio shown here.

The types of partners in each dataset parallel the differences described above. Partners that manage systems are by far the most common offenders, whether their role is accidental or deliberate. Assets often involved in these breaches are point-of-sale systems within the hospitality and retail industries. Organizations that outsource their IT management and support also outsource a great deal of trust to these partners. In the end, what we said last year remains true; poor governance, lax security, and too much trust is often the rule of the day. Outsourcing should not mean "Out of sight, out of mind."

Threat Actions

Threat actions describe what the threat agent did to cause or contribute to the breach. There are usually multiple actions across multiple categories during a breach scenario. Verizon uses seven primary categories of threat actions, which are depicted in Figure 14 along with the percent of breaches and compromised records associated with each.

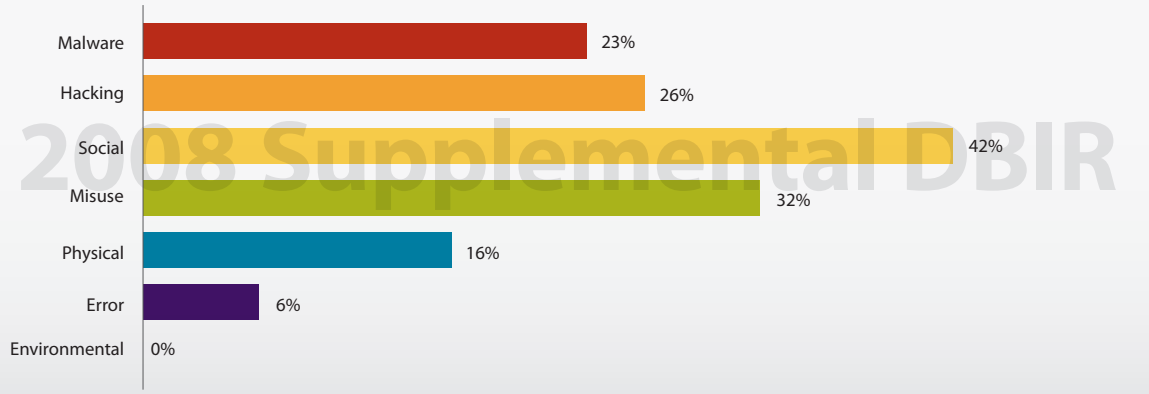
Figure 14. Threat action categories by percent of breaches and records



As with the findings for threat agents, we imagine Figure 14 raises some eyebrows among those familiar with previous versions of this report. Before going any further, we'd like to direct attention to Figure 15 to see if we can turn some of those raised eyebrows into head nods and an "ah-ha" or two. In the 2008 Supplemental DBIR, we presented all the same basic statistics as in the original report except sliced up by industry. Figure 15 shows the prevalence of threat actions in Financial Services from that report. Though by no means a mirror image of Figure 14, it does demonstrate that a dataset containing a large proportion of financial organizations will exhibit a more "balanced" mix of threat actions and higher values in the Misuse and Social categories. On the other hand, the Retail and Hospitality industries are very lopsided toward Hacking and Malware. Therefore, Figure 14 is not a new trend or sudden change in the threat environment. It aligns perfectly well with what we would expect of a merged Verizon-USSS dataset that contains a higher-than-normal proportion of financial organizations.

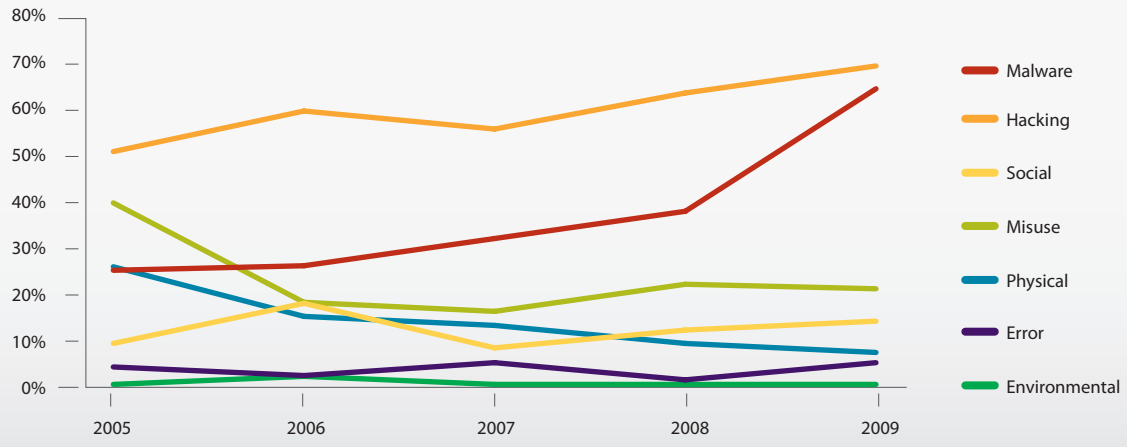
This is quite a sobering statistic but one that adds yet another chapter to a story we already know: In the big breaches, the attacker hacks into the victim's network (usually by exploiting some mistake or weakness) and installs malware on systems to collect (lots of) data. That the USSS cases tell the same story certainly makes it more compelling though.

Figure 15. Flashback: Threat action categories by percent of breaches in Financial Services as shown in the 2008 Supplemental DBIR



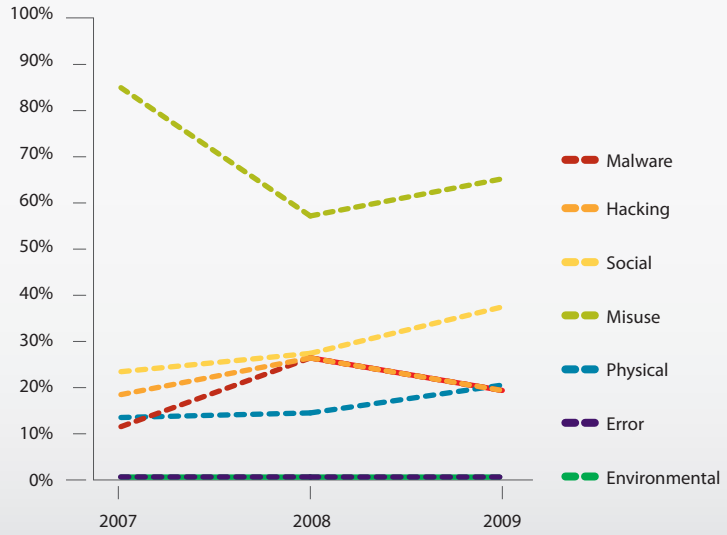
Though less prevalent than in previous reports, Hacking and Malware are even more dominant than normal with respect to compromised records. This is quite a sobering statistic but one that adds yet another chapter to a story we already know: In the big breaches, the attacker hacks into the victim's network (usually by exploiting some mistake or weakness) and installs malware on systems to collect (lots of) data. That the USSS cases tell the same story certainly makes it more compelling though.

Figure 16. Threat action categories over time by percent of breaches (Verizon cases)



Those wishing to compare 2009 results to previous years for Verizon's caseload can do so in Figure 16. Another version of the same chart is provided for the three years for which we have data from the USSS *(Figure 17)*. The most noticeable change in 2009 among breaches worked by Verizon was a substantial upswing in malware. For the most part, USSS trends held steady, with Social and Misuse showing some growth while Hacking and Malware declined slightly. The following sections provide a more in-depth analysis of each threat action category.

Figure 17. Threat actions over time by percent of breaches (USSS cases)



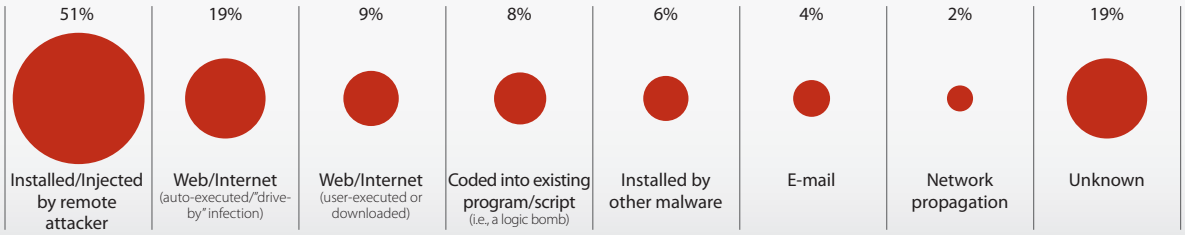
Malware (38% of breaches, 94% of records)

Malware is any software or code developed for the purpose of compromising or harming information assets without the owner's informed consent. It factored into 38% of 2009 cases and 94% of all data lost. When malware is discovered during an investigation, the IR team often works with ICSA Labs, an independent division of Verizon, to conduct the analysis. Through this collaboration, investigators are able to better help the customer with containment, removal, and recovery. Malware can be classified in many ways but we utilize a two-dimensional approach that identifies how it was distributed (infection vector) and what the malware did (functionality). These characteristics have a direct bearing on preventive measures.

Infection Vectors

Per Figure 18, the most frequent malware infection vector is once again installation or injection by a remote attacker. This is often accomplished through SQL injection or after the attacker has root access to a system. Both have the troublesome ability to evade antivirus (AV) software and other traditional detection methods, which has a lot to do with their consistent place at the top of this list.

Figure 18. Malware infection vectors by percent of breaches within Malware



The web continues to be a common path of infection. Among web-based malware, we distinguish auto-executed "drive-by downloads" from those involving user interaction. Many of the latter incorporate a social engineering aspect ("click to clean your system"). The web installation vector is more opportunistic in nature than the "installed by attacker" variety that usually targets a pre-selected victim. Once the system is infected, the malware alerts an external agent who will then initiate further attacks. The web is a popular vector for the simple reason of that's where the users are. Overly-trusting browsers and users operating with administrative privileges only add to this popularity.

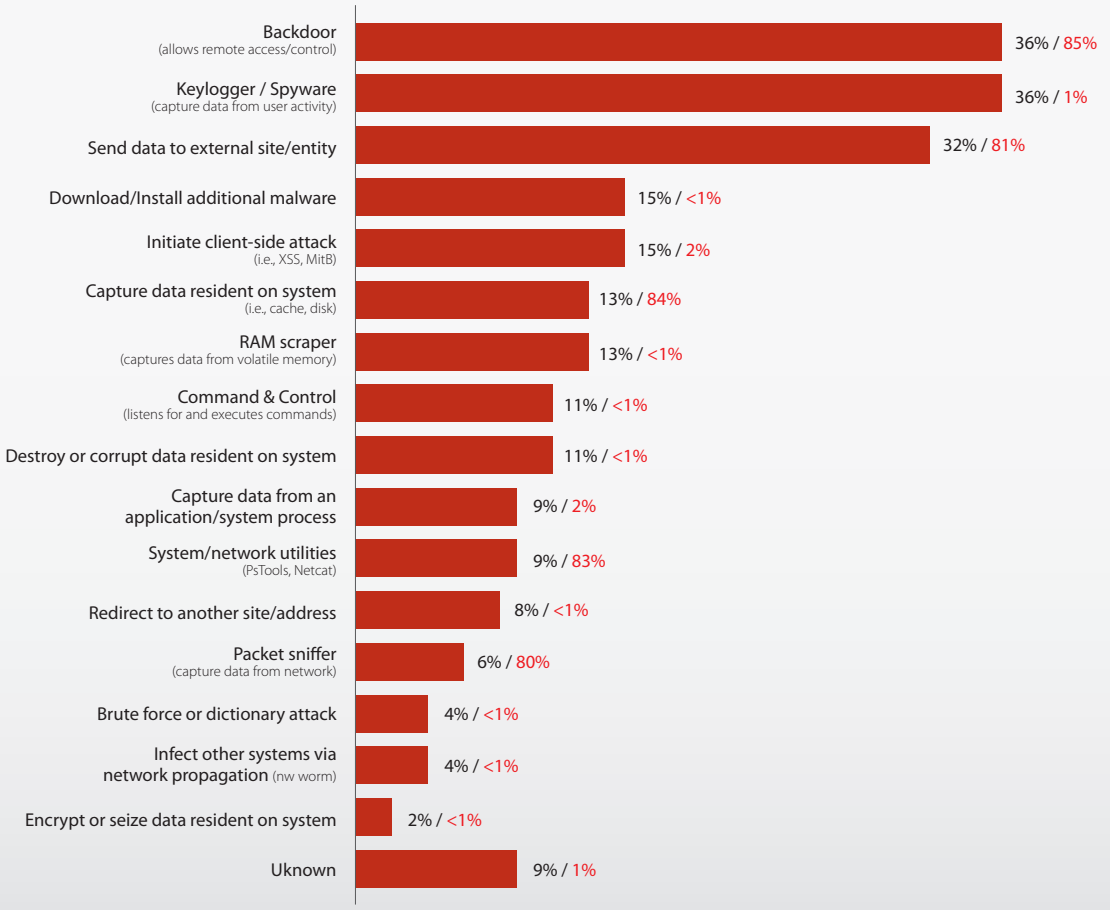
While not extremely common, we did observe several cases in which malware was coded directly into an existing program or script. This, of course, requires access to the system but also knowledge of how the code works. Not surprisingly, these often involve malicious insiders who developed the code or administer the system on which it runs. However, a few very interesting cases of this type were committed by outsiders. One of these involved an external agent that had access to the system for over six months. During this time, he studied the input/output process and developed a custom script to siphon data when new accounts were created.

The rather high percentage of "unknown" in Figure 18 is attributable to many factors. Many times there were no logs, corrupted evidence, and/or users were unavailable for interview. Occasionally, we see some of the "old school" infections vectors like e-mail and network propagation. Outside the world of data breaches, these are still alive and well but when stealth is critical and persistence is the goal, these vectors have less merit.

Malware Functionality

To better capture the intricacies of modern malware, we have defined a more detailed set of functions in the VERIS framework than in previous years. At a broad level though, malware still serves three basic purposes in data breach scenarios: enable or prolong access, capture data, or further the attack in some manner.

Figure 19. Malware functionality by percent of breaches within Malware and percent of records



In terms of enabling access, backdoors were logically atop the list again in 2009 (tied with keyloggers). Backdoors allow attackers to come and go as they please, install additional malware, wreak havoc on the system, retrieve captured data, and much more. Their effectiveness is evidenced by the large percentage of data loss involving backdoors.

Criminals are also getting more proficient and prolific in developing methods to capture data. This can be seen in Figure 19, where many of the functions listed focus on this. Keyloggers and spyware that record user activity were frequent but not involved in some of the larger cases in 2009. This is quite a change from 2008 where they were associated with over 80% of data compromised. "Associated" is the operative word here as keyloggers don't usually steal the bulk of data themselves but instead are used to gain access to install other types of malware for that purpose (i.e., packet sniffers). When malware captures

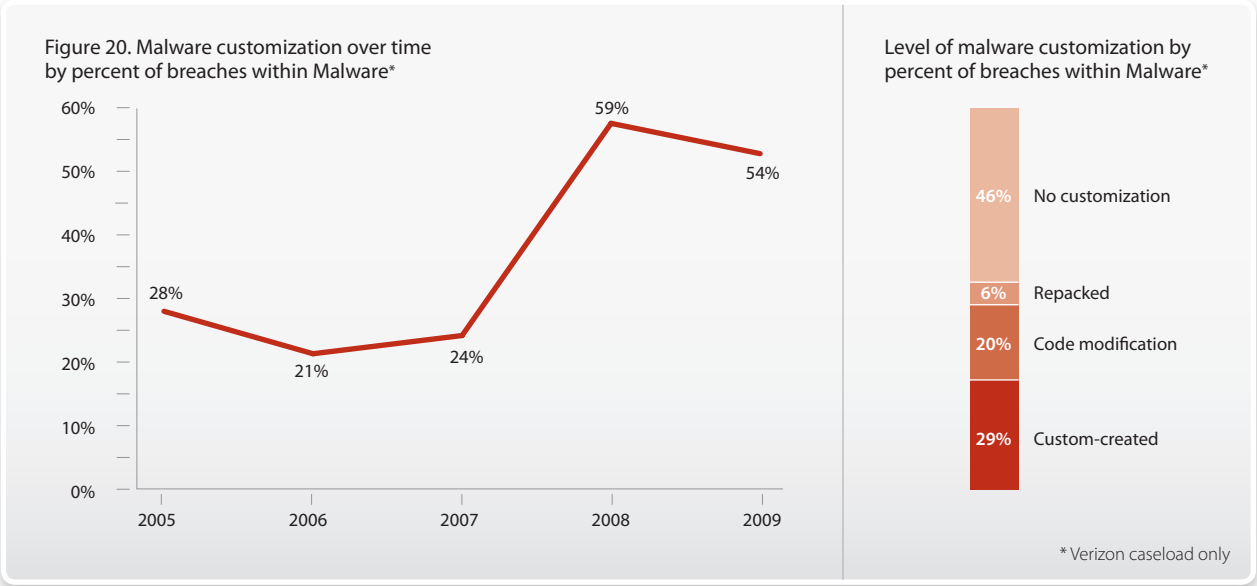
data on the system (13% of cases), it often does so from forms that cache credentials and other sensitive info. Though only used in some of the smaller cases in 2009, the use of "RAM scrapers" to capture data from a system's volatile memory, continues to increase (13%). We refer the reader to our 2009 Supplemental DBIR for more information on this type of malware. Packet sniffers, while not as common as other varieties of malware, continue to compromise large numbers of records and are usually a factor in the bigger breaches. Malware that "Captures data from an application/system process" (9%) is often associated with the "Coded into existing program/script" infection vector discussed above.

The last major grouping of malware encompasses functions that facilitate the attack in some manner. As is evident, malware often sends data to an external entity (32%). This is sometimes stolen data (like credentials) but is also used to let an attacker know that a system is compromised. We also observed several cases in which malware was used to perform client-side attacks such as man-in-the-browser and cross-site scripting. When malware downloads additional code (15%), it is often in the form of updates or capability extensions. Attackers seem to have an affinity for system and network utilities like PsTools and Netcat. Though these tools are not inherently malicious, criminals are deploying and using them in that way. To clarify, if utilities were added to the system by an attacker, they are listed here under malware. If they were already on the system and were abused as a part of the attack, this would show up under Hacking (i.e., via OS Commanding). It is very interesting to note that there were no confirmed cases in which malware exploited a system or software vulnerability in 2009 (though it was suspected based on partial samples that three may have done so).

In terms of malware furthering the attack, our investigations continue to highlight the importance of detecting and responding to malware quickly. In some incidents, the affected company missed an opportunity to lessen the aftermath of infection by ignoring or not adequately investigating initial antivirus alerts. Regrettably, those alerts sound less often these days.

HOW DO THEY GET MY DATA OUT?

When malware captures sensitive information, it must then be exfiltrated from (or taken out of) the victim's environment. There are two basic ways this happens: either the malware sends it out of the organization or the attacker re-enters the network to retrieve it. The general rule of thumb is that smaller packets are sent out (i.e., credentials captured by keyloggers) while larger hauls of data are retrieved (i.e., data collected by a packet sniffer). While any amount of data leaving the owner's possession is never a good thing, the act does (or at least can) provide evidence of foul play. It's a matter of looking for the right indicators in the right places. We advocate paying attention to what goes out of your network and what changes take place within your systems. Don't have any customers or partners in Eastern Europe yet periodic bursts of traffic are sent there from your networks? What about those ZIP or RAR files that showed up last week and have been growing steadily ever since? Maybe there's a perfectly good explanation for these things…but you'll never know unless you take steps to identify and verify them.



Malware Customization

We are not so happy to say that the increase in customized malware we reported last year appears not to be a fluke limited to 2008. 2009 revealed a similar proportion of breaches (54% of those involving malware) and an incredible 97% of the 140+ million records were compromised through customized malware across the Verizon-USSS caseload.

The level of customization apparent in malware varies substantially. Some are simply repackaged versions of existing malware in order to avoid AV detection. From Figure 20, it is evident that many attackers do not stop there. More often than not in 2009, they altered the code of existing malware or created something entirely new. As an example of modified code, we observed several instances of RAM scrapers that were "last year's models" with a few tweaks like the added ability to hide and/or encrypt the output file of captured data. Over the last two years, custom-created code was more prevalent and far more damaging than lesser forms of customization.

An incredible 97% of the 140+ million records were compromised through customized malware across the Verizon-USSS caseload.

As a defender, it's hard not to get a little discouraged when examining data about malware. The attackers seem to be improving in all areas: getting it on the system, making it do what they want, remaining undetected, continually adapting and evolving, and scoring big for all the above. We are not, however, totally devoid of hope. A major improvement would be to keep attackers from ever gaining access to the system before they are able to install malware. This, of course, is not without its own challenges as will be discussed next.

Hacking (40% of breaches, 94% of records)

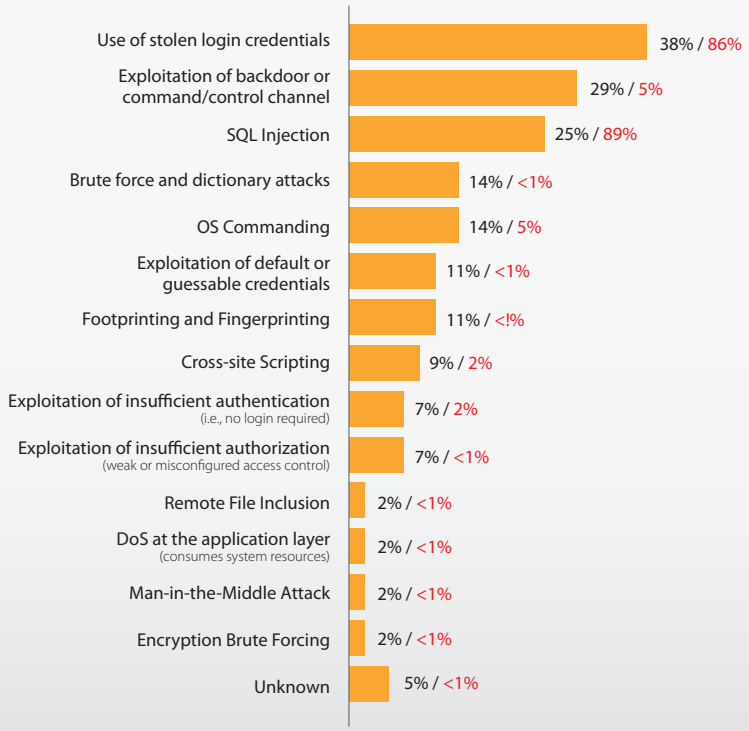
VERIS Classification Note: There is an action category for Hacking and for Misuse. Both can utilize similar vectors and achieve similar results; in Misuse, the agent was granted access (and used it inappropriately) whereas with Hacking access was obtained illegitimately.

Actions in the Hacking category encompass all attempts to intentionally access or harm information assets without (or in excess of) authorization by thwarting logical security mechanisms. Hacking affords the criminal many advantages over some of the other categories; it can be accomplished remotely and anonymously, it doesn't require direct interaction or physical proximity, and there are many tools available to automate and accelerate attacks. The latter lowers the learning curve and allows even less-skilled threat agents to cause a lot of trouble. In this section, we examine the types of hacking observed by Verizon and the USSS in 2009, the paths through which these attacks were conducted, and other details about this important category.

Types of Hacking

The attacks listed in Figure 21 will look a bit different to those familiar with previous DBIRs. The changes are due to our effort to standardize on a classification system for hacking methods in connection with the public release of VERIS. Internally, we had more freedom to simply describe what we observed in our caseload but in order for the USSS (and hopefully others) to use VERIS a more formal approach was necessary. The resulting list (which is not shown here in its entirety) is not exhaustive, as detailed as it could be, or perfect. It is, however, useful for most attacks and provides enough specificity for the intended purpose. It is derived from our own work and from open attack taxonomies from the Web Application Security Consortium (WASC), the Open Web Application Security Project (OWASP), and the Common Attack Pattern Enumeration and Classification (CAPEC) from Mitre. Cross-referencing these is not a quick, easy, or conflict-free process. The list of hacking types in VERIS uses the WASC Threat Classification v2.0 as a baseline[12] and pulls from the others to round out areas not addressed in WASC (i.e., non-application attacks). We refer users to the links above for definitions and examples.

Figure 21. Types of hacking by percent of breaches within Hacking and percent of records



12 Thanks to Jeremiah Grossman and Robert Auger from WASC for volunteering their time to serve as a sounding board on attack classification matters.

Evident from Figure 21, there are two standout types of hacking responsible for the majority of breaches and stolen records in 2009—SQL injection and the use of stolen credentials. Both were among the top offenders in our previous report but this year sees them at a whole new level.

The use of stolen credentials was the number one hacking type in both the Verizon and USSS datasets, which is pretty amazing when you think about it. There are over 50 types recognized in the VERIS framework—how can two completely different caseloads show the same result? We have our theories. One of the main reasons behind this is the proliferation of password-gathering malware like Zeus. In fact, though phishing, SQL injection, and other attacks can and do steal credentials, malware nabbed more than all others combined by a ratio of 2:1. There is much more discussion of this in the malware section. Stolen credentials offer an attacker many advantages, not the least of which is the ability to disguise himself as a legitimate user. Authenticated activity is much less likely to trigger IDS alerts or be noticed by other detection mechanisms. It also makes it easier to cover his tracks as he makes off with the victim's data.

Though phishing, SQL injection, and other attacks can and do steal credentials, malware nabbed more than all others combined by a ratio of 2:1.

SQL injection is a technique for controlling the responses from the database server through the web application. At a very high level, the attacker inserts another SQL statement into the application through the web server and gets the answer to their query or the execution of other SQL statements. SQL injection is almost always an input validation failure. If the application trusts user input and does not validate it at the server, it is likely to be vulnerable to SQL injection, cross-site scripting, or one of the other input-validation vulnerabilities. In data breach scenarios, SQL Injection has three main uses: 1) query data from the database, 2) modify data within the database, and 3) deliver malware to the system. The versatility and effectiveness of SQL Injection make it a multi-tool of choice among cybercriminals.

HAPPY 10TH BIRTHDAY SQL INJECTION!

Though first discussed publicly on Christmas Day in 1998, the first advisory on SQL injection was released in 1999. So, perhaps we should say "Happy (belated) 10th birthday" to one of the most widespread and harmful attack methods we've investigated over the years. However, we'd like to alter the customary birthday jingle tagline and instead hope that "not many more" will follow.

The secret to SQL injection's longevity and success is due to a combination of many factors. It's not a terribly difficult technique, making it available to a large pool of miscreants. It exploits the inherently necessary functions of websites and databases to accept and provide data. It can't be fixed by simply applying a patch, tweaking a setting, or changing a single page. SQL injection vulnerabilities are endemic, and to fix them you have to overhaul all your code. Needless to say, this is difficult and sometimes nigh impossible if it is inherited code. There are some tools to help, but it still comes down to coding and developer knowledge. Unfortunately, training gets cut when budgets get tight and application testing is forfeited or compressed to make up time in overdue development projects. All in all, not an easy concoction to swallow but just passing the cup isn't working either. The data in this report testify to the fact that there are many people on the Internet willing to do application testing for you if you don't. Let's pay the good guys instead and make sure SQL injection doesn't live through many more birthdays.

Exploitation of backdoors is another common method of network and system intrusion. In most cases a backdoor is created as a function of malware that was installed at an earlier stage of the attack. The agent then has control of or can access the system at will. It accomplishes the goals of concealment and persistence that cybercriminals crave. As in years past, we most often see backdoors utilized to exfiltrate data from compromised systems.

OS Commanding involves running programs or commands via a web application or through the command prompt after gaining root on a system. Obviously not a capability one wants to grant to an adversary. It can also be used to manipulate systems utilities such as PsTools and Netcat that are legitimately on a system or that have been placed there by the attacker.

What may be striking to many of our readers is the drop in "exploitation of default or guessable credentials" since our last report. This was the most common type in the Hacking category last year and responsible for over half of records breached. It was still fairly common in 2009 but associated with only a fraction of overall data loss (<1%). The drop seems to correspond with fewer cases in the Retail and Hospitality industries stemming from third party mismanagement of remote desktop connections to POS systems.

Vulnerability Exploits

In the past we have discussed a decreasing number of attacks that exploit software or system vulnerabilities versus those that exploit configuration weaknesses or functionality. That downward trend continued this year; so much so, in fact, that there wasn't a single confirmed intrusion that exploited a patchable[13] vulnerability. On the surface this is quite surprising—even shocking—but it begins to make sense when reviewing the types of hacking discussed above. SQL injection, stolen credentials, backdoors, and the like exploit problems that can't readily be "patched."

There wasn't a single confirmed intrusion that exploited a patchable[13] vulnerability.

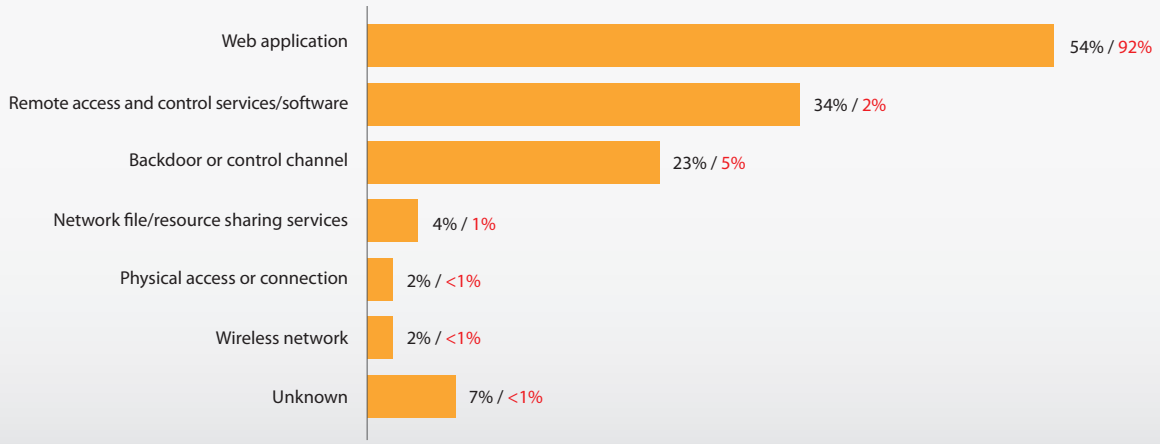
Organizations exert a great deal of effort around the testing and deployment of patches—and well they should. Vulnerability management is a critical aspect of any security program. However, based on evidence collected over the last six years, we have to wonder if we're going about it in the most efficient and effective manner. Many organizations treat patching as if it were all they had to do to be secure. We've observed companies that were hell-bent on getting patch x deployed by week's end but hadn't even glanced at their log files in months. This kind of imbalance isn't healthy. Therefore, we continue to maintain that patching strategies should focus on coverage and consistency rather than raw speed. The resources saved from doing that could then be put toward something more useful like code review and configuration management.

13 The word "patchable" here is chosen carefully since we find that "vulnerability" does not have the same meaning for everyone within the security community. While programming errors and misconfigurations are vulnerabilities in the broader sense, lousy code can't always be fixed through patching and the careless administration patch has yet to be released. Furthermore, many custom-developed or proprietary applications simply do not have routine patch creation or deployment schedules.

Attack Pathways

After being edged out in 2008 as the most-used path of intrusion, web applications now reign supreme in both the number of breaches and the amount of data compromised through this vector. Both Verizon and USSS cases show the same trend. This falls perfectly in step with the findings pertaining to types of attacks discussed above. Web applications have the rather unfortunate calling to be public-facing, dynamic, user-friendly, and secure all at the same time. Needless to say, it's a tough job.

Figure 22. Attack pathways by percent of breaches within Hacking and percent of records



Remote access and control solutions also present challenges. On one side stands the organization's internal assets and on the other side a perfectly benign and trusted entity. Well, as evidenced by these results, that last part is not always true and therein lies the rub. Because these solutions are so often picked on and because there are many different types of them, we gathered a bit more detail during 2009. This is what we found:

- Third party remote desktop software (i.e., LogMeIn) – 13%
- Native remote desktop services (i.e., VNC) – 9%
- Remote access services (i.e., VPN) – 13%

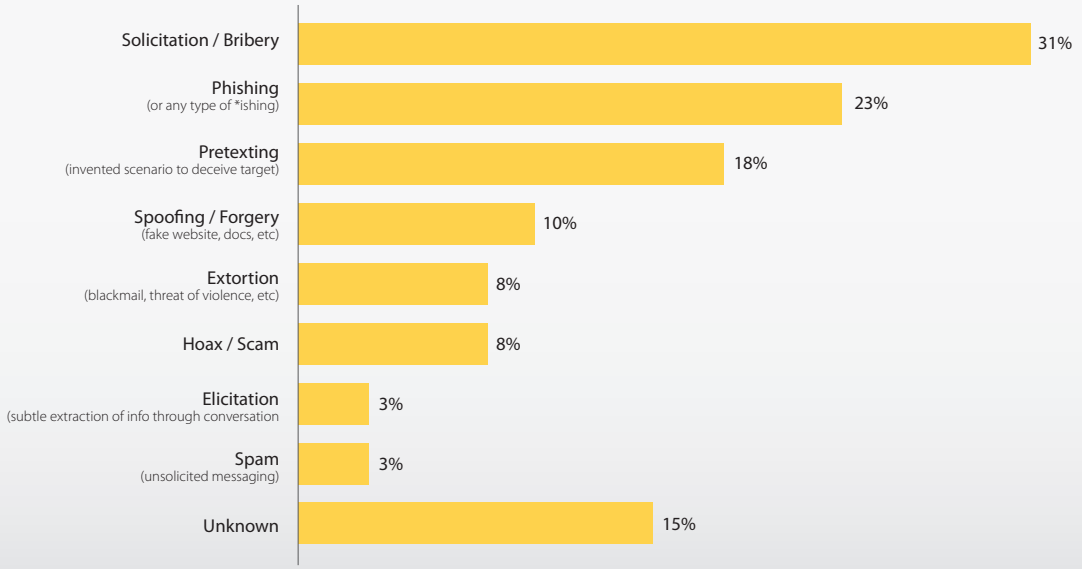
Backdoors were discussed briefly above and more fully in the Malware section. Since their entire existence is to allow malicious agents to traverse the perimeter unnoticed, it's hardly surprising they are a common vector of intrusion. This marks the third year in a row that only a single incident occurred in which wireless networks were used to infiltrate organizational systems. It was completely open. The physical access or connection vector may seem odd in combination with hacking but there are instances in which this comes into play. For instance, one case involved connecting two systems and running a cracking utility against the SAM database on the target system.

Social (28% of breaches, 3% of records)

Social tactics employ deception, manipulation, intimidation, etc. to exploit the human element, or users, of information assets. These actions are often used in conjunction with other categories of threat (i.e., malware designed to look like antivirus software) and can be conducted through technical and non-technical means. Within the past year, social tactics played a role in a much larger percentage (28% vs. 12% in 2008) of breaches, due mainly to the addition of the USSS cases.

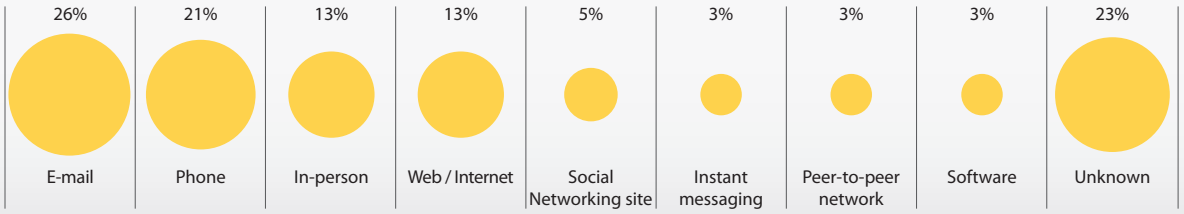
VERIS Classification Note: Those familiar with the 2008 and 2009 DBIRs may recognize this as a new category. This category was previously referred to as Deceit; we believe the change better reflects the broad nature of human-targeted threats.

Figure 23. Types of social tactics by percent of breaches within Social



As seen in Figure 23, solicitation and bribery occurred more often than any of the other types of social tactics recognized by the VERIS framework. This may seem odd, but the explanation is quite simple; these were scenarios in which someone outside the organization conspired with an insider to engage in illegal behavior (usually embezzlement as seen in the next section). According to the USSS, these are usually organized criminal groups conducting similar acts against numerous organizations. They recruit, or even place, insiders in a position to embezzle or skim monetary assets and data, usually in return for some cut of the score. The smaller end of these schemes often target cashiers at retail and hospitality establishments while the upper end are more prone to involve bank employees and the like. Other common social tactics observed in 2009 were phishing and pretexting. These are classic attacks that have been discussed extensively in our previous reports.

Figure 24. Paths of social tactics by percent of breaches within Social



Similar to last year's report, e-mail is still the vector of choice for conducting social attacks. The criminals also apparently like to maintain that personal touch by using the phone or even in-person contact with the victims to get the information they need. Security concerns around social networking sites have been discussed quite frequently of late, but this vector did not factor prominently into breach cases worked by Verizon or the USSS. However, the seemingly non-stop growth of these sites, their extensive use from corporate assets, and the model they employ of inherently trusting everything your "friends" do may be too attractive for criminals to ignore for long. We are interested to see if this vector plays a larger role in data breaches over the next few years.

The targets of social tactics are overwhelmingly regular employees and customers. As in years past, we continue to stress how important it is to train all employees about the various types of social attacks. A security awareness campaign should, at the very least, train them to recognize and avoid falling for the opportunistic varieties like phishing and other scams. Employees in sensitive, trusted, or public-facing positions should also be prepped for more targeted tactics and reminded of corporate policies that (hopefully) deter misconduct. Including social tactics in mock incident or penetration tests can be a good measure of the effectiveness of awareness programs and overall readiness of the organization to thwart these attacks.

Table 4. Targets of social tactics by percent of breaches within Social

Regular employee/end-user	26%
Customer (B2C)	15%
Executive/upper management	5%
System/network administrator	5%
Finance/accounting staff	3%
Helpdesk staff	3%
Unknown	3%

According to the USSS, solicitation usually involves organized criminal groups conducting similar acts against numerous organizations. They recruit, or even place, insiders in a position to embezzle or skim monetary assets and data, usually in return for some cut of the score.

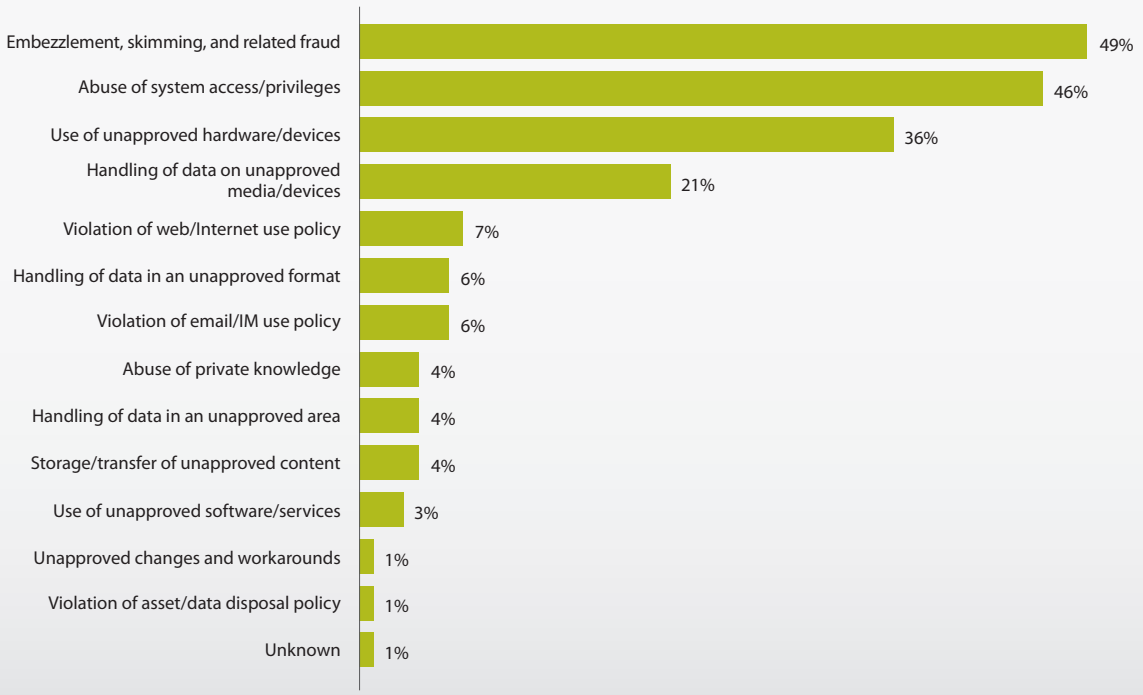
Misuse (48% of breaches, 3% of records)

We define misuse as using organizational resources or privileges for any purpose or in a manner contrary to that which was intended. These actions can be malicious or non-malicious in nature. The category is exclusive to parties that enjoy a degree of trust from the organization like insiders and partners. For the first time since we began this study, Misuse was the most common of all threat actions (48%) in our dataset. It was not, however, responsible for a large proportion of records breached (3%). It may seem strange that such a frequently occurring problem accounts for so small a number of records, but when one considers the circumstances that surround misuse it begins to make sense.

VERIS Classification Note: There is an action category for Hacking and for Misuse. Both can utilize similar vectors and achieve similar results; in Misuse, the agent was granted access (and used it inappropriately) whereas with Hacking, access was obtained illegitimately. Additionally, the line between Misuse and Error can be a bit blurry. In general, the categories divide along the line of intent. Errors are wholly unintentional, whereas Misuse involves willful actions typically done in ignorance of policy or for the sake of convenience, personal gain, or malice.

Embezzlement, skimming, and related fraud were seen more often than other forms of misuse and were exclusive to cases worked by the USSS. These actions were typically perpetrated by employees entrusted with the oversight or handling of financial transactions, accounts, record keeping, etc. Not surprisingly, this often occurred in financial institutions, retail stores, and restaurants. In many cases the use of handheld skimmers and other devices were utilized to facilitate the theft. This accounts for much of the "use of unapproved hardware/devices" depicted in Figure 25. While such activity may not fit some people's notions of cybercrime, cases included in this study did constitute a legitimate data breach. Payment cards, personal information, bank account data, and other sensitive information were compromised and often sold to external parties or used by the insider to commit fraud. It may not be the type of thing readers have come to associate with the DBIR but that is precisely why the addition of the USSS data is so valuable; it lets us study cases we would otherwise never see.

Figure 25. Types of misuse by percent of breaches within Misuse



The prevalence of embezzlement and skimming is one of the major reasons why the total amount of data compromised through misuse is so comparatively low. An employee engaging in this type of fraud has a completely different M.O. than an uberhacker systematically draining data from a large payment card processor. The employee has a vested interest in keeping their job, remaining undetected, and avoiding prosecution. Siphoning small amounts of data or monetary assets over a longer period of time is more suited to this than a "grab as much as you can and run" approach. Embezzlers also have the luxury of targeting exactly what they want in the amount they want when they want it.

Abuse of system access and privileges follows a close second behind embezzlement. As the name implies, it involves the malicious use of information assets to which one is granted access. System access can be used for any manner of maliciousness but in this report, naturally, its result was data compromise. While common among the USSS' cases (42% of all those involving misuse), it was even more so among Verizon's (67%). Though not apparent from Figure 25, which covers 2009 cases, the abuse of system access tends to compromise much more data than embezzlement and other types of misuse. It often involves system and network administrators (especially the larger breaches) but also other types of employees.

Handling of data on unapproved media and devices was a common type of misuse in both caseloads. It is typically used in conjunction with other forms like "abuse of access" as a convenient way to transport data. Sometimes the devices themselves are contraband but more often the data in question were not approved for storage on an otherwise sanctioned device. We continue to find that the success of a breach does not hinge on the perpetrator being able to use a certain portable device. Unfortunately, insiders have a plethora of choices when it comes to media and devices fit for secreting data out of their employer. For this reason, we have always held that it is easier to control the datasource than the media.

Figure 25 lists several other forms of misuse uncovered during 2009 investigations. Policy violations, storing unapproved content, and other dubious activities can directly breach data (i.e., via personal e-mail accounts) and often pave the way for other badness like the installation of malware. Also, experience shows that employees who willfully engage in "minor" misconduct are often the very same employees engaging in major crimes down the road. Better to establish policies and procedures that nip it in the bud early.

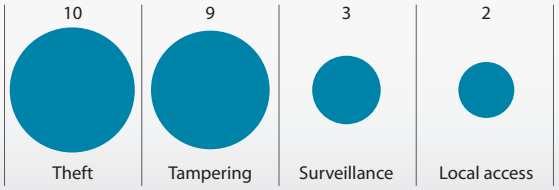
Embezzlement, skimming, and related fraud were seen more often than other forms of misuse and were exclusive to cases worked by the USSS. These actions were typically perpetrated by employees entrusted with the oversight or handling of financial transactions, accounts, recordkeeping, etc.

Physical (15% of breaches, 1% of records)

This category includes human-driven threats that employ physical actions and/or require physical proximity. As in years past, physical attacks continue to rank near the bottom of our list of threat actions. We recognize that this is not in line with what our readers commonly hear and, as we have stated in the past, it is largely due to our caseload. The nature of a great many physical attacks precludes the need for any investigation, and furthermore, they often do not lead to actual data compromise. When regulated information is stored on a stolen laptop, it is considered "data-at-risk" and disclosure is often required. This is true whether or not the criminal actually accessed the information or used it for fraudulent purposes. Our dataset, on the other hand, is comprised of incidents in which compromise was confirmed (or at least strongly suspected based on forensic evidence). The same is true of the USSS' cases, yet the combined dataset still exhibits the highest percentage of physical attacks we've ever reported.

VERIS Classification Note: Natural hazards and power failures are often classified under Physical threats. We include such events in the Environmental category and restrict the Physical category to intentional actions perpetrated by a human agent. This is done for several reasons, including the assessment of threat frequency and the alignment of controls.

Figure 26. Types of physical actions by number of breaches



In almost half of the cases involving physical actions, theft was the type. It would appear that theft is not any more or less prevalent to any particular agent, as we observed external, internal, and partner entities partaking in this crime[14]. Typically, the assets that were stolen were documents, but also frequently included desktop or laptop computers. In our caseload, theft typically occurred in non-public areas within the victim's facility like offices and storage rooms, although there were a few exceptions to this rule.

KNOW YOUR ATTRIBUTES: CONFIDENTIALITY AND POSSESSION

The lost or stolen laptop scenario is one of the reasons we really like the distinction made between Confidentiality and Possession in the "Parkerian Hexad" rather than the more well-known "CIA Triad." In the VERIS framework, we borrow Donn Parker's six security attributes of Confidentiality, Possession, Integrity, Authenticity, Availability, and Utility. The first two perfectly reflect the difference between data-at-risk and data compromise that we so often discuss in these reports. From VERIS:

Confidentiality refers to limited observation and disclosure of an asset (or data). A loss of confidentiality implies that data were actually observed or disclosed to an unauthorized agent rather than endangered, at-risk, or potentially exposed (the latter fall under the attribute of Possession and Control).

Possession refers to the owner retaining possession and control of an asset (or data). A loss of possession or control means that the organization no longer has exclusive (or intended) custody and control over the asset or is unable to adequately prove it. The concept of endangerment (exposure to potential compromise or harm) is associated with this attribute whereas actual observation or disclosure of data falls under confidentiality.

14 A VERIS classification distinction should be made here: If an insider stole assets, funds, or data they were granted physical access to as part of their job duties, we would consider this to be in the "Misuse" rather than "Physical" action category.

Nearly equal in number to theft, all instances of tampering were related to ATM and gas pump skimmers and were unique to the USSS caseload. These are electronic devices that fit over credit card reader slots and often (though not always) work in concert with hidden cameras to capture your account number and PIN. Although some of these devices are rudimentary and crude, others are ingeniously constructed and are incredibly difficult to spot[15]. The cases that involved video surveillance were, as one might expect, all ATMs rather than gas pumps. The majority of these occurred in outdoor areas at the victim location such as an ATM located outside of a bank. This type of crime, while not organized crime as we typically speak of in connection with large-scale hacking cases, does indeed have organization and defined methods. It is most commonly the work of small gangs of criminals who specialize in this type of theft. It should be noted that while physical actions of this type constituted a rather small number of cases, they encompassed a large number of individual crimes. For instance, several cases of this type worked by the USSS in 2009 involved skimmers that were set up at over 50 separate ATMs (in each case) covering a large geographic region.

Table 5. Location of physical actions by number of breaches

Victim location—Indoor non-public area (i.e., offices)	7
Victim location—Outdoor area (grounds, parking lot)	7
External location—Public area or building	3
Victim location—Indoor public/ customer area	3
External location—Public vehicle (plane, train, taxi, etc)	2
Victim location—Disposal area (i.e., trash bin)	1

Error (2% of breaches, <1% of records)

Error refers to anything done (or left undone) incorrectly or inadvertently. Given this broad definition, some form of error could be considered a factor in nearly all breaches. Poor decisions, omissions, misconfigurations, process breakdowns, and the like inevitably occur somewhere in the chain of events leading to the incident. For this reason, we distinguish between error as a primary cause of the incident vs. contributing factor. If error is a primary cause it independently and directly progresses the event chain leading to an incident. On the other hand, if error is a contributing factor, it creates a condition that—if/when acted upon by another threat agent—allows the primary chain of events to progress. For example, a misconfiguration that makes an application vulnerable to attack is a "contributing factor" whereas one that immediately crashes the server is the "primary cause."

We include all that gobbledygook because, quite honestly, how to best classify the role of error in a breach confuses us at times (and we created the classification system). In past DBIRs, we merged all errors together in a single chart if they "significantly" contributed to the breach. Over time, determining whether an error was "significant enough to be significant" and thus counted as a statistic in the report, caused no few heated discussions (yes, we're geeks and take this stuff seriously). Therefore, we've decided to bypass all that and handle things slightly differently than we have in the past. In Table 6, we present only errors fitting the "primary cause" description given above. We can directly observe these and they had a direct and measurable role in the breach. To us, it seems the most straightforward and honest approach and we hope it satisfies you as well.

15 http://krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/

Table 6. Types of causal errors by number of breaches

Misconfiguration	2
Loss or misplacement	1
Publishing error (i.e., posting private info on public site)	1
Technical / System malfunction	1

It will undoubtedly be noticed that the overall numbers are much lower than they have been in the past. Mainly, this is a result of the causal vs. contributory distinction. It is also true that incidents directly resulting from an error are less likely to require outside investigation as it's often painfully obvious what happened. Please don't let these low numbers mislead you; though not shown among the causal variety in Table 6, contributory error is ALMOST ALWAYS involved in a breach. It would be a mistake to use our classification minutia as an excuse not to unyieldingly strive to minimize errors and their impact to data security in your organization.

Environmental (0% of breaches, 0% of records)

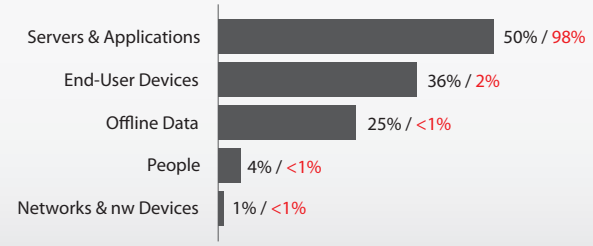
This category not only includes natural events like earthquakes and floods but also hazards associated with the immediate environment (or infrastructure) in which assets are located. The latter encompasses power failures, electrical interference, pipe leaks, and atmospheric conditions. Nothing in this category contributed to data breaches in either the Verizon or USSS caseloads in 2009. Although environmental hazards most often affect the attribute of availability, they do occasionally factor into scenarios resulting in the loss of confidentiality as well. We have, for instance, investigated incidents in the past in which a power outage led to a device rebooting without any of the previously-configured security settings in place. An intruder took advantage of this window of opportunity, infiltrated the network, and compromised sensitive data. Such events are not common but are worth some consideration.

Compromised Assets

We discussed the agents, their actions, and now we turn to the assets they compromised in 2009. This section specifically refers to the assets from which data were stolen rather than assets involved in other aspects of the attack (i.e., an external agent often breaches the internal network in order to compromise data from a database but only the latter would be referenced here). Those familiar with this section from previous DBIRs may notice a few changes. First, what was previously called "Online Data" is now "Servers and Applications" simply because it's more descriptive and sets a clearer boundary between it and the other categories. We also made "People" its own category because information can be directly stolen from them (think phishing and torture) and they (we?) should receive separate consideration and protection. Figure 27 shows results for the five asset categories. Those interested in a more specific list of the most compromised asset types can refer to Table 7.

What has not changed is that servers and apps account for 98.5% of total records compromised.

Figure 27. Categories of compromised assets by percent of breaches and percent of records



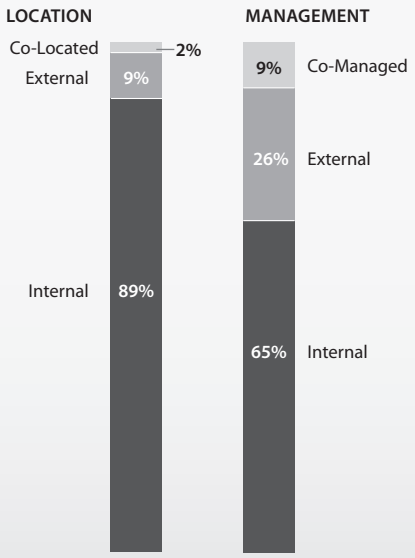
Once again, servers and applications were compromised more than any other asset (that makes six straight years). However, 2009 shows quite a drop from 2008 levels (94% to 50%) primarily due to cases contributed by the USSS. Verizon-only cases also showed less of a super majority at 74% than in previous years. What has not changed is that servers and apps account for 98% of total records compromised (see Figure 27). The top types of assets within this category are basically the same as they have always been: databases, web servers, and point-of-sale (POS) servers.

Breaches involving end-user devices nearly doubled from last year. This was quite consistent between both the Verizon and USSS datasets (37% and 36% respectively). Much of this growth can be attributed to credential-capturing malware discussed earlier in this report.

Offline data is the yin to the servers and apps yang. Where the latter dropped, the former grew. Whereas our cases have been almost devoid of offline data theft (remember—this is different from, for instance, the use of portable media to facilitate data theft, which we see fairly regularly), it occurs often among those investigated by the USSS. Most of these involved insiders stealing IP, engaging in embezzlement and skimming, and actions of that nature. This is another one of those areas where the merged dataset serves to create a more complete view of the world. That view, however, doesn't change our perspective on where most loss occurs; offline assets once again comprised less than 1% of all compromised records. The same was true of the people and networks categories.

Cloud computing is an important topic and the relationship of hosted, virtualized, and externally-managed systems to data breaches is an important area of study. Figure 28 shows the location and management of these assets discussed in this section. The question of whether outsourcing contributes to the susceptibility of assets to compromise cannot be answered from these results. That would require more information. For instance, is the 89% shown for internally-sited assets higher or lower than that of the general population? If such a statistic exists, it would make for an interesting comparison. For now, we will simply relay our findings and continue to collect what information we can.

Figure 28. Location and management of compromised assets by percent of breaches*



* Only assets involved in 2% or more of breaches shown

Table 7. Types of compromised assets by percent of breaches and percent of records*

Type	Category	% of Breaches	% of Records
Database server	Servers & Applications	25%	92%
Desktop computer	End-User Devices	21%	1%
Web app/server	Servers & Applications	19%	13%
Payment card	Offline Data	18%	<1%
POS server (store controller)	Servers & Applications	11%	<1%
Laptop computer	End-User Devices	7%	<1%
Documents	Offline Data	7%	<1%
POS terminal	End-User Devices	6%	<1%
File server	Servers & Applications	4%	81%
Automated Teller Machine (ATM)	End-User Devices	4%	<1%
FTP server	Servers & Applications	2%	3%
Mail server	Servers & Applications	2%	4%
Customer (B2C)	People	2%	<1%
Regular employee/end-user	People	2%	<1%

* Only assets involved in 2% or more of breaches shown

Compromised Data

In terms of data theft, we are glad to say that 2009 was no 2008. Just among breach cases worked by Verizon and the USSS, over 360 million records were compromised in 2008 (overlap removed). While nowhere near the 2008 figure, 2009 investigations uncovered evidence of 143 million stolen records, making it the third-highest year in the scope of this study (see Figure 29). Not exactly a successful year for the defenders but we'd be happy if the 50% drop continued over the next few.

Figure 29. Number of records compromised per year in breaches investigated by Verizon and the United States Secret Service

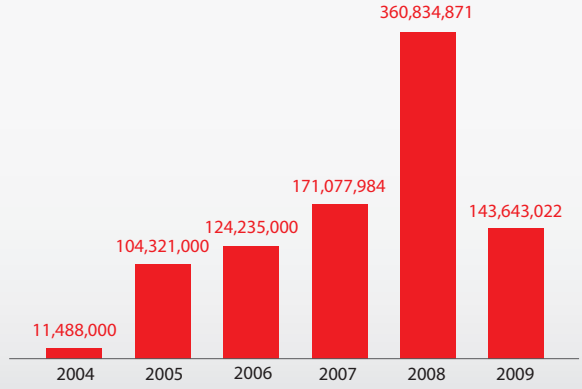
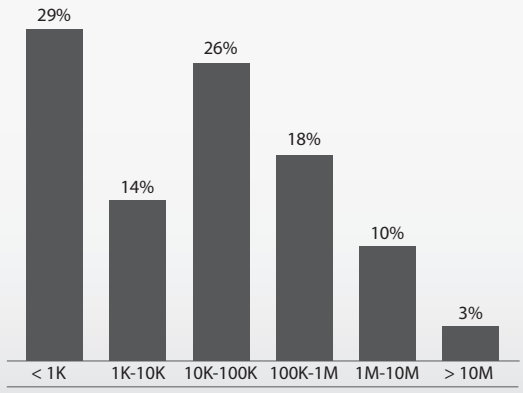


Figure 30. Distribution of records compromised by percent of breaches, 2004-2009



What's not apparent in Figure 29 is that this total is the low-end estimate for 2009. In about 25% of cases, investigators confirmed compromise but were unable to quantify losses, and so, these cases did not contribute to the 143 million figure. The true number is somewhere north of that. The difficulty in quantifying exact losses is also part of the reason Figure 29 shows different values than in previous years (the major reason being that 2007 onward reflects additional USSS cases). Occasionally, we learn of exact losses after the close of an investigation (i.e., when the case goes to trial) and we update our figures accordingly.

As was the case in the previous year, most of the losses in 2009 came from only a few breaches. The average number of records lost per breach was 1,381,183, the median a scant 1,082, and the standard deviation a whopping 11,283,151. While those figures are interesting to understand a bit more about the variance among 2009 cases, loss distributions are far more interesting when they describe larger samples. Therefore, we'd like to break from discussing 2009 for a moment and present what we hope will be useful data for those of you who get into this kind of thing. Figure 30 and Table 8 present descriptive statistics on all breaches and all 900+ million records investigated by Verizon and the USSS since 2004 (at least those that have been studied and classified using VERIS for the purposes of this study).

With that short excursion out of the way, let's return to examining 2009 results, specifically, which types of data were stolen during breaches worked last year. The first observation is that Figure 31 is not as one-dimensional as in years past. Although still the most commonly breached type, payment card

data dropped from 81% of cases to 54% in 2009. Both Verizon and the USSS showed the same result within a few percentage points. It does still account for 78% of total records breached but that is also down (from 98%). Payment cards are prized by criminals because they are an easy form of data to convert to cash (which is what most of them really want). Most payment card cases worked by Verizon and the USSS involve fraudulent use of the stolen data. Losses associated with post-breach fraud are not counted as part of this study but total in the tens of millions of dollars just for the subset of breaches for which we know an amount.

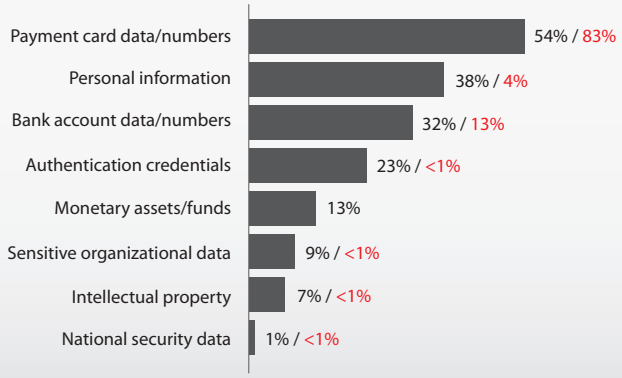
Personal information and bank account data were the second and third-most compromised data types. Like payment cards, both are useful to the criminal for committing fraud. Bank account data rose substantially due to the many cases of insider misuse at financial institutions worked by the USSS. Often related to this, monetary assets or funds stolen directly from these and other compromised accounts were fairly common.

The usefulness of authentication credentials to cybercriminals has been discussed already in this report so we won't do so again here. Sensitive organizational data (like financial reports, e-mails, etc.), intellectual property, and national security data were not nearly as common as some of the more directly cashable types of data but there are reasons for this. Perhaps the primary reason is that disclosure or outside investigation is not usually mandatory as it often is with payment cards and personal information. This means we are less likely to conduct forensics. Furthermore, since most organizations discover a breach only after the criminal's use of stolen data triggers fraud alerts, we infer that breaches of data not useful for fraud are less likely to be discovered. In other words, this kind of information is likely stolen more often than these statistics show. It also tends to harm the organization (or nation) a great deal more in smaller quantities than do payment cards and the like.

Table 8. Descriptive statistics on records compromised, 2004-2009

Total records	912,902,042
Mean[16]	1,963,230
Median[17]	20,000
Standard deviation[18]	13,141,644
Percentiles[19]	
10th	12
25th	360
50th	20,000
75th	200,000
90th	1,200,001
99th	60,720,000

Figure 31. Compromised data types by percent of breaches and percent of records



16 The average of a set of numbers
17 The middle value in an ascending set of numbers
18 A measure of variability in a set of numbers
19 The value below which a certain percent of a population falls

Attack Difficulty

Given enough time, resources and inclination, criminals can breach virtually any single organization they choose but do not have adequate resources to breach all organizations. Therefore, unless the value of the information to the criminal is inordinately high, it is not optimal for him to expend his limited resources on a hardened target while a softer one is available. While rating the difficulty of attacks involves some subjectivity, it does provide an indicator of the level of effort and expense required to breach corporate assets. This, in turn, tells us a lot about the criminals behind these actions and the defenses we put in place to stop them.

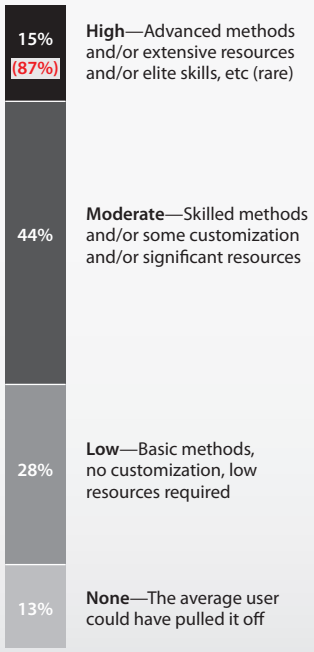
Our investigators assess the various details around the attack and then classify it according to the following difficulty levels:

- **None:** No special skills or resources required. The average user could have done it.
- **Low:** Basic methods, no customization, and/or low resources required. Automated tools and script kiddies.
- **Moderate:** Skilled techniques, some customization, and/or significant resources required.
- **High:** Advanced skills, significant customization, and/or extensive resources required.

Attack difficulty is not a part of the VERIS framework, so it is not a data point collected by the USSS (the same applies to the Attack Targeting and other sections). The primary focus of sharing between the organizations was on objective details about each case. Therefore, results in this section pertain only to Verizon's 2009 caseload.

From 2004–2008, over half of breaches fell in the "None" or "Low" difficulty ratings. The scales tipped in 2009 with 60% now rated as "Moderate" or "High." This finding is in line with the assertions outlined in the beginning of the Results and Analysis section: the breaches worked by our IR team are, in general, getting larger and more complex. This also mirrors our historical data pertaining to the Financial and Tech Services industries.

Figure 32. Attack difficulty by percent of breaches and records*



* Verizon caseload only

Given enough time, resources and inclination, criminals can breach virtually any single organization they choose but do not have adequate resources to breach all organizations.

Looking more closely at the distributions, the percentage of breaches on the low end ("None") and high end ("High") of the difficult rating remains similar to that reported in last year's study. Also, highly difficult attacks once again account for the overwhelming majority of compromised data (87% of all records). The real growth this year is in the moderately difficult category.

Attack scenarios are most effectively and efficiently prevented earlier in their progression rather than later. Said differently, stop adversaries before they own the box because it's awfully hard to stop them once they have.

As discussed in the section detailing hacking activity, and continuing from last year's report, techniques used by criminals to infiltrate corporate systems remain relatively low in skill and resource requirements (though there are certainly exceptions). The sophistication is once again found in the malware that is used in these attacks. These programs are often written from scratch or customized substantially to evade detection and serve a particular purpose in the attack.

Difficult attacks, therefore, are not necessarily difficult to prevent. At the risk of stating the obvious, there is a message here that should be clearly understood: attack scenarios are most effectively and efficiently prevented earlier in their progression rather than later. Said differently, stop adversaries before they own the box because it's awful hard to stop them once they have.

Attack Targeting

Standard convention in the security industry classifies attacks into two broad categories: opportunistic and targeted. Due to significant grey area in this distinction, we find it useful to separate opportunistic attacks into two subgroups. The definitions are provided below:

- **Random Opportunistic:** Attacker(s) identified the victim while searching randomly or widely for weaknesses (i.e., scanning large address spaces) and then exploited the weakness.
- **Directed Opportunistic:** Although the victim was specifically selected, it was because they were known to have a particular weakness that the attacker(s) could exploit.
- **Fully Targeted:** The victim was first chosen as the target and then the attacker(s) determined a way to exploit them.

Figure 33. Attack targeting by percent of breaches and records*

* Verizon caseload only

The percentage of fully targeted attacks in our dataset (27%) is consistent with last year's report (28%), which means the majority of breach victims continue to be targets of opportunity. This is both good news and bad news. Good for those in our profession who's job difficulty levels correlate highly with criminal determination. Bad because it means many of us have made ourselves targets when we otherwise might not have been. Doubly bad because when targeted attacks are successful, they can be quite lucrative for the attacker. In 2009, targeted attacks accounted for 89% of records compromised. Laying this information side by side with data points in the Attack Difficulty section, one begins to get the message many criminals are hearing: find a juicy target (even if well-protected), apply your resources, work hard, and you'll reap the reward. We need to change that message.

We still believe that one of the fundamental self-assessments every organization should undertake is to determine whether they are a Target of Choice or Target of Opportunity.

Though the same overall proportion, random and directed opportunistic attacks have fluctuated somewhat in the last year. As discussed in last year's report, we encounter many breaches that seem neither truly random nor fully targeted—particularly in the Retail and Hospitality industries. In a very common example, the attacker exploits Software X at Brand A Stores and later learns that Brand B Stores also runs Software X. An attack is then directed at Brand B Stores but only because of a known exploitable weakness. We don't believe the dip in directed opportunistic attacks stems from changes in the threat environment. Rather, it is more likely due to the lower percentage of retailers and breaches that involve compromised partner assets within our 2009 caseload.

We still believe that one of the fundamental self-assessments every organization should undertake is to determine whether they are a Target of Choice or Target of Opportunity. The security media hype machine would like us to believe that we're all Targets of Choice and there's nothing we can do to stop the new *[insert whatever you like here]* threat. This simply isn't true and is not a healthy line of reasoning for security management. Consider instead questions like these: Do you have information the criminals want? How badly do they want it? How can they profit from it? How far would they go to obtain it? How difficult would it be for them to get it if they started trying today? What could you do to decrease the chances they will choose you or increase the work required to overcome your defenses? Not answering such questions honestly and properly can result in serious exposure on one hand and serious overspending on the other.

Unknown Unknowns

Past DBIRs have shown a strong correlation between security incidents and a victim's lack of knowledge about their operating environment, particularly with regard to the existence and status of information assets. Though the numbers are down in 2009, the year can hardly be called an exception. In nearly half of Verizon's cases, investigators observed what we not so affectionately call "unknown unknowns." These are classified as meeting at least one of the following conditions:

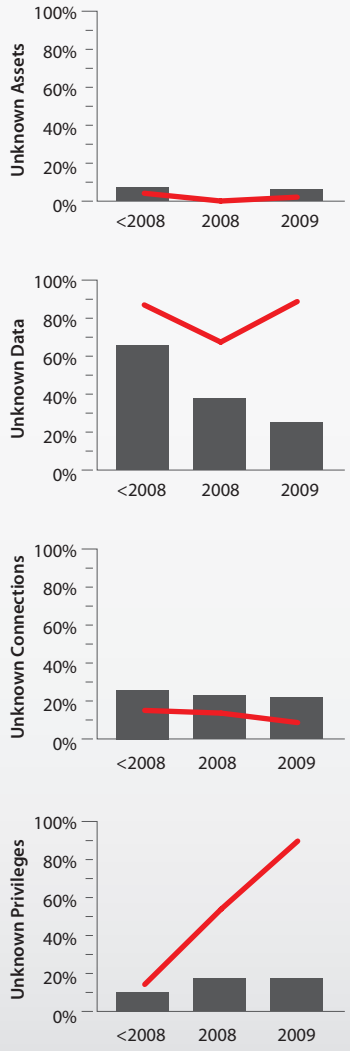
- **Assets** unknown or unclaimed by the organization (or business group affected)
- **Data** the organization did not know existed on a particular asset
- Assets that had unknown network **connections** or accessibility
- Assets that had unknown user accounts or **privileges**

The downward trend in the overall representation of unknowns as a contributor to data breaches is somewhat perplexing (from 90% several years ago to 43% this past year). As seen in Figure 34, this is mainly the result of a steady decline in assets that were storing unknown data. This could be because organizations are getting better at managing their environment; lets hope so. The case could also be made that demographics are a factor. As reported in our 2008 Supplemental DBIR (and supported by data collected since then), Financial Services organizations boast a much better track record when it comes to unknown unknowns. It makes sense that the growing share of our cases worked in this industry would influence these statistics. We also suspect the growth of certain regulations, like those that restrict POS systems from storing data locally, are having a positive effect. It could also be argued that the problem has simply shifted elsewhere; that attackers have changed their tactics. They no longer rely on the accidental storing of data in the clear but are employing RAM scrapers, packet sniffers, and other methods to actively and selectively capture the data they desire.

Setting "unknown data" aside, the other categories are fairly level. Losing track of network connections and accounts seems to be a persistent problem for data breach victims. Data loss linked to cases involving "unknown privileges" rocketed up again to 90%. In the past we've recommended practices like asset discovery, network and data flow analysis, and user account reviews, and we'd be remiss not to restate their value here.

Finally, it is very important to note that though the overall occurrence of "unknowns" is down, it would be wrong to relegate them to a problem of yester year. By examining these results from the perspective of data loss, one realizes that the "impact" of unknown unknowns has never been higher, contributing to nine of ten records breached in 2009. What we don't know continues to hurt us.

Figure 34. Unknown Unknowns by percent of breaches and percent of records



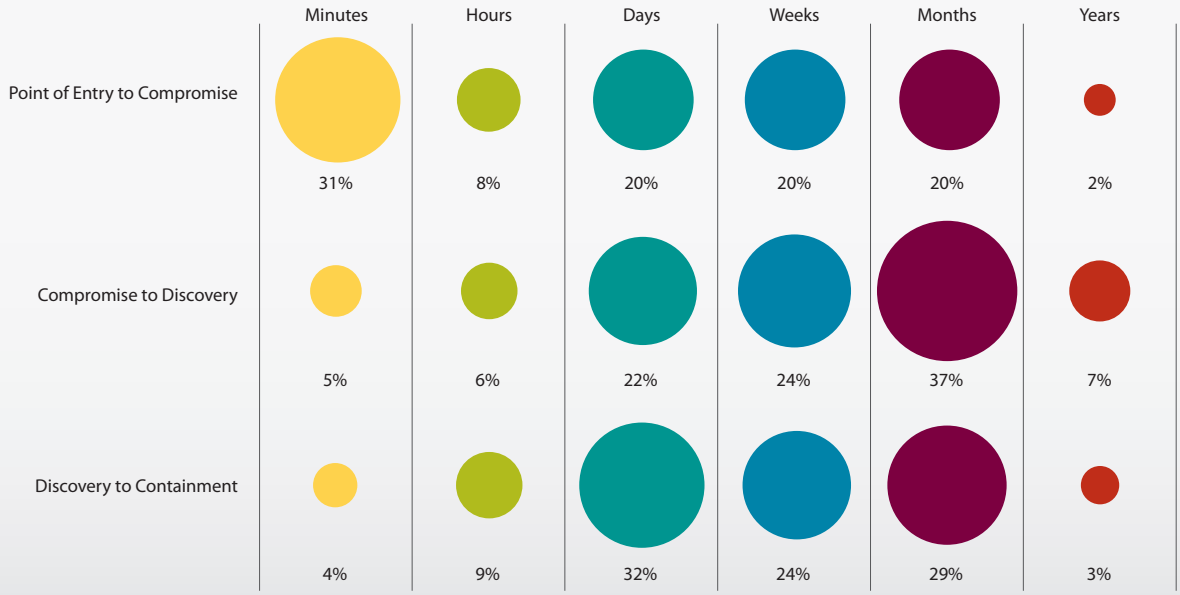
By examining these results from the perspective of data loss, one realizes that the "impact" of unknown unknowns has never been higher, contributing to nine of ten records breached in 2009. What we don't know continues to hurt us.

Timespan of Breach Events

If you've ever seen a Hollywood version of a data breach, it probably went down something like this: the attacker launches some nifty tool with flashy graphics, punches keys for 30 seconds, and then exclaims "We've got the files!" Meanwhile, on the defending side an analyst looks up at a large screen, goes pale, and stammers "Sir—they've breached our firewall." Based on our experience, real-world breaches follow a very different script. Understanding that script tells us a lot about the interplay between attackers and defenders.

In describing the timeline of a breach scenario, one could identify numerous discrete events if so inclined. Separating events into three major phases serves our purposes quite well and closely aligns with the typical incident response process. These phases are depicted in Figure 35 and discussed in the paragraphs that follow.

Figure 35. Timespan of events by percent of breaches



Point of Entry to Compromise

This phase covers the attacker's initial breach of the victim's perimeter (if applicable) to the point where they locate and compromise data. This often involves an intermediate step of gaining a foothold in the internal network. The amount of time required to accomplish this varies considerably depending on the circumstances. If data are stored on the initial point of entry, compromise can occur very quickly. If the attacker must navigate around the network probing for data, it can take considerably longer. The timeline also changes based on the methods and tools employed by the attacker.

In over 60% of breaches investigated in 2009, it took days or longer for the attacker to successfully compromise data. The Verizon and USSS datasets vary little on this statistic. While some may interpret this to be a rather small window of time, it could be worse. If victims truly have days or more before an attack causes serious harm, then this is actually pretty good news. It means defenders can take heart that they will likely get more than one chance at detection. If real-time monitoring fails to sound an alarm, perhaps log analysis or other mechanisms will be able spot it.

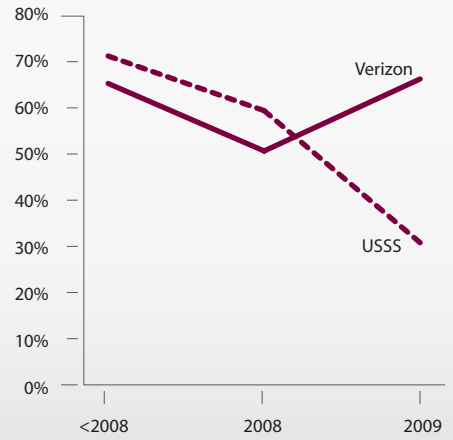
If victims truly have days or more before an attack causes serious harm, then this is actually pretty good news. It means defenders can take heart that they will likely get more than one chance at detection.

Unfortunately, we're speaking hypothetically here. The bad news is that organizations tend not to take advantage of this second window of opportunity. The telltale signs are all too often missed, and the attacker has all the time they need to locate and compromise data.

Compromise to Discovery

Over the last two years, the amount of time between the compromise of data and discovery of the breach has been one of the more talked about aspects of this report. It is not without reason; this is where the real damage is done in most breaches.

Figure 36. Percent of breaches that remain undiscovered for months or more



That a breach occurred is bad enough but when attackers are allowed to capture and exfiltrate data for months without the victim's knowledge, bad gets much worse. In the 2009 DBIR, we closed this section hoping that the slight improvement we observed from the previous year would continue. While Figure 35 would seem to suggest it's time for some modest celebration, we're not sipping champagne just yet.

Yes, it's true that the percentage of breaches extending months or more before discovery is down for the third year in a row (65% to 50% to 44%). While the first two of those figures speak to Verizon's dataset only, the last includes USSS data. Figure 36 gives a clearer picture of what's really going on and explains our hesitation. For Verizon cases, 2009 was actually the worst year yet in terms of the time to discovery metric. For the USSS, it was the best by far. That the merged statistic is down (which best represents "what we know of the world") is a slightly encouraging sign. At least we'll choose to view it as one and continue to hope and work for improvement.

Discovery to Containment

Once an organization discovers a breach, they will obviously want to contain it as quickly as possible. It should be noted that this is a triage effort and not a complete remediation of the root causes of the breach. Containment is achieved when the "bleeding has stopped" and data are no longer flowing out of the victim. This can be as simple as unplugging the network cable from the affected system, but as Figure 35 shows, it's usually not that easy.

The Verizon, USSS, and merged datasets offer nearly identical testimony on this; over half of all breaches go uncontained for weeks or more after they have been discovered. That's either one extremely hard-to-find network cable or something else is afoot. The truth of the matter is that some breaches are harder to contain than others and some victims are more prepared to handle them than others. Organizations represented on the far left of Figure 35 either had very simple containment or a good plan that enabled them to execute quickly. Those on the far right had tougher duty, weren't prepared, or both.

While there are scores of reasons for this, many containment problems can be traced back to failing to remember the five P's: Proper Planning Prevents Poor Performance.

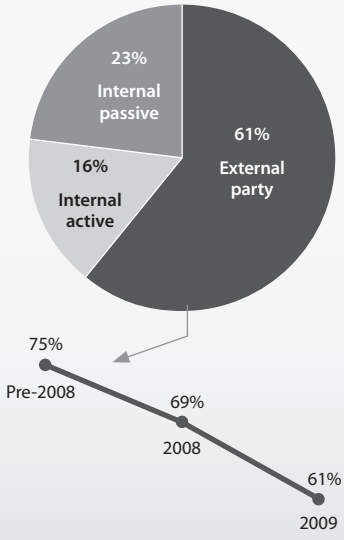
While there are scores of reasons for this, many containment problems can be traced back to failing to remember the five P's: Proper Planning Prevents Poor Performance. We often find organizations have a plan (check P #2) but they downloaded a template from the web and never tailored, distributed, or rehearsed it (uncheck P #1). Others, in their frantic attempts to stop the breach, actually make matters worse and damage valuable evidence at the same time. A lack of adequate and current information like network diagrams is also a common time sink to the response process. Finally, contractual problems can slow the containment of a breach (i.e., What happens when assets involved in an incident are hosted by a third party? What does it take to get the cable pulled?). Again, proper planning prevents poor performance.

Breach Discovery Methods

We discussed how long it takes for victims to discover a breach but it is equally important to examine how they make that discovery or, rather, how others make it for them. The time to discovery is inextricably bound to the method of discovery, as some methods take longer than others. Both metrics are indicators of the maturity of the security program since they reflect on the ability of the organization to detect and respond to threat actions. Unfortunately, Verizon's past research consistently finds that breaches are not found by the victim organization, but by an outside party. We would like to be able to proclaim that this was the result of caseload bias and that things really aren't all that bad outside our sample, but alas, we cannot. Data obtained from the USSS show a very similar finding.

We can offer some good news from 2009, though—perhaps even a glimmer of hope. As seen in Figure 37, breaches discovered by external parties are down for the third year running (75% to 69% to 60%). The difference was made up by internal active measures (those actually designed and deployed to detect incidents) while internal passive discoveries (someone just happened to notice something awry) remained static. Through the rest of this section, we dive into each in more detail[20].

Figure 37. Simplified breach discovery methods by percent of breaches



20 Comparing the discovery methods listed here (and the complete list in VERIS) to prior reports will show significant differences. In most cases, we simply split out existing categories into more discrete items.

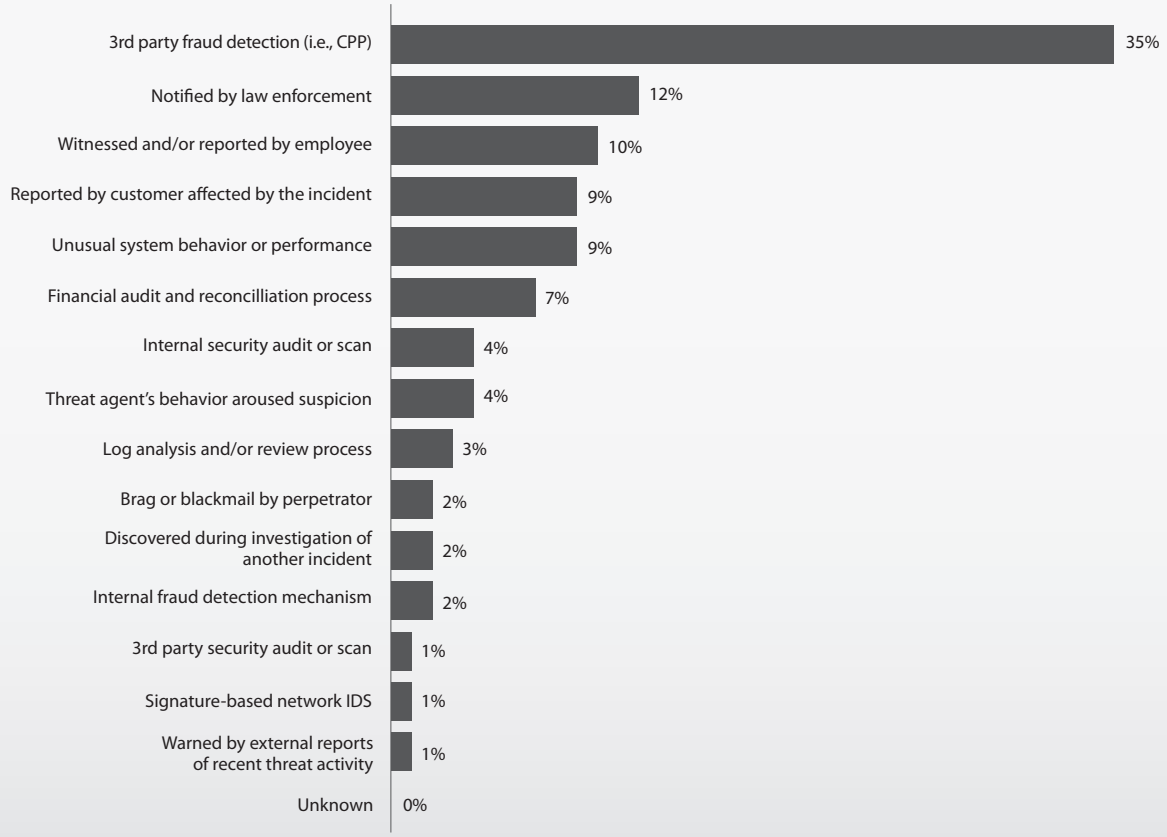
Discovery by external parties

Though substantially lower than ever before, third party fraud detection is still the most common way breach victims come to know of their predicament. When this happens, the organization was usually identified because fraud pattern analysis pointed to them as the common point of purchase (CPP) for payment cards involved in the compromise. We find it more than a little ironic that the most effective way of detecting data breaches is for the perpetrator to fraudulently use what was stolen.

Third party fraud detection is still the most common way breach victims come to know of their predicament.

Notification by law enforcement is second on the list of discovery methods. Underground surveillance, criminal informants, intelligence operations, fraud investigations, etc. are all examples of how law enforcement personnel learn about the breach. Having your customers inform you of a breach is probably the worst of all options. Such notification often comes in the form of a very distressed "what happened to my money?" or some derivative of that not fit for print.

Figure 38. Breach discovery methods by percent of breaches



Internal passive discovery

It turns out that employees aren't bad breach detectors, which is a good thing because most organizations have a decent amount of them. While performing their everyday duties, personnel occasionally witness an incident or stumble upon something that makes them report it. Systems affected by a breach often exhibit unusual behavior or degraded performance. These methods are consistently toward the top of our list and though such discoveries are accidental, it is proof that employees can and should be considered a third line of defense against breaches. Training (good training) can enhance their ability to identify and report incidents and so, seems like a smart direction in which to allocate some budget.

Internal active discovery

Organizations spend far more capital on active measures to detect incidents but results show—at least for breach victims—disappointingly little return. Before discussing what's not working, let's touch on some things that are (sort of).

Internal audit methods—both financial and technical—are the bright spot in all of this. Financial audit and reconciliation processes found several account and ledger discrepancies that were investigated by the organization and discovered to be the result of a breach (remember *The Cuckoo's Egg*?). The increased prominence of this is likely due to the larger ratio of financial institutions in the combined dataset and the nature of breaches worked by the USSS. Technical audits (routine system checks, scans, etc.) also uncovered a respectable number of breaches. Organizations that treat routine security audits in a "just get it done as cheaply and quickly as possible" manner are squandering what could be an effective detection method.

ON LOGS, NEEDLES, AND HAYSTACKS

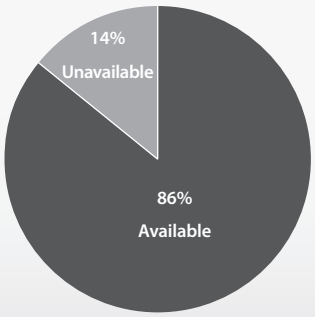
These findings are not easy to digest, especially when you consider that the log data used by our forensic investigators are the very same log data stored on the victim's systems. It cannot be a pleasant experience to learn that the six months of log data you've been collecting contained all the necessary indicators of a breach. It is, however, a common experience. We consistently find that nearly 90% of the time logs are available but discovery via log analysis remains under 5%. That is a very large margin of error. What gives?

Many claim—with good reason—that looking for evidence of malicious activity among the huge number of logs collected in the typical organization is like looking for a needle in a haystack. Maybe they're right (but there are good needle-searching tools out there to help). However, maybe looking for needles isn't what we should be doing; maybe we should be looking for haystacks.

Our investigators spend a great deal of time searching through log files for evidence. It is absolutely true that we have the benefit of hindsight in doing this; we can narrow the search to a certain window of time, certain systems, certain types of events, etc. Nevertheless, we often find what we're looking for because of three major tip-offs: 1) abnormal increase in log data, 2) abnormal length of lines within logs, 3) absence of (or abnormal decrease in) log data. We've seen log entries increase by 500% following a breach. We've seen them completely disappear for months after the attacker turned off logging. We've noticed SQL injection and other attacks leave much longer lines within logs than standard activity. Those are more like haystacks than needles.

No, it's not perfect. It won't catch everything. By all means, if your solution finds needles effectively, do it. We have little doubt, however, that if the organizations we've studied had tuned their systems to alert on abnormalities like this and actually looked into them when alarms went off, that 5% would be a lot higher. We might need to find needles to find perfection (close the gap to 86%), but just finding the haystacks would be a very real improvement.

Figure 39. Availability of log evidence for forensics by percent of breaches*



* Verizon caseload only

Overall, however, the data in context of the broader security industry suggest that we must remain pessimistic about the state of active detection mechanisms within organizations. In the 2009 DBIR, we reported that event monitoring and log analysis, which should be the doyen of detection, successfully alerted only 6% of breach victims. This year that figure has dropped—yes dropped—to 4%. Of that 4%, log analysis lead to the discovery of a handful of breaches while intrusion detection systems identified only one. As with each prior year, we will offer our assessment as to why this situation exists. This time, we use a simple Q&A structure.

Q: Are IDS and log analysis tools ineffective?

A: No. Among breach victims they aren't very effective but the controls themselves can be effective.

Q: Were these technologies utilized by organizations in your dataset?

A: Sometimes. The leading failure is definitely that these tools are not deployed. None of these technologies showed more than a 40% adoption rate among our sample. As further evidence of this, see the level of non-compliance with requirement 10 in PCI DSS.

Q: What happened with those that did use them? Why didn't they help?

A: Usually poor configuration and monitoring. Event monitoring and analysis tools are not "set and forget" technologies, yet many treat them that way. We commonly find these devices neutered (intentionally or unintentionally) to the point of ineffectiveness so as to cause minimal noise and disruption (which is understandable). They are also often undermanned and/or completely unwatched.

Q: You said "usually"—not "always." Are you saying some do a decent job of deploying, configuring, and monitoring detective technologies and the attacker still gives them the slip?

A: Yes. The techniques and level of artifice used in many threat actions discussed throughout this report are unlikely to be seen as malicious by these tools. If an attacker authenticates using stolen credentials, this will look like a legitimate action. Devices scanning for certain pre-defined signatures or hashes will not see those that are altered in some manner. There is no such thing as a silver bullet and if there were, the werewolves would wear armor.

Q: Can you offer any hope?

A: Yes. We continue to find that victims usually have evidence of the attack in their log files. This year that figure was 86%, which suggests that, while we might miss the attack as it happens in real-time, we have a good chance of detecting it later. Combine that with the previous section showing that we have a little breathing room before actual data compromise occurs, and one begins to see some brightness ahead through the gloom. We'll never bask in that light, however, if we do nothing to adjust our course.

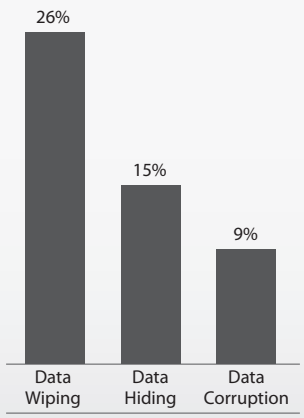
The short answer is that we are not seeing a significant representation of organizations making consistently strong efforts to detect and respond to security events among the victims in these datasets. We truly hope to see that change in the coming years.

Many claim—with good reason—that looking for evidence of malicious activity among the huge number of logs collected in the typical organization is like looking for a needle in a haystack. However, maybe looking for needles isn't what we should be doing; maybe we should be looking for haystacks.

Anti-Forensics

Few criminals want to be behind bars and those who engage in actions to breach information assets are no different. In the wake of the Albert Gonzalez prosecution and other crackdowns, cybercriminals have more reason than ever to hide their tracks and not get caught. Anti-forensics consist of actions taken by the attacker to remove, hide, and corrupt evidence or otherwise foil post-incident investigations. There are varying flavors of anti-forensics, and their use is generally determined by the perpetrator's intended actions. This type of activity is at least partially responsible for the breach discovery and response struggles discussed earlier in this report.

Figure 40. Types of anti-forensics by percent of breaches*



* Verizon caseload only

Investigators found signs of anti-forensics in about one-third of cases in 2009—roughly equivalent to the prior year's DBIR. It should be understood, however, that the very nature of these techniques centers on not leaving signs of their use. Therefore, we believe this figure represents the low-end estimate of the actual prevalence of anti-forensics across our caseload.

While the overall use of anti-forensics remained relatively flat, there was some movement among the techniques themselves. Data wiping, which includes removal and deletion, is still the most common but declined slightly. Data hiding and data corruption remain a distant—but gaining—second and third; the former rose by over 50% and the latter tripled (we're working with fairly small numbers on those though). The use of encryption for the purposes of hiding data contributed most significantly to the increase in that technique while the most common use of data corruptions remains log tampering.

These changes reflect some broader trends observed by investigators over the last year and half with respect to anti-forensics. While the objective to remain hidden is still very real, the ability of criminals to compromise and immediately exfiltrate large quantities of data is diminishing. That's not to say they aren't successfully doing so, but positive action on the part of many organizations has eliminated, for instance, large stores of unencrypted data residing on systems. As a result, perpetrators find it necessary to steal data "on the fly" using malware like network sniffers and RAM scrapers. These tools accumulate a stockpile of data over time and the criminal will want to protect and hide their loot to avoid discovery. Think pirates and buried treasure (which is mostly myth but let's not ruin a good metaphor with technicalities).

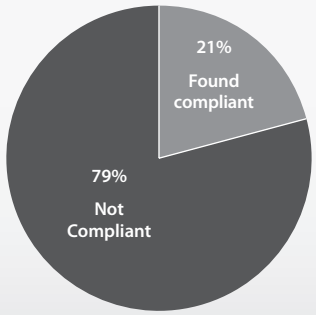
Perpetrators find it necessary to steal data "on the fly" using malware like network sniffers and RAM scrapers. These tools accumulate a stockpile of data over time and the criminal will want to protect and hide their loot to avoid discovery.

Another recent trend is that anti-forensics seem to have trickled down to smaller breaches. In the past, these techniques were much more common in large-scale breaches but the distribution is becoming more uniform. The proliferation of commercial and freeware utilities that can perform these functions makes anti-forensics more accessible and easy to share within criminal communities.

This is clearly a trend of interest to our IR team as the use of anti-forensics can have a profound impact on almost every facet of an investigation. We will certainly continue to monitor and report on the evolution of anti-forensics within cybercrime.

PCI DSS Compliance

Figure 41. PCI DSS compliance status based on last assessment*



* Verizon caseload only

Although the concepts of regulatory compliance, security, and risk are overlapping and interrelated, it is their correlation to data breach incidents that proves most reflective of the Payment Card Industry (PCI) and what changes are necessary to reduce account data compromises. Analysis of Verizon's 2009 dataset offers useful insight into the divergent nature of organizational security efforts and the many attack methods outlined in this report. To better understand this, we draw the distinction between the concepts of 'compliance' and 'validation' against the Payment Card Industry Data Security Standard (PCI DSS). Compliance is a continuous maintenance process while validation is a point in time event. The difference between security efforts and breach incidents runs parallel to these concepts.

The PCI DSS is a set of control requirements created by the Payment Card Industry to help protect cardholder information. Based on the demographics and compromised data types presented in this report, it is no surprise that a sizeable proportion of the organizations in Verizon's[21] caseload are subject to PCI DSS. For these cases, investigators conduct a review of which PCI DSS requirements were and were not in place at the time of the breach. The results of this assessment are recorded, usually appended to the case report, and then conveyed to the relevant payment card brands. This exercise is not an official PCI DSS assessment and it does nothing to uphold or overrule the victim's compliance status. It does, however, provide useful insight into the condition of the security program and posture of the organization at the time of the incident.

Since these organizations are breach victims, the burning question is "were they compliant?" Over three-quarters of organizations suffering payment card data breaches within our caseload had not been validated as compliant with PCI DSS.

Since these organizations are breach victims, the burning question is "were they compliant?" Figure 41 gives the answer to this question and, interestingly, it is the same one that was given last year. Over three-quarters of organizations suffering payment card data breaches within our caseload had not been validated as compliant with PCI DSS at their last assessment or had never been assessed.

If we accept that a non-compliant organization is more likely to suffer a data breach, then the more interesting component in Figure 41 is the 21% that had validated as compliant during their last PCI DSS assessment. This is especially so when one considers that all but one of them were Level 1 merchants. The reader should not immediately interpret this as a failure of the PCI DSS to provide excellent guidance, but rather consider the concepts mentioned above of validation vs. compliance. Due to the point-in-time nature of assessments, it is entirely possible (even probable) for an organization to validate their compliance at time A but not be in a compliant state at the time of the breach. This may reflect a desire within organizations to achieve compliance with the standard for the purposes of validation but a lesser commitment to maintaining that state over the long-term. Furthermore, the validation process is not always consistent among Qualified Security Assessors (QSAs). It should also be remembered that compliance with the PCI DSS (or any other standard) is not an absolute guarantee against suffering a data breach.

21 All findings referenced in this section reference only Verizon's caseload.

Regarding the size of the organizations suffering data breaches, although over a third of data breaches originated from the largest merchants (Level 1) the remainder resulted from the small and medium sized merchant population. Although the large data breaches may outstrip all others in volume of card numbers compromised, it is often the smaller merchants that struggle the most in recovering from the fallout of a data breach. This analysis underscores the need for adoption of basic security practices for these merchants such as the use of PA-DSS compliant payment applications, secure remote management tools, and stronger controls when using trusted third party vendors for maintenance.

The aggregate data from the post-investigation PCI Requirements Matrix for 2009 is presented in Table 9, and is compared to our 2008 findings.

Table 9. Percent of relevant organizations in compliance with PCI DSS requirements based on post-breach reviews conducted by Verizon IR team*

Build and Maintain a Secure Network	2008	2009
Requirement 1: Install and maintain a firewall configuration to protect data	30%	35%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	49%	30%
Protect Cardholder Data		
Requirement 3: Protect Stored Data	11%	30%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks	68%	90%
Maintain a Vulnerability Management Program		
Requirement 5: Use and regularly update anti-virus software	62%	53%
Requirement 6: Develop and maintain secure systems and applications	5%	21%
Implement Strong Access Control Measures		
Requirement 7: Restrict access to data by business need-to-know	24%	30%
Requirement 8: Assign a unique ID to each person with computer access	19%	35%
Requirement 9: Restrict physical access to cardholder data	43%	58%
Regularly Monitor and Test Networks		
Requirement 10: Track and monitor all access to network resources and cardholder data	5%	30%
Requirement 11: Regularly test security systems and processes	14%	25%
Maintain an Information Security Policy		
Requirement 12: Maintain a policy that addresses information security	14%	40%

* Verizon caseload only

There have been a number of changes from 2008 to 2009 and it is important to highlight this delta and its implications and impact on data breaches. Year over year the PCI DSS requirements that saw the greatest increase in compliance were 4, 10, and 12 (22%, 25%, and 26% respectively). Those requirements with the greatest decrease in compliance were 2 and 5 (-19% and -9% respectively). Although Requirement 10 (audit Logging) is still low at 30% compliance, the increase may pay dividends in avoided compromise and shortened response time in the future. Requirement 6 (secure software development) is also quite low but given the problems discussed in this report, any improvement in that area must be viewed as a plus.

When reviewing the percentages for each requirement, several very interesting statistics begin to surface. Requirements 6 and 11—which many organizations complain are the most onerous—are indeed the least compliant across our caseload. These are trailed only slightly by Requirements 2, 3, 7, and 10. Considering the range of controls that this represents, it does not bode well for the security of systems within these organizations.

At the top of the missed list are items in Requirement 6, including secure software development. Attacks relevant to this practice, such as SQL injection, are consistently among the most common and damaging year over year. Considering the fact that vulnerable code can exist not only in custom applications which a company can alter, but also in commercial off the shelf software (COTS) suggests that iterative layers of protection are needed to prevent attacks that exploit these vulnerabilities.

The question most pertinent to security management becomes, if companies fail to maintain the ongoing operational maintenance of systems throughout time, does that increase the likelihood of a data breach?

The lack of compliance in Requirement 11 reflects poorly as this section is meant to validate the proper implementation and robust nature of other controls in the standard. Testing, measuring, and reviewing that reality is in line with belief is something we consistently recommend because it is consistently a problem. Knowing (not just recording) what is actually occurring within networks and systems is likewise critical.

At this point, it's worth considering a common thread that readers may have noticed among the least-met control areas discussed so far—they all require maintenance processes. If this doesn't immediately sink in, take a moment and let it do so. The question most pertinent to security management becomes, if companies fail to maintain the ongoing operational maintenance of systems throughout time, does that increase the likelihood of a data breach?

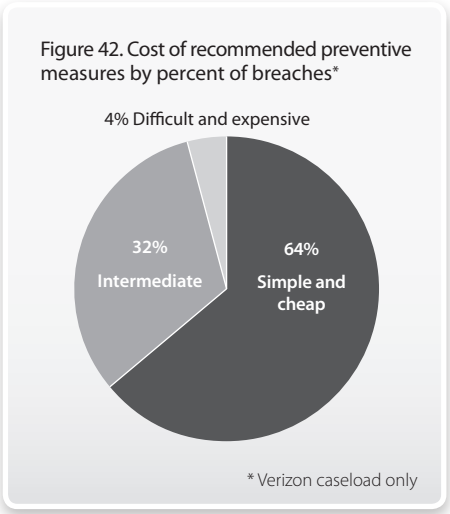
On the other end of the spectrum, a staggering 90% of the organizations breached were found to be encrypting transmission of cardholder data and sensitive information across public networks in compliance with PCI DSS Requirement 4. This is not proof that encryption is useless; it is simply evidence of what we discuss often in this report. Attackers are adept at maneuvering around a strong control (like encryption) to exploit other points of weakness. Perhaps the real strength of encryption should not be measured in key size, but rather in the context of the organization's aggregate security posture.

The use of AV software another requirement toward the top of the compliance list, shares a similar fate to that of encryption. In order to skirt detection, attackers continue to develop and use repacked or customized malware to breach systems.

Clearly PCI DSS is designed not to be a series of compartmentalized controls operated independently to protect information assets. The standard is authored to provide an approach towards security, built to make unauthorized access to systems and data iteratively harder through a series of control gates. When viewed from that perspective, preventing a security breach from turning into a data compromise becomes a much more realistic goal. Hopefully studies like this can be leveraged to complement compliance requirements with risk management efforts to reduce the total cost of security.

Conclusions and Recommendations

Although the overall difficulty of attacks observed in 2009 was a bit higher than previous years, our findings show that the difficulty of preventing them dropped. Only 4% of breaches were assessed to require difficult and expensive preventive measures. This finding is partially explained by Figure 43 in which these recommended preventive measures are divided into several broad categories. Configuration changes and altering existing practices fix the problem(s) much more often than major redeployments and new purchases. The same was true of previous years.



There is an important lesson about security management in all this. Yes, our adversaries are crafty and resourceful but this study always reminds us that our profession has the necessary tools to get the job done. The challenge for us lies in selecting the right tools for the job at hand and then not letting them get dull and rusty over time. Evidence shows when that happens, our adversaries are quick to take advantage of it. Don't let them.

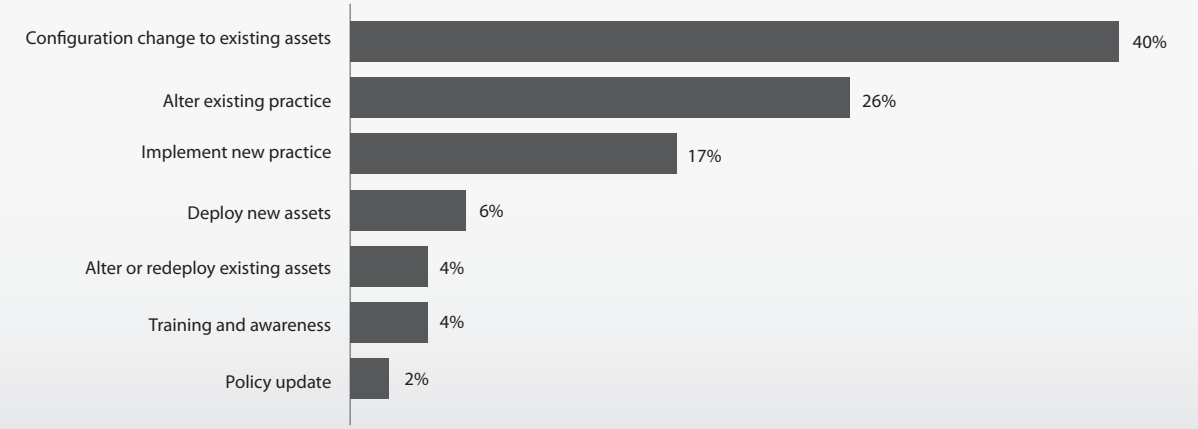
Creating a list of solid recommendations gets progressively more difficult every year we publish this report. Think about it; our findings shift and evolve over time but rarely are they completely new or unexpected. Why would it be any different for recommendations based on those findings? Sure, we could wing it and prattle off a lengthy list of to-dos to meet a quota but we figure you can get that elsewhere. We're more interested in having merit than having many. We did find a few new ones (or extensions of old ones) that we believe to have merit based on our analysis of 2009 and they are listed below. We do, of course, continue to recommend our old ones that can be found in the 2008 and 2009 DBIRs and the 2009 Supplemental report.

Restrict and monitor privileged users: Thanks to data from the USSS, we saw more insider breaches this year than ever before. Insiders, especially highly privileged ones can be difficult to control but there are some proven strategies. Trust but verify. Use pre-employment screening to eliminate the problem before it starts. Don't give users more privileges than they need (this is a biggie) and use separation of duties. Make sure they have direction (they know policies and expectations) and supervision (to make sure they adhere to them). Privileged use should be logged and generate messages to management. Unplanned privileged use should generate alarms and be investigated.

Watch for "minor" policy violations: Sticking with the insider theme, we mentioned several times about a correlation between "minor" policy violations and more serious abuse. Perhaps we should label this as the "Broken Window Theory of Cybercrime." We recommend, then, that organizations be wary of and adequately respond to policy violations. Based on case data, the presence of illegal content, pornography, etc. on user systems (or other inappropriate behavior) is a reasonable indicator of a future breach. Actively searching for such indicators rather than just handling them as they pop up may prove even more effective.

Implement measures to thwart stolen credentials: Stolen credentials were the most common way of gaining unauthorized access into organizations in 2009. Regardless of whether it is a blip or a trend, it's worth doing something to counter it. Keeping credential-capturing malware off systems is priority number one. Consider two-factor authentication where appropriate. If possible, implement time-of-use rules, IP blacklisting (consider blocking large address blocks/regions if they have no legitimate business purpose), and restricting administrative connections (i.e., only from specific internal sources). A "last logon" banner and training users to report/change passwords upon suspicion of theft also have promise.

Figure 43. Categorization of recommended mitigation measures by percent of breaches*



* Verizon caseload only

Monitor and filter egress network traffic: Most organizations at least make a reasonable effort to filter incoming traffic from the Internet. This probably stems from a (correct) view that there's a lot out there that we don't want in here. What many organizations forget is that there is a lot in here that we don't want out there. Thus, egress filtering doesn't receive nearly the attention of its alter ego. Our investigations suggest that perhaps it should. At some point during the sequence of events in many breaches, something (data, communications, connections) goes out that, if prevented, could break the chain and stop the breach. By monitoring, understanding, and controlling outbound traffic, an organization will greatly increase its chances of mitigating malicious activity.

Change your approach to event monitoring and log analysis: A quick review of a few findings from this report will set the stage for this one. 1) In most attacks, the victim has several days or more before data are compromised. 2) Breaches take a long time to discover and 3) when that finally happens, it usually isn't the victim who finds it. 4) Finally, almost all victims have evidence of the breach in their logs. It doesn't take much to figure out that something is amiss and a few changes are in order. First, don't put all your eggs in the "real-time" basket. IDS/IPS should not be your only line of defense. You have some time to rely on more thorough batch processing and analysis of logs. Next, focus on the obvious things (the "haystacks") rather than the minutia (the "needles")[22]. This need not be expensive; a simple script to count log lines/length and send an alert if out of tolerance can be quite effective. Finally, make sure there are enough people, adequate tools, and/or sufficient processes in place to recognize and respond to anomalies. We are confident that this approach will reap benefits and save time, effort, and money.

Share incident information: This final recommendation will also serve as our concluding paragraph. We think this report is a proof that it can be done responsibly, securely, and effectively. We believe that the success of our security programs depends on the practices we implement. Those practices depend upon the decisions we make. Our decisions depend upon what we believe to be true. Those beliefs depend upon what we know and what we know is based upon the information available to us. The availability of information depends upon those willing to collect, analyze, and share it. If that chain of dependencies holds, you could say that the success of our security programs depends upon the information we are willing to share. We believe that this is a call to action and commend all those who take part.

Thank you for taking the time to read this report.

22 See "On Logs, Needles, and Haystacks" in Discovery Methods if it isn't clear what we're talking about.

Appendices from the United States Secret Service

Many readers of the DBIR have questions surrounding what happens after the breach. Where does the information go? How do the perpetrators move it? What goes on behind the scenes in the criminal community? What is being done to stop it? While our investigators have some visibility into these matters, they are squarely in the purview of the United States Secret Service. Thus, the following appendices come directly from the USSS. One delves into the shady world of online criminal communities and the second focuses on prosecuting cybercrime using the example of the USSS' efforts to bring Albert Gonzalez to justice.

Appendix A: Online Criminal Communities

No Monolithic Computer Underground

One of the significant challenges in producing an analysis of the computer underground lies in the diversity of the online criminal community, which manifests itself in a variety of ways. For example, criminals may choose to cluster around a particular set of Internet Relay Chat channels, Internet-based chat rooms or web-based forums. In some instances, a group of online criminals may come from a particular geographic area and may know each other in real life; in other instances, the criminals may be dispersed across the globe and know one another only through their online interaction. Many online underground venues are populated largely by the young and the curious who are not hard-core criminals and whose capabilities and sophistication are as limited as their experience. Other, more exclusive online groups count among their members professional criminals who have a decade or more of experience and extensive contacts in diverse criminal communities.

This diversity also is reflected in the groups' interests and aims. One group may see the researching of vulnerabilities and development of new exploits as a technical challenge fundamentally related to the basics of computer security. Another group may have little or no interest in underlying technological issues, but will happily use exploits developed by others in order to intrude into third-party computer systems and harvest data of commercial value. Still other online criminal communities show even less interest in coding and exploits, but utilize the Internet as an operating base, taking advantage of the anonymity and instantaneous communications the Internet affords them. As such, one needs to keep in mind that blanket statements such as, "Here is what the criminals are doing now..." may reflect only one particular group or type of criminal community and not be universally applicable.

Well-Developed Organizational Structure

Two of the hallmarks that distinguish effective online criminal groups are organizational structure and access to a well-developed criminal infrastructure. Again, these can be manifested in a variety of ways depending on the online community from which the group emerged.

One striking manifestation of these trends in online criminality is found in the web-based online forums that first began to emerge approximately a decade ago. In the early days, these online forums were established by hacking groups or by groups of carders (criminals who traffic in or exploit stolen credit card data). Many of these forums have a strong representation of members from Eastern Europe, although membership often spans the globe and includes members from multiple continents. By utilizing the built-in capabilities of the forum software, the people behind the organization are able to set up a system of forum administrators and moderators who form the core of the organization and who maintain order at the site.

These administrators control the membership of the organization and can simply banish or limit disruptive members, members who cannot back up the claims they make or those who provide poor quality services. At the same time, other members can be elevated within the organization and given enhanced status—such as the rank of Vendor or VIP Member—which will be evident to all other forum members. As the forum continues to grow, existing members can develop good (or bad) reputations for the goods and services they provide; at some forums, these informal authority structures have been augmented by formalized reputation systems similar to those used at online auction sites, so that all forum members will be able to assess another member's reliability at a glance. At many forums, persons who want to become a full-time vendor of goods or services must undergo a formal review process in which senior members of the forum must inspect and rate the product to be vended. By studying the forums, a member who is interested in purchasing, for example, an exploit toolkit will be able to compare the pricing, feature sets and terms of sale of the available toolkits, review the reputations of their respective vendors and conduct interactive discussions with other customers in order to mine their experience with fielding the toolkits under real-world conditions. These abilities enhance the buying experience as well as the quality of goods and services available to the criminal community.

Some of these online forums developed into online bazaars for criminal goods and services. By 2004, such forums as DumpsMarket, CarderPortal, Shadowcrew and CarderPlanet were already well-developed criminal marketplaces overseen by an experienced group of administrators who were often established criminals. While these and similar forums are sometimes called "carding forums," in reality these sites serve as a business platform for a fusion of criminal communities, each of which provides its own contribution to the development of the organization's capabilities by making a greater variety of reliable criminal services available to all members. Some of the major classes of participants in these forums include the following broad categories:

- Carders (Traffic in and exploit stolen financial data)
- Hackers / Security Technologists
  - Perform targeted intrusions for harvesting of data
  - Develop exploits and exploit toolkits
  - Decryption services
  - Anonymity services (proxies, criminal-run VPNs, private messaging systems, etc.)
  - Provide security engineering and consulting services
- Spammers
- Bot Herders (Build and run botnets, which have a variety of criminal uses)
- Money Launderers
- Renegade Hosters and Internet Developers
  - Provide stable platform for criminal business, i.e., criminal sites
  - "Bulletproof Hosts" for phishing, malware drop sites, etc.
- Malware Developers (Creation/dissemination of specialized crimeware)
- Document Forgers (Produce counterfeit drivers' licenses, passports, checks, etc.)
- Information Services (Research services for identity theft)
- Specialized Hardware Providers (ATM skimmers, card production equipment, etc.)
- Calling Services (Provide fraudulent telephone calls to defeat out-of-band authentication)
- Drop Managers (Recruit and manage "drops" or money mules)

Over the past decade, there have been several dedicated carding forums operating at any one time, and many of the more mainstream "hacking forums" (especially in Eastern Europe) have developed sub-forums which include many of the services typically found at a carding forum. Not surprisingly, many of the most serious and/or widespread online attacks attributed to criminal sources over the past decade—both in terms of malware and intrusions—have been linked to established members of these online criminal forums.

As evident from the array of criminal service providers listed in the previous section, the development of diverse online criminal organizations has greatly enhanced the criminal infrastructure available to pursue large-scale criminal activity. At the same time, these criminals' ability to operate anonymously has been augmented by parallel trends on the Internet. One example of such a trend is found—paradoxically enough—in the increasing availability of easy-to-use security technologies; e.g., professional online criminals tend to be avid users of strong encryption, which they use to complicate investigations and conceal evidence of their online activities.

Another online phenomenon often preferred by the criminal community is the appearance of so-called digital currencies. Online digital currencies, such as E-gold, whose operators pleaded guilty to money laundering and illegal money remitting charges in 2008, have allowed online criminals to pay one another for services and goods and to move the proceeds of their criminal schemes internationally with little to no regulation or oversight. The far-reaching availability of a reliable criminal infrastructure in combination with other developments on the Internet presents a global challenge to law enforcement, which has found itself forced to adapt in order to apprehend and prosecute online criminals.

Steady Growth in Attackers' Numbers and Capabilities

By the mid-2000s, online criminal organizations such as those represented by the carding forums had already developed effective and sustainable organizational models which allowed their members to perpetrate some of the most serious security incidents of the time. By this time, even the computer trade and popular press began to notice a pronounced trend which had long been obvious to observers of the carding scene: Today's cybercriminals are not hobbyists seeking knowledge or thrills; they are motivated by the illicit profits possible in online crime.

Since that time, the organizations have continued to evolve; many of the trends seen online have not been favorable to the defenders:

- Online criminal organizations as represented by the Internet forums continue to grow in terms of membership. When it closed in August 2004, the infamous CarderPlanet site was the largest forum of its kind—at its height, the CarderPlanet forum had approximately 7,900 user accounts. By 2010, there are multiple analogous forums whose membership dwarfs that number. At the present time, there are multiple online hacking forums, venues with significant criminal traffic advertising malware, DDoS and hacking services on a daily basis, which have many tens of thousands of registered users.
- As time has gone by, an "old guard" of experienced cybercriminals has developed. It is no longer unusual for a professional criminal to have almost a decade of experience under his belt, during which time he may have been able to develop solid, long-term relationships with a trusted group of similarly experienced associates. Some of these professionals no longer operate with any sort of public presence on Internet venues, but rather deal exclusively with a smaller group of trusted associates. Some of these professionals also are believed to have developed operational relationships with established criminals in the real world as well, which augments their capabilities in ways that the Internet cannot.

- At the same time, the illicit profits associated with top Internet criminals also appear to have grown significantly. A decade ago, someone whose criminal operations brought in tens of thousands of dollars annually was considered fairly successful, depending on the community in which he operated. More recently, experienced cybercriminals have been linked to various attacks and schemes that are known to have garnered them millions of dollars in profits.
- The commercialization of the computer underground continues to develop. One of the more visible manifestations of this phenomenon can be found in the various "affiliate programs" which recruit young hackers into schemes such as "software loads" or "software installs" or the promotion of dubious Internet pharmacies. Some of these affiliate programs have been known to advertise on underground forums, openly recruiting affiliates who will make their botnets available to these schemes in return for a small percentage of the final take.
- Some groups of attackers have been able to develop significant familiarity with and expertise in particular types of target systems, such as those used to process financial data. In some cases, this experience has allowed attackers to manipulate target systems in novel ways that have allowed them to mount attacks that may not have been envisioned before they were successfully executed. In some instances, attackers are known or believed to have had advanced technical or scientific training at prestigious foreign educational institutions, which they have been able to apply in their criminal work through such pursuits as attacking encryption systems.
- The criminal community continues to develop and deploy new back-office services that enhance existing practices. One example of this is found in the multiple antivirus checking services that are run by various criminal groups. These services have purchased subscriptions to dozens of commercially available antivirus and security software packages and allow their customers—for a small fee—to upload malware to see if any current security product will detect it. This type of service allows criminals to know with certainty if the malware they are planning to deploy will be detected by any of the widely deployed antivirus products.
- Criminals are surprisingly adaptive in developing entire new categories of online schemes. One example of this can be found in the fake anti-virus industry that has boomed over the past couple of years; this scam typically involves bogus alerts on the desktops of Internet users designed to trick them into purchasing a useless piece of software which would purportedly protect their system. While there had been scams along this line earlier in the 2000s, in 2008 traffic relating to this "business model" exploded on underground forums, and by 2010 fake security products comprised a significant percentage of all malware, according to industry estimates.

The Criminal Marketplace

One of the perennial questions surrounding the online underground marketplace concerns the cost of various goods and services. Although such figures often appear in the popular press as part of titillating headlines, in reality the pricing of goods tends to be a complex issue, as it depends on a wide variety of factors including the circumstances of the sale, the exclusivity and quality of the goods in question, the volume in which they are acquired, the number of competing vendors, etc. Consider the question, "How much does it cost to buy a car? A comprehensive answer would have to note that one can buy an aging jalopy for a few hundred dollars, while a luxury sports car can cost more than a quarter of a million dollars. The underground exhibits the same variety in terms of pricing. If a criminal needs a piece of spyware, he can download several samples of such software (many of low quality in one regard or another) from several Internet archives, possibly trying to modify it for his needs. Alternately, he can spend several thousand dollars and buy a full-featured, undetectable spyware package from a current vendor who will support it. If he needs an exclusive package, there have been reports of other spyware products that can cost tens of thousands of dollars, if one knows the right people.

Much the same is true in terms of prices of such goods as stolen credit cards. First of all, there is a wide variety of types of cards (classic cards, gold cards, platinum cards, cards issued by U.S. banks, cards issued by foreign banks, etc.), and these distinctions influence the price. Secondly, some vendors have an "all sales final" policy with no guarantee of validity, whereas others will replace invalid card data; the latter group of vendors tends to have higher prices. Thirdly, buyers who deal in volume almost always get a better price than people who purchase small amounts of stolen cards. Fourthly, cards are sold in the underground in different formats, which is one of the main factors in determining the price of the data. So-called "cvv2s" typically include the card number, expiration date, cardholder name and address, and the CVV2 security code from the back of the card. This type of data typically sells for $1 to a few dollars per unit, depending on the type of card and circumstances of the sale. Another type of card is called a "full-info" card—this type of card includes all the data associated with a "cvv2" but is enhanced with other data about the cardholder such as his date of birth, mother's maiden name, Social Security Number, place of birth, and other information that will aid in authenticating fraudulent transactions. Full-info cards will typically cost more than $10 and up per unit in the underground, depending on a variety of factors. Credit card track data (electronic data from the magnetic stripe on the back of a credit card) is called in the underground a "dump." The price for dumps usually starts at around $15 and may be considerably more, depending on the type of card and validity rate of the data being sold.

Appendix B: Prosecuting Cybercrime—The Albert Gonzalez story

In April 2005, the United States Secret Service (USSS) San Diego Field Office initiated an online undercover operation, Carder Kaos, targeting top tier suspects participating in financial crimes committed through the Internet. Operation Carder Kaos focused its investigation on a suspect known online as "Maksik", since identified as Maksym Yastremskiy, a Ukrainian national regarded as the most prolific vendor of compromised credit card numbers in the world. A series of undercover online purchases of credit cards led to face-to-face meetings with Yastremskiy in Thailand, the United Arab Emirates, and Turkey where enough evidence was obtained to secure an indictment. In July 2007 another undercover meeting in Turkey was arranged and Yastremskiy was arrested and prosecuted by Turkish authorities. Maksym Yastremskiy is currently serving a thirty-year sentence in Turkey.

As a result of the Carder Kaos investigation, the USSS, Criminal Intelligence Section (CIS) leveraged considerable intelligence and directly identified two suspects who perpetrated the network intrusions that provided Maksik with his database of illicit credit card numbers. The suspects were known online as "Johnnyhell" and "Segvec". Based on the forensics from the intrusion of the restaurant chain, Dave & Busters, and evidence recovered from Maksik's computer, "Jonnyhell" was identified as Alexander Suvorov. Following a coordinated international effort led by the USSS, Suvorov was arrested in Germany in March 2008, as he prepared to travel to Bali, Indonesia. In July 2009, Alexander Suvorov was extradited to the United States and has pled guilty to his involvement in the network intrusion of Dave & Busters.

Building on this success, CIS and other agents concentrated efforts on identifying the real world identity of "Segvec". Using traditional law enforcement techniques, agents linked "Segvec" and additional high level targets to multiple network intrusions including the TJX Corporation intrusion, acknowledged at the time to be the single largest compromise of customer credit card numbers and accounts in the Unites States. Working in unprecedented cooperation with the private sector, USSS agents associated Albert Gonzalez with the online moniker "Segvec".

In May 2008, USSS agents arrested Albert Gonzalez, and he was later indicted along with eight other co-conspirators for hacking into the wireless computer networks of TJX Corporation, BJ's Wholesale Club, OfficeMax, Barnes & Noble, Forever 21, Discount Shoe Warehouse, Boston Market, and Sports Authority. The defendants from the United States, Estonia, Ukraine, the People's Republic of China, and Belarus demonstrate the worldwide reach of this illicit community.

In January 2009, Heartland Payment Systems detected an intrusion in its processing system and learned of the subsequent theft of credit card data. The comprehensive USSS investigation revealed more than 130 million credit card accounts had been compromised and data was sent to a command and control server managed by an international group related to other ongoing USSS investigations. During the course of the investigation, the USSS revealed that this international group committed other intrusions into multiple corporate networks from which they stole credit card and debit card data. The USSS relied on a variety of investigative methods, including computer forensics, log analysis, malware analysis, search warrants, Mutual Legal Assistance Treaties with our foreign law enforcement partners, and subpoenas to identify three main suspects. Albert Gonzalez was again found to be involved, and in August 2009, Gonzalez and two other suspects were charged for their involvement in the data breaches into Heartland Payment Systems, 7-11, JC Penny, Wet Seal, and Hannaford Brothers.

In March 2010 Albert Gonzalez was sentenced to 20 years in prison for his involvement in these data breaches. This investigation to date is the largest data breach in United States history and also represents the longest sentence for a cyber criminal.

About Verizon Investigative Response

Security breaches and the compromise of sensitive information are a very real concern for organizations worldwide. When such incidents are discovered, response is critical. The damage must be contained quickly, customer data protected, the root causes found, and an accurate record of events produced for authorities. Furthermore, the investigation process must collect this evidence without adversely affecting the integrity of the information assets involved in the crime.

The IR team has a wealth of experience and expertise, handling over 650 security breach and data compromise cases in the last six years. Included among them are many of the largest breaches ever reported. During these investigations, the team regularly interacts with governmental agencies and law enforcement personnel from around the world to transition case evidence and set the stage for prosecution. The expansive data set generated through these activities offers an interesting glimpse into the trends surrounding computer crime and data compromise.

About the United States Secret Service

As the original guardian of the nation's financial payment system, the United States Secret Service has established a long history of protecting American consumers, industries and financial institutions from fraud. Over the last 145 years, our investigative mission and statutory authority have expanded, and today the Secret Service is recognized worldwide for our expertise and innovative approaches to detecting, investigating and preventing financial and cyber fraud.

Today's global economy has streamlined commerce for both corporations and consumers. Financial institutions and systems are readily accessible worldwide. Today's financial fraud and cybercriminals have adapted to this new means of global trade and seek to exploit this dependence on information technology. Cybercriminals consequently have become experts at stealing stored data, data in transit, and encrypted data. They operate based on trust, long standing criminal relationships, high levels of operational security, and reliability. The culture also has evolved over the last decade and is now described as non-state sponsored, transnational and is almost impossible to infiltrate due to its dynamic nature and operational security.

To combat these emerging threats, the Secret Service has adopted a multi-faceted approach to aggressively combat cyber and computer related crimes by establishing a network of 29 Electronic Crimes Task Forces (ECTF), including the first international ECTF located in Rome, Italy, 38 Financial Crimes Task Forces (FCTF) and a Cyber Investigations Branch. This approach enables the Secret Service to detect, prevent, and aggressively investigate electronic crimes including cyber attacks on the nation's critical infrastructures and financial payment systems.

In Fiscal Year 2009, agents assigned to Secret Service offices across the United States arrested more than 5,800 suspects for financial crimes violations.

For more information or to report a data breach, please contact your local Secret Service office: www.secretservice.gov.

Cyber Intelligence Section

The Cyber Intelligence Section (CIS) of the Secret Service was founded in 2005 to combat trends in fraud and identity theft. The CIS serves as a central repository for the collection of data generated through the agency's field investigations, open source Internet content and a variety of information obtained through financial and private industry partnerships as it relates to identity theft, credit card fraud, bank fraud, and telecommunications fraud.

CIS leverages technology and information obtained through private partnerships, to monitor developing technologies and trends in the financial payments industry that may enhance the Secret Service's abilities to detect and mitigate attacks against the financial and telecommunications infrastructures. CIS penetrates, disrupts and dismantles online criminal networks, investigates and coordinates network intrusion investigations, and provides case agents with actionable intelligence to support their investigations.

How does the Secret Service get involved in a data breach investigation?

The Secret Service is the only entity within the Department of Homeland Security that has the authority to investigate violations of Title 18, United States Code, Section 1030 (Computer Fraud). Congress also directed the Secret Service in Public Law 107-56 to establish a nationwide network of Electronic Crimes Task Forces (ECTFs) to "prevent, detect, and investigate various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." Members of ECTFs include academic partners, international, federal, state and local law enforcement partners, and more than 3,100 private sector partners.

Furthermore, the methodology employed by CIS has prevented data theft by providing intelligence recovered during criminal investigations to assist victim companies in mitigating further exposure of their network assets.

THE LEGAL DUTY TO PROVIDE INFORMATION SECURITY: WHO, WHAT, WHEN, WHERE, AND HOW

J.("JAY") T. WESTERMEIER
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP
Two Freedom Plaza
11955 Freedom Drive
Reston, VA 20190-5675
jay.westermeier@finnegan.com
Tel: 571-203-2480

Prepared For:

D.C. Bar
Continuing Legal Education Program
D.C. Bar Conference Center
1101 K Street, NW, 1st Floor
Washington, DC 20005

August 10, 2010

Information Security*

By

J.T. Westermeier**

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification and destruction.[1] Information security has become a critical legal issue. Security is an essential element of privacy. The risks of computer hackers, computer viruses and worms, identity theft, denial of service attacks, theft, terrorist attacks, sabotage, surveillance and intrusion by competitors and malicious acts by disgruntled employees, among other vulnerabilities, are increasing at an alarming exponential rate. There has been a blistering rise of Internet threats in recent years. Not only are security solutions essential for protecting information and privacy in a networked economy; they are also critical enablers for the development of e-business. Managing the risks from these unprecedented threats to the enterprise has become a vital risk management concern for the

* The article is adapted from Section 15.03 on information security written by J.T. Westermeier and published in Supplement to Computer Contracts by Esther Roditti (August 2009).

** J.T. Westermeier is of counsel in the Reston, Virginia office of Finnegan, Henderson, Farabow, Garrett & Dunner, LLP. He is past President of the International Technology Bar Association (formerly known as the Computer Law Association); Life Fellow, American Bar Foundation; 2001 Burton Award for Legal Achievement; and a member or former member of the advisory boards for E-Commerce Law & Strategy, Computer Law Reporter, BNA's Computer Technology Law, BNA's Electronic Commerce & Law, GIS Law; The Commercial Law Advisor, Intellectual Property Counselor, Internet Law and Business, and Information Strategy: The Executives Journal. He is listed in Intellectual Asset Management magazine's "IAM250-The World's Leading IP Strategists" (2009-2010); The International Who's Who of Internet and e-Commerce Lawyers (2009-2010); The International Who's Who of Business Lawyers, 2008, 2010; Best Attorneys in America (Information Technology; 2003-2010); Virginia Super Lawyers (Intellectual Property; 2006-2010); Washington, D.C., Super Lawyers (Intellectual Property; 2007-2010); Super Lawyers Corporate Edition of Top Attorneys in Business Services (Intellectual Property; 2009); peer-rated "AV® Preeminent™ by Martindale-Hubbell, and many other honorary lists of distinction.

[1] The Federal Information Security Act of 2002 (44 U.S.C. § 3542) defines "Information Security" as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide - (A) integrity, which means guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information."

company's board of directors and top management, with the result that effective information security programs have become a legal necessity.

Prudent risk management and due care with respect to information security programs are necessary to avoid potential legal liability and adverse publicity. Information security is a continuous, never-ending risk management process to protect the confidentiality, integrity and availability of information systems and information content. Today many security defenses are applied in-depth or in layers.

In these materials I will discuss: (i) the expansion of the legal duty to provide security to information and communications systems; (ii) the evolving legal standard to provide "reasonable security" requiring a risk-based process to develop and maintain a comprehensive information security program; (iii) the duty to disclose security breaches to those who may be adversely affected by such breaches; and (iv) the Massachusetts "Standards for the Protection of Personal Information " Regulation. I will also discuss (i) recommended security practices; (ii) contractual protection; (iii) legal battle plans for information security incidents; (iv) forensic software: and (v) ethical considerations applicable to information security.

I. LEGAL DUTY TO PROVIDE SECURITY

A growing number of statutes provide the legal framework for the duty to provide information security in the U.S. These statutes require safeguards for sensitive information and incident response plans. The duty to provide security may come from different laws, jurisdictions and other sources.

The Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") protects sensitive consumer information relating to health information. All entities that handle protected health information, whether directly or indirectly, are required to comply with the security

ormation
rams are
rity is a
rity and
nses are
urity to
sonable
mation
versely
rsonal
actual
e: and
ovide
n and
laws,
tects
cted
rity

regulations set forth in the Department of Health and Human Services regulations implementing the security provisions of HIPAA in 2003. 45 C.F.R. Part 164.

The Gramm-Leach-Bliley Act of 1999 ("**GLBA**") protects the privacy of consumer financial information by placing obligations on financial institutions. The Federal Trade Commission (FTC), along with banking agencies and regulatory authorities, has promulgated regulations to implement the GLBA's requirements and restrictions. For example, the FTC's Safeguards Rule requires covered entities to maintain information security programs that include responding to attacks, intrusions or other system failures.

In early 2005, the FTC established the Disposal Rule that requires electronic files to be erased or destroyed in such a way that personal information (*e.g.,* credit report data, credit scores, employment histories, insurance claims, check-writing histories, residential or tenant histories and medical information) cannot be read or reconstructed.

The Sarbanes-Oxley Act of 2002 ("**SOX**") creates significant information security compliance obligations. Section 404 of the SOX Act requires corporate executives to certify regularly as to the adequacy of their companies' internal control over financial reporting. Without proper security measures, companies cannot confidently sign-off on their books or their internal controls. Therefore, information security has emerged as a crucial requirement for SOX compliance. Auditors assessing interval controls evaluate information technology controls, and more specifically security controls. Under SOX, there are significant possible criminal penalties for false and misleading statements by executives. Criminal penalties reach $5 million in fines and 20 years in prison.

The USA Patriot Act ("**Patriot Act**") requires a broad range of financial institutions to establish policies and procedures to help combat terrorism. Among many other measures, the Patriot Act requires that financial institutions adopt diligent internal auditing and investigation

procedures which necessitate adoption of an appropriate response plan and the use of the best available technology. Incident response procedures now require companies to quickly determine the "what, when, and how" of an attack by using the best available technology that allows a company to preserve the evidence immediately and investigate using appropriate forensic tools.

The electronic transaction laws (E-SIGN and UETA) require all companies to provide security for storage of electronic records relating to online transactions.

Evolving case law suggests that corporate directors, by virtue of their fiduciary obligations to the company, will find that their duty of care includes responsibility for the security of the company's information systems. *See, e.g., Caremark International, Inc. Derivative Litigation*, 698 A. 2d 959, 970 (Del. Ch. 1996).

A recent case respecting the admissibility of electronic records underscores the importance of information security. *See, e.g., American Express v. Vinhnee,* 2005 Bankr. LEXIS 2602 (9th Cir. BK App. Panel 2005).

ISO/IEC 27001, is an international information security system standard. It is one of the most widely used security standards. It was started by the British Standards Institute in 1995. This standard recognizes that information security is a relative concept and that a process-oriented approach to information security is the most appropriate process applied in each situation.

ISO/IEC 27001 requires that management:

- Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities and impacts;
- Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
- Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

ISO/IEC 27002 (the Code of Practice for Information Security Management) is often used together with the ISO/IEC 27001 standard. ISO/IEC 27002 provides additional information regarding controls. The ISO/IEC 27002 standards is divided into eleven control areas: (1) security policy, (2) organizing information security, (3) asset management, (4) human resources security, (5) physical and environmental security, (6) communication and operations, (7) access controls, (8) information systems acquisition/development/maintenance, (9) incident handling, (10) business continuity management and (11) compliance.

The Basel Committee on Banking Supervision ("**Basel Committee**") is the leading international financial standards-setting institute. The Basel Committee has promulgated important standards relating to electronic banking that should be considered more broadly even though they are not laws *per se*. In the Basel Committee's report relating to "Risk Management for Electronic Banking", the Basel Committee places the burden on the company's Board of Directors and management to achieve effective risk management. Under Principle 1 of the Basel Committee's Risk Management Principles, "The Board of Directors and senior management [are required to] establish effective management over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks." The second principle requires "[t]he Board of Directors and senior management … [to] review and approve the key aspects of the bank's security control process". There is no question that in today's information security risk environment that effective information security has become a Boardroom issue and a concern of top management. If a company fails to have an effective information security risk management strategy and incident response plan, the Board of Directors and senior management will be culpable if an incident occurs. As the Basel Committee notes, this culpability arises because the protection of assets is one of the Board's fiduciary duties and one of senior management's fundamental responsibilities.

The Basel Committee did not "attempt to dictate specific technical solutions" because of the evolving nature of technology and the resultant changing nature of best practices. In this regard, the Basel Committee recognized that "many security controls and other risk management techniques continue to evolve rapidly to keep pace with new technologies".

In essence, information security is no longer just good business practice. It is becoming a legal obligation and the legal liability standards are evolving.

Several recent developments provide support for the trend that every company now has (or will have) a legal obligation to provide security for its own information and communications.

1. The FTC has significantly broadened the scope of its enforcement actions by asserting that a failure to provide appropriate information security was, itself, an unfair trade practice in violation of Section 5 of the FTC Act. These FTC complaints and consent orders are discussed in depth in these materials.

2. States have enacted laws imposing a general obligation on all companies to ensure the security of personal information to "implement and maintain reasonable security procedures and practices" to protect personal information about state residents. *See, e.g.*, California, Arkansas, Maryland, Massachusetts, Nevada, Oregon Rhode Island, Texas and Utah. After January 1, 2009, a new Massachusetts data security regulation went into effect requiring, among other things, that businesses implement written comprehensive information security programs and encrypt sensitive personal data that is transmitted wirelessly or stored on mobile devices. The Massachusetts statute is discussed below.

3. Recent case law suggests there may be a common law to provide security protection, the breach of which constitutes a tort. *See, e.g., Wolfe v. MBNA America Bank,* 485 F.Supp. 2d 874, 882 (W.D. Tenn. 2007); *Guin v. Brazos Higher Education Service*, 2006 U.S. Dist. LEXIS 4846 (D. Minn. Feb. 7, 2006); *Bell v. Michigan Council*, 2005 Mich. App. LEXIS 353 (Mich. App.

Feb. 15, 2005). *In Re TJX Companies Retail Security Breach Litigation*, 2007 U.S. LEXIS 7723 (D. Mass. October 12, 2007), the court recognized a "negligent misrepresentation" claim on the grounds that the banks impliedly represented that they had taken reasonable security measures to safeguard personal and financial information. *In Re TJX Companies Retail Security Breach Litigation*, 564 F.3d 489 (1st Cir. May 5, 2009), the First Circuit held the defendants in this breach of information security identity theft case had standing to appeal the district court's ruling and the banks issuing credit cards and debit cards stated a claim for negligent misrepresentation and unfair or deceptive practices under Massachusetts law. However, the Court of Appeals held that the issuing banks' negligence claim was barred by the economic loss doctrine and that the issuing banks were not third party beneficiaries to agreements between the "processing banks" and the credit card companies. In the Complaint the issuing banks alleged that TJX and Fifth Third Bank had ignored security measures required by the credit card companies, i.e., that a firewall configuration be employed, stored data be protected, transmissions of cardholder data be encrypted, and access to cardholder data and network resources be tracked. The First Circuit believed the Federal Trade Commission complaints and consent decrees condemning as "unfair conduct" similar to the conduct charged by plaintiffs to be relevant. The First Circuit noted that there is a substantial body of FTC complaints and consent decrees relating to inadequate information security practices to be instructive rather than conclusive, unfair and deceptive practices covered by Chapter 93A of the Massachusetts law. The Court of Appeals does not believe the FTC information security cases should be ignored. These FTC cases provide useful guidance that may be used by courts. They are discussed at length in these materials.

The plaintiffs argued that by accepting credit cards and payment authorizations the defendants impliedly represented that they would comply with the credit card company regulations. The First Circuit also determined that the issuing banks were not third-party

beneficiaries to the contracts between the participating banks and VISA and MasterCard that bound the participating banks to certain security procedures. Here the agreements in question expressly provided that they were not for the benefit of and may not be enforced by any third party.

Another case is *In Re Hannaford Bros. Co. Customer Data Security Breach Litigation*, 2009 WL 1325056 (D. Me. May 12, 2009). This case addresses the issue of whether a customer can recover from a grocer any loss resulting from the third-party data theft of electronic payment data from the grocer. Does the customer have a cause of action against a retailer who is the victim of a data theft involving the customer's personal information?

The plaintiffs claim that wrongdoers obtained access to Hannaford's information technology systems and stole an estimated 4.2 million debit card and credit card numbers, and other personal information.

The court found that in a grocery transaction where a customer uses a debit or credit card, a jury could find that Hannaford is subject to an implied contractual term that it will use reasonable care in its custody of the consumers' card data, the same level of care as the negligence tort standard discussed in this ruling.

The complaint alleged that Hannaford's technology system had multiple short falls, including but not limited to: (i) lack of proper monitoring solutions; (ii) failure to encrypt internal network traffic flowing between store and processor; (iii) point-of-sales systems that were open to attack; (iv) insecure wireless connections; and/or (v) remote access deficiencies.

The court concluded that it was unlikely that the Maine courts would extend Maine law to apply an implied, warranty of fitness to a grocer's electronic payment processing systems.

The district court makes reference to the FTC website and FTC complaints charging companies with security deficiencies, alleging that companies failed to use reasonable and

appropriate security measures to prevent unauthorized access to personal information stored on computer networks, in violation of the Federal Trade Commission Act. The district court concluded that the FTC interpretation in these information security cases, as recognized by the First Circuit in the TJX Massachusetts case, support accepting the allegations here as stating a claim under Maine's Unfair Trade Policies Act that declare unfair or deceptive acts or practices in the conduct of any trade or commerce to be unlawful. The plaintiffs alleged that Hannaford's failure to disclose the data theft promptly was unfair and deceptive.

The court then focused on "cognizable injury" for the three claims that survive under Maine law. The court concluded that consumers who did not have a fraudulent charge actually posted to their account cannot recover. Furthermore, the court did not permit damages that were too remote to justify a damage award.

Thus, the court concluded under current Maine law, consumers whose payment data are stolen can recover against the merchant only if the merchant's negligence caused a direct loss to the consumer's account. The threat of a loss is insufficient by itself to permit consumers to recover.

4. Several states have enacted laws requiring the encryption of social security numbers in the event they are communicated over the Internet.

5. There are regulations and laws to destroy data in a secure manner. Banking regulators, the SEC and the FTC have adopted regulations regarding the destruction of personal data. At least eight states have adopted similar requirements. Maryland is one of these states. Maryland requires a business when destroying a customer's records containing personal information to take reasonable steps to protect against unauthorized access to or use of the personal information.

6. Most states have enacted security breach notification statutes requiring that business notify citizens if their "personal information" is compromised or may have been compromised.

These statutes are in response to the tremendous increase in identity theft related to breaches of information security and are discussed in Section VI of this article.

7. Security is a condition of admissibility of electronic business records.

More and more reasons for businesses to encrypt their computerized records are becoming apparent. The principal driver for encryption has been the need to protect information against unauthorized access. Recently, another strong reason for encryption has arisen in connection with establishing the necessary evidentiary foundation to support the admissibility of computerized business records in legal proceedings. The growing importance of concerns about demonstrating the accuracy, reliability and integrity of computerized business records was demonstrated by *Vinhnee v. American Express Travel Related Services Company, Inc.*, 2005 Bankr. LEXIS 2602 (9th Cir. BK App. Panel 2005). Here, American Express lost the case against the debtor in the bankruptcy proceeding because American Express did not establish the continuous accuracy, integrity and reliability of its computerized monthly billing statements regarding the debtor. As such, the trial court refused to admit the evidence American Express was relying upon. This case points to a significant change in the way courts view computerized evidence.

In this ruling by the Ninth Circuit Court of Appeals Appellate Bankruptcy Panel, the Panel noted that the electronic nature of computer records requires an additional authentication foundation to assure the continuing accuracy of the records. The need for more extensive authentication of electronic records arises in part because digital technology makes it easier to alter the text of documents scanned into a database. This ruling teaches that the additional evidentiary foundation for computerized business records will need to address how access to the database is controlled and how changes to the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing

integrity of the database. These additional requirements have become necessary to demonstrate that records have not been changed since their creation. The Ninth Circuit observes that authenticating electronic records requires one to demonstrate that the record retrieved from the file is the same record that was originally placed in the file.

Since more than 93% of business records are maintained as electronic records, these additional evidentiary requirements for computerized records are likely to affect the way electronic records are maintained and used in court. The need to establish the continuing accuracy and integrity of records for them to be admissible as business records in legal proceedings may further lead businesses to use encryption methods in storing such records.

II. EMERGENCE OF A LEGAL STANDARD

The key issue from a legal perspective is defining the scope and extent of a company's "legal" obligation to implement information security measures. The FTC cases respecting information security are very instructive, as acknowledged by several courts considering liability claims relating to information security.

The FTC levied the largest fine in its history against Choicepoint, Inc. for the company's failure to protect consumer privacy and for violations of federal law. In the Choicepoint FTC matter, at least 163,000 consumers had their personal information compromised and at least 800 of those consumers became victims of identity theft, which in 2005 as well as in recent years was the country's fastest growing crime. In this proceeding, Choicepoint was ordered to pay $10 million in civil penalties and $5 million in consumer redress to settle the FTC's charges. Choicepoint's FTC settlement required it to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes and to establish a

"comprehensive information security program".[2] Below we will examine the evolving meaning of what constitutes a comprehensive information security program based on these FTC consent orders.

1. Overview of FTC Cases.

In all of these FTC cases, the FTC entered into a Consent Order with the respondent company requiring the company to establish, implement and thereafter maintain a "comprehensive information security program" that is "reasonably designed to protect the security, confidentiality and integrity of personal information collected from or about consumers." The FTC requires that the company's information security program "contain administrative, technical and physical safeguards appropriate to the respondent's size and complexity, the nature and scope of respondent's activities and the sensitivity of the personal information collected from or about consumers." While the FTC's focus in these consent orders is on protecting consumer information, the applicability of the consent orders is much broader. These FTC consent orders help to set the minimum legal standards for information security programs and are of extreme importance to the legal community.

Adequate security means that companies maintain effective security that is commensurate with risk, including the magnitude of harm resulting from unauthorized access, use, disclosure, disruption, impairment, modification or destruction of information. In each of these FTC cases, the FTC has required the respondent companies to implement a "comprehensive information security" program. The "comprehensive information security" program required by the FTC has evolved over time but in essence consists of the following elements:

[2] *United States v. ChoicePoint, Inc.* (Stipulated Final Judgment, FTC File No. 052-3069, N.D. Ga. Jan. 26, 2006).

(1) Accountability. Companies should designate an employee or employees to coordinate and be accountable for the information security program.

(2) Risk Assessment. Companies should identify reasonably foreseeable material risks, both internal and external, to the security, confidentiality and integrity of information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and do an assessment of the sufficiency of any safeguards in place to control those risks. At a minimum, the risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures. The employee training risks should include the risks posed by lack of training and failure to screen employees.

(3) Safeguards. Companies should design and implement reasonable safeguards to control the risks identified through risk assessment, and conduct regular testing or monitoring of the effectiveness of the safeguards' key controls, systems and procedures. This element includes both the implementation of safeguards and regular testing or monitoring to verify the effectiveness of these safeguards.

(4) Service Providers. Companies should develop and use reasonable steps to retain service providers capable of appropriately safe guarding protected information they receive from the Companies and require service providers by contract to implement and maintain appropriate safeguards.

(5) Maintenance. Companies should evaluate and adjust their information security program in light of the results of testing and monitoring, any material changes to operations or

business arrangements, or any other circumstances that the company knows or has reason to know may have a material impact on the effectiveness of its information security program.

The foregoing elements are present in each of the "comprehensive information security programs" the FTC has required companies to set up. The more recent FTC consent orders relating to information security have also required a regular audit or assessment of the Company's required information security program.[3] In one of the more recent consent orders, the respondent company is required to "obtain an assessment and report" an 'Assessment' from a qualified, objective independent third-party professional, using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biennially thereafter for twenty (20) years after service of the order. "The third-party professional is required to certify" that respondent's security program is operating "with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, has so operated throughout the reporting period." The FTC requires that each independent assessment "be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network Security (SANS) Institute; or a similarly qualified person or organization" approved by the FTC. This outside audit may be viewed as a sixth element of the minimum requirements that should be met by the comprehensive information security program.

[3] The Federal Information Security Management Act includes a requirement for agencies to conduct an annual review and independent assessment by agency inspectors general.

2. Suggested Best Practices.

These FTC consent order cases also suggest some best practices that should be considered. We believe these cases are very instructive. While the FTC cases relate to personal information, most of the defective practices identified could relate to any form of protected information. Summaries of these cases are included below. I will address below the insufficient practices identified by the FTC in these cases in the context of the management framework for a comprehensive information security program.

Many of the deficient information security practices identified by the FTC concerned risk assessments. One company was alleged to have failed to assess risks to the information collected and stored both online and offline.[4] Others failed to assess the risks related to inadequate access controls, employee screening, employee training, disposal of information, and website attacks. Others failed to assess the risks related to the failure to encrypt information in transmission and in storage, and otherwise assess the risks applicable to data retention practices. Others concerned the failure to implement detection measures, response plans and measures to minimize any losses, regular audit or monitoring procedures, and security investigation processes. Others failed to provide oversight to contractors and otherwise manage service providers.

3. Risk Assessment.

Risk assessment is a very critical component of the management process for information security. It needs to be continually updated. The process is never-ending. Risk assessments are viewed from a reasonable cost perspective. Where proven security controls were available at a relatively low cost, the FTC found the company had failed to protect information security adequately, especially where the FTC believes the risk should have been foreseeable. For

[4] *E.g.*, in the Analysis of the Proposed Consent Order to Aid Public Comments in *Nations Title Agency, Inc.*, File No. 0523117, the FTC noted a Kansas City television station had found sensitive documents discarded in a dumpster located in an unsecured area.

example, the failure to install firewalls at appropriate connections and use updated current virus-detection software is more likely to be viewed as a deficient practice because firewalls and virus detection software are widely used. Another example is the requirement to use access controls and intrusion detection systems.

Incident response plans need to be implemented as part of an overall security plan. These response plans needs to manage, contain and minimize problems from unexpected events. Proper incident response requires use of computer tools and training, a rapid forensic response, and collecting and preserving the evidence in a forensically sound manner. Now let's look at the specific FTC Consent Orders relating to information security programs.

The legal standard for information security can be formulated generally using an analytic model comparable to the analytical model used for negligence. Security procedures should be reasonable and appropriate under the circumstances. What is reasonable for a particular company will vary based, among other factors, upon its size and complexity, the nature of its business, and the sensitivity of the information it collects.[5]

Legal risk analysis requires that the gravity and probability of injury be balanced against the safeguards which could have been performed to avoid the injury. The procedure was aptly explained by Judge Learned Hand in a case which had nothing to do with information security — *United States v. Carroll Towing Co.*[6] This case involved a barge's liability for failure to watch over a barge which broke away from a pier after another barge's crew had shifted its morning lines. In the *Carroll Towing* case, the unattended, runaway barge ran into a tanker causing it to lose its cargo and sink. Under the circumstances, Judge Leonard Hand ruled that the owner's

[5] *See* "FTC Working to Protect Consumers and Businesses from Information Security Breaches", FTC Press Release, April 21, 2004.

[6] 159 F.2d 169 (2d Cir. 1947).

duty to provide against resulting injuries, as in other similar situations, is a function of three variables.[7]

1. The probability the barge will break away from its moorings.
2. The gravity of the resulting injury.
3. The burden of adequate precautions.

In the *Carroll Towing* case, the relationship among the three variables identified by Judge Learned Hand was expressed in the following terms:

If the probability be called P; the injury L; and the Burden B; liability depends upon whether B is less than L multiplied by P; *i.e.*, whether $B < PL$.[8]

This legal standard requires companies to conduct ongoing risk analyses of internal and external threats and implement simple, low-cost and readily available defenses and safeguards to cyberattacks and other risks. This legal standard will be clearer when examined in the context of the specific FTC "information security cases" below.

III. DEVELOPING LEGAL DEFINITION OF "REASONABLE SECURITY"

The following FTC cases illustrate the comprehensive process approach to information security. The process is never completed. It is ongoing and continually reviewed, revised, and updated. This "process oriented" legal standard for corporate information security has been widely adopted in a series of financial regulations required by the Gramm-Leach-Bliley Act.

The legal trend requires companies to develop comprehensive information security programs, but leaves the details to the facts and circumstances of each situation. The legal standard for assessing security risks and implementation of safeguards to protect these risks is similar to the legal analysis applicable to the legal liability for negligence.

[7] 159 F.2d at 173.

[8] *Id.*

Good security is an ongoing process of assessing risks and vulnerabilities. The risks companies must confront change over time. Companies must assess the risks they face on an ongoing basis and make constant adjustments to prevent or reduce those risks. Below we will discuss many of the FTC "information security" consent order cases.

(1) ***In the Matter of Twitter, Inc., (FTC File No. 092-3093 – June 24, 2010).***

In the Complaint, the FTC alleges that Twitter violated Section 5(a) of the FTC Act by falsely representing that it uses at least reasonable safeguards to protect user information and maintains at least reasonable safeguards to honor the privacy choices exercised by users, and by failing to provide reasonable and appropriate security to prevent unauthorized access to non-public user information and honor the privacy choices exercised by users who designated certain tweets as non-public.

The Complaint noted that since approximately July 2006, Twitter had operated a social networking website known as www.twitter.com. Using this Twitter website the Complaint states that users are able to send "tweets", which are brief messages of 140 characters or less to users who sign up to receive such messages via email and phone text. The Complaint observes that Twitter offers privacy settings through which a user may designate tweets as non-public. In addition, Twitter collects certain non-public user information, such as an email address, Internet Protocol ("IP") addresses, mobile telephone number (for users who receive messages by phone), and a username for any Twitter account that a user has chosen to "block" from exchanging tweets with any user.

In the Complaint the FTC alleges that Twitter failed to provide reasonable and appropriate security to prevent unauthorized access to non-public user information and honor the privacy choices exercised by users designating certain tweets as non-public. As the result of Twitter's security failures Twitter failed to prevent unauthorized administrative control of the

Twitter system. Many of Twitter's security failures related to passwords and other access controls.

Twitter allegedly failed to "establish or enforce policies to make administrative passwords hard to guess, including policies that: (1) prohibit the use of common dictionary words as administrative passwords; or (2) require that such passwords be unique – i.e., different from any password that the employee uses to access third-party programs, websites, and networks."

Twitter also allegedly failed to "establish or enforce policies sufficient to prohibit storage of administrative passwords in plain text in personal email accounts."

Another alleged password failure related to Twitter's failure to suspend or disable administrative passwords after a reasonable number of unsuccessful login attempts.

There was also concern regarding the failure to change passwords periodically. Twitter allegedly failed to "enforce periodic changes of administrative passwords, such as by setting [these] passwords to expire every 90 days.

Three other alleged Twitter security failures were alleged relating to access controls. First, Twitter allegedly failed to "provide an administrative login webpage that is made known only to authorized persons and is separate from the login webpage provided to other users." Second, Twitter allegedly failed to "restrict each person's access to administrative controls according to the needs of that person's job." Third, Twitter allegedly failed to "impose other reasonable restrictions on administrative access, such as by restricting access to specified IP addresses."

The FTC Complaint alleges that between January and May 2009 intruders were able to exploit these password and access control security failures by Twitter on two occasions to obtain unauthorized administrative control of the Twitter system. By acquiring administrative control

of the Twitter system the intruders were able to: (i) gain unauthorized access to nonpublic tweets and nonpublic user information, and (ii) reset any user's password and send unauthorized tweets from any user account.

In the Complaint the FTC references several particular instances relating to the actions the intruders were able to carry out based on the alleged security failures. On or about January 4, 2009 the Complaint states an intruder used an automated password guessing tool to derive an employee's administrative password, after submitting thousands of guesses into Twitter's public login webpage. The "guessed" password was a weak, lowercase, letter-only, common dictionary word. Using this password, the intruder was able to access non-public user information and non-public tweets for any Twitter user. The intruder was also able to reset user passwords. Some of these fraudulently - reset user passwords were obtained by other intruders and used to send unauthorized tweets from user accounts, including: according to the Complaint, one tweet purportedly from Barack Obama, that offered his more than 150,000 followers a chance to win $500 in free gasoline, in exchange for filling out a survey. According to the Complaint unauthorized tweets were sent from eight other user accounts, including the Fox News account.[9]

Another incident recited in the Complaint allegedly occurred on or about April 29, 2009 when an intruder was able to compromise a Twitter employee's personal email account by inferring the employee's Twitter administrative password, based on two similar passwords, which had been stored in the account, in plain text, for at least six months prior to the intruder's attack. Using this password, the intruder was able to access non-public user information and non-public tweets for any Twitter user and reset at least one user's password.

[9] It is interesting to speculate whether Twitter would have received the FTC complaint if an intruder had not implicated President Obama.

The Complaint contained two counts for alleged violations of the FTC Act. The first count related to false or misleading representations pertaining to the security measures Twitter claimed to use to prevent unauthorized access to non-public user information. The second count related to Twitter's alleged failure to use reasonable and appropriate security measures to honor the privacy choices exercised by users.

(2) ***In the Matter of Dave & Busters, Inc., (FTC File No. 082 3153 – March 25, 2010)***

Dave & Buster's is headquartered in Dallas, Texas, and owns and operates 53 restaurants and entertainment complexes in the United States under the names Dave & Buster's, Dave & Buster's Grand Sports Café and Jillians. According to the FTC Complaint against Dave & Buster, between April 30, 2007 and August 28, 2007 an intruder connected to Dave & Buster's computer networks numerous times without authorization, installed unauthorized software, and intercepted personal information in transit from in-store networks to Dave & Buster's credit card processing company.

FTC:WATCH identified the intruder as Albert Gonzalez. According to FTC:WATCH, Gonzalez and two foreign co-defendants would drive past retailers along U.S. 1 in Miami with a laptop computer. They would exploit vulnerable wireless signals at these retailers to access without authorization of the retailer's computer networks. They would then install sniffer programs that captured credit and debit card numbers as this personal information moved through Dave & Buster's computer systems.

The Dave & Buster's information security breach compromised approximately 130,000 credit or debit cards used by consumers in the United States. As of the date the FTC issued its complaint against Dave & Buster's issuing banks for the payment cards implicated by the data breach had collectively claimed several hundred thousand dollars in fraudulent charges on some of these implicated accounts.

In the Complaint, the FTC alleged that Dave & Buster's had engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for persona information on its computer networks. The FTC alleged that Dave & Buster's failure to provid reasonable and appropriate information security permitted the intruder to exploit th vulnerabilities described in the Complaint as discussed below.

The FTC alleged that Dave & Buster's had failed to employ sufficient measures to detec and prevent unauthorized access to computer networks or to conduct security investigations. Th intruder was able to access the Dave & Buster's computer networks repeatedly over a four month period. The length of this undetected "breach" period supports the FTC's allegatior While these alleged insufficient practices are general in nature the FTC mentions specificall two measures that could have been employed by Dave & Buster's that were not employed - a intrusion detection system and monitoring system logs. Since both of these protective measur were mentioned specifically by the FTC, companies should consider employing such measur in their information security programs.

The FTC also alleged that Dave & Buster's had failed to restrict third party access to i networks adequately. Several measures the FTC suggested to restrict third party access are restrict connections to specified IP addresses or grant access on a temporary, limited basi These methods for restricting third party access should be considered in connection wi information security programs.

The FTC also alleged that Dave & Buster's failed to monitor and filter outbound traff from its networks to block and filter the unauthorized export of sensitive personal informatio Monitoring outgoing traffic should be used where applicable to prevent the unauthorized expo of protected information.

The FTC also alleged that Dave & Buster's failed to use "readily available" security measures to limit access between in-store networks, such as by employing firewalls or isolating the payment card system from the rest of the corporate network. Firewalls are a proven "readily available" strategy that should be used to limit access. Similarly, critical systems that do not require connectivity should be isolated to reduce the risks resulting from connectivity. These strategies should be considered in your information security programs.

The FTC also alleged that Dave & Buster's failed to use "readily available security measures" to limit access to its computer network through wireless access points on the networks. Again, the FTC finds Dave & Buster's failure to use "readily available" information security measures under the circumstances to be insufficient.

(3) ***In the Matter of Genica Corporation, (FTC File No. 082 3113 – February 5, 2009)***

Genica Corporation, Compgeeks.com d/b/a Computer Geeks Discount Outlet and geeks.com are engaged in the business of selling computer systems, peripherals, and consumer electronics to consumers over the Internet through www.geeks.com. In selling products through the www.geeks.com website the Respondents collected sensitive personal information from consumers to obtain authorization for credit card purchases. Respondents stored this personal information in clear, readable text on their corporate computer network accessible through the www.geeks.com website.

For a period of at least six months in 2007, hackers were able to exploit repeatedly the failures of the Respondents to guard against SQL injection attacks on the www.geeks.com website and web application. Through these attacks, the hackers were able to access unencrypted personal information on Respondents' network and export the information of hundreds of customers, including credit card numbers, expiration dates, and security codes, over the Internet to outside computers.

The FTC alleged that Respondents had engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the personal information on their network. Among other things, the FTC specifically alleged that the Respondents (i) had stored personal information in clear, readable text that should have been stored in encrypted form; (ii) did not adequately assess the vulnerability of their web application and network to commonly known or reasonably foreseeable attacks, such as "Structured Query Language" ("SQL") injection attacks; (iii) did not implement simple, free or low-cost, and readily available defenses to such attacks; (iv) did not use readily available security measures to monitor and control connections between computers on the network and from the network to the Internet; and (v) failed to employ reasonable measures to detect and prevent unauthorized access to personal information, such as by logging or employing an intrusion detection system.

(4) ***In the Matter of Premier Capital Lending, Inc., (FTC File No. 0723180 – November 6, 2008).***

Premier Capital Lending, Inc. ("PCL") is a mortgage lender that specializes in loans to fund the combined purchase of real estate and manufactured homes. PCL permitted a seller of manufactured homes to have access to consumer reports from a consumer reporting agency through PCL's online portal.

In 2006 a hacker obtained access to the seller's computer system and obtained the PCL-issued login credentials to the consumer reporting agency. Using this login, the hacker obtained credit reports on consumers who were not PCL customers. Once PCL determined the hacker's requests were unauthorized, PCL terminated the seller's login authorization, notified law enforcement and sent breach notification letters to the consumers whose reports the hacker had obtained.

The FTC claimed that PCL had failed to: (i) access the risks of allowing a third party to access consumer reports through PCL's account; (ii) implement reasonable steps to address that these appropriate data security measures were present; (iii) conduct reasonable reviews of consumer report requests made on PCL's account, using readily available information (such as management reports or invoices) for signs of unauthorized activity, such as spikes in the number of requests made on the account or made by particular PCL users or blatant irregularities in the information used to make the requests; and (iv) access the full scope of consumer report information stored and accessible through PCL's account and, thus, compromised by the hacker.

(5) ***In the Matter of the TJX Companies, Inc., (FTC File No. 0723055 – March 27, 2008).***

TJX is an off-price retailer selling apparel and home fashions in over 2500 stores worldwide, including T.J. Maxx, Marshalls, A.J. Wright, Bob's Stores and HomeGoods stores. Customers pay for purchases using credit cards, debit cards, cash and personal check. TJX maintains a computer network linking its stores. These networks are used to process sales transactions and provide wireless access to the networks for wireless devices. In connection with these purchases, TJX collects sensitive personal information. Apparently, TJX's problems were attributable to its Wi-Max wireless access devices.

Since at least July 2005, FTC claimed TJX had engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its networks. In particular, the FTC claimed TJX: (i) created an unnecessary risk to personal information by storing it on, and transmitting it between and within, in-store and corporate networks in clear text when it should have been encrypted; (ii) did not use readily available security measures to limit wireless access to its networks, thereby allowing an intruder to connect wirelessly to in-store networks without authorization; (iii) did not require network administrators and other users to use strong passwords or to use different passwords to access

different programs, computers, and networks; (iv) failed to use readily available security measures to limit access among computers and the Internet, such as by using a firewall to isc authorization computers; and (v) failed to employ sufficient measures to detect and prevent unauthorized access to computer networks to conduct security investigations, such as by patching or updating anti-virus software or following up on security warnings and intrusion alerts.

As the result of TJX's inadequate security, intruders were able to access TJX's netwo without authorization, install hacker tools, download personal information stored in clear text remote computers, and intercept payment card authorization requests in transit from in-store networks to TJX's central corporate network. The breach of security compromised tens of millions of unique payment cards used by consumers in the United States and Canada. In addition, the breach compromised the personal information of approximately 455,000 consum who had made unreceipted merchandise returns.

(6) ***In the Matter of Reed Elserveir, Inc. and SEISINT, Inc., (FTC File No. 0523094 – March 27, 2008).***

Reed Elserveir, Inc. (REI) acquired Seisint in 2004 and has operated Seisint as a wholl owned subsidiary within LexisNexis. Seisint and REI have engaged in the business of collecting, maintaining and selling information about consumers. Seisint sells verification products under its "Accurent" trade name and REI sells similar verification products under various LexisNexis trade names. These verification products are used by insurance companies debt collectors, employers, landlords, law firms, law enforcement and other government agencies. The verification products collect and aggregate information about millions of consumers and businesses from public and nonpublic sources. Through these products customers are able to search electronically for information maintained in computer databases.

Customers pay a fee to search for and retrieve information from these verification product databases.

Under Seisint's and REI's procedures an unauthorized person logging-in with user credentials of a legitimate verification product customer would be authenticated and could then access all of the information the legitimate customer could access, including sensitive nonpublic information if the customer were authorized to receive this information. In particular, the FTC claimed Seisint and REI had failed to establish or implement reasonable policies and procedures governing the creation and authentication of user credentials for authorized customers accessing the verification product databases.

The FTC claimed that Seisint and REI had failed to establish user ID and password structures that created an unreasonable risk of unauthorized access to sensitive consumer information stored in their verification product databases. On multiple occasions, the FTC asserted attackers had obtained user credentials of legitimate customers that were used to make thousands of unauthorized searches for consumer information on these verification product databases. Since March 2005, REI, through LexisNexis, has notified over 316,000 consumers that the attacks disclosed sensitive information about them that could be used to conduct identity theft.

(7) ***In the Matter of Goal Financial, LLC (FTC File No. 072 3013 – March 4, 2008).***

Goal Financial markets and originates a variety of student loans and provides loan related services. In connection with its business, Goal Financial collects sensitive personal information from consumer loan applications and other sources, and retains this personal information in paper documents as well as in an electronic database.

The FTC found that Goal Financial had engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumers' sensitive personal

information, including social security numbers, dates of birth, and income and employment information.

In particular, the FTC found that Goal Financial had failed: (i) to assess adequately r to the information it collected and stored in its paper files and on its computer network; (ii) t restrict access adequately to authorized employees with respect to personal information store its paper files and on its computer network; (iii) to implement a comprehensive information security program, including reasonable policies and procedures in key areas such as the collection, handling, and disposal of personal information; (iv) to provide adequate training employees about handling and protecting personal information and responding to security incidents; and (v) in a number of instances to require third-party service providers by contra protect the security and confidentiality of personal information. The FTC noted as example these failures that employees without authorization removed more than 7000 consumer files transferred these files to third parties and that an employee sold to the public hard drives tha not been processed to remove the data on the drives, thus exposing in clear text the sensitive personal information of approximately 34,000 consumers.

The FTC filed its complaint against Goal Financial alleging that its security failures violated the Safeguards Rule promulgated by the FTC that became effective May 23, 2003. Rule requires financial institutions to protect the security, confidentiality and integrity of customer information by developing a comprehensive written information security program contains reasonable administrative, technical and physical safeguards, including: (1) design one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality and integrit customer information, and assessing the sufficiency of any safeguards in place to control th risks; (3) designing and implementing information safeguards to control those risks identifie

through the risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

The FTC also found that Goal Financial had violated the Privacy Rule, effective July 1, 2001, applicable to financial institutions by disseminating a privacy policy, including its security policies and practices that contained false or misleading statements regarding the measures implemented to protect consumers' personal information.

(8) ***In the Matter of Life Is Good, Inc. (FTC File No. 072 3046 – January 17, 2008).***

The Life Is Good respondents design and distribute retail apparel and accessories and operate a retail website. Since at least October 2005, the FTC alleged the Life Is Good respondents had engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for the consumer information stored on their network, including credit card numbers, expiration dates, and security codes. In particular, the FTC asserted that the respondents: (1) stored the consumer information in clear, readable text; (2) created unnecessary risks to consumer information by storing such information indefinitely on their network, without a business need, and by storing credit card security codes; (3) did not adequately assess the vulnerability of their web application and network to commonly known or reasonably foreseeable attacks, such as "Structured Query Language" (SQL) injection attacks; (4) did not implement simple, free or low-cost , and readily available defenses to such attacks; (5) did not use readily available security measures to monitor and control connections from the network to the Internet; and (6) failed to employ reasonable measures to detect unauthorized access to consumer information.

The FTC alleged that a hacker was able to exploit the above weaknesses by using SQL injection attacks on respondents' website and web application. Using these SQL attacks, the hacker was able to export to the hacker's browser consumer information for thousands of customers, including credit card numbers, expiration dates, and security codes.

(9) ***In the Matter of Guidance Software, Inc., (FTC File No. C-4187 – March 30, 2007).***

In the FTC's complaint against Guidance Software, Inc., the FTC alleged that Guidance Software had engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive personal information stored on Guidance Software's corporate network. In particular, the FTC asserted even though Guidance Software employed SSL encryption, Guidance Software: (1) stored the personal information in clear readable text; (2) did not adequately assess the vulnerability of its web application and network to certain commonly known or reasonably foreseeable attacks, such as Structured Query Language (or "SQL"); (3) did not implement simple, low cost and readily available defenses to such attacks; (4) stored in clear readable text network user credentials that facilitate access to sensitive personal information on the network; (5) did not use readily available security measures to monitor and control connections from the network to the Internet; and (6) failed to employ sufficient measures to detect unauthorized access to sensitive personal information.

The FTC alleged that a hacker had exploited the weaknesses set forth above by using SQL injection attacks to install common hacking programs on Guidance Software's corporate network. Using this method, the hacker obtained unauthorized access to information for thousands of credit cards. When Guidance Software became aware of the unauthorized access, the company took steps to prevent further unauthorized access, provided breach notification for customers for whom it had or could obtain addresses, and notified law enforcement.

The FTC found also that Guidance Software had misrepresented that it had implemented reasonable and appropriate measures to protect sensitive personal information it obtained from customers against unauthorized access. The FTC alleged in the complaint that Guidance Software's acts or practices violate Section 5(a) of the FTC Act.

In the Consent Order, Guidance Software was required to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality and integrity of personal information collected from or about consumers. The content of the program must be in writing and contain administrative, technical and physical safeguards appropriate to Guidance Software's size and complexity, and the nature and scope of its activities, and the sensitivity of the personal information collected.

(10) ***In the Matter of Nations Title Agency, Inc., (FTC File No. 052 3117 – May 10, 2006).***

The NTA respondents provide services in connection with financing home purchases and refinancing existing home mortgages. In providing these services, the FTC noted that the NTA respondents routinely obtain sensitive consumer information from banks and other lenders, real estate brokers, consumers, public records and others. It is interesting that the FTC referred to public record information in this context of sensitive consumer information.

The FTC found that the Respondents had failed to provide reasonable and appropriate security for consumers' personal information. The FTC found the Respondents' practices to be inadequate in the aggregate. First, the FTC found that the Respondents had failed to assess risks to the information they collected and stored both online and offline. It is important to stress that information security risks apply to both online and offline collection and storage.

Second, the FTC alleged that the NTA respondents had failed to implement reasonable policies and procedures in key areas, such as employee screening and training and the collection, handling and disposal of personal information. The FTC noted sensitive personal information

had been discarded in Respondents' dumpster in an unsecured area. Information secur programs need to include the secure disposal of protected information.

Third, the FTC alleged that Respondents had failed to implement simple, low-cc readily available defenses to common website attacks, or to implement reasonable acc controls, such as strong passwords, to prevent a hacker from gaining access to Responden computer network. The FTC noted that a hacker had exploited the Respondents' failure implement available defenses to common website attacks by using a common website attack obtain unauthorized access to personal information. The failure to employ available, cc effective defenses is likely to be viewed as inadequate information security. If protection can obtained at a reasonable cost it should be obtained.

Fourth, the FTC alleged that the NTA respondents had failed to employ reasonal measures to detect and respond to unauthorized access to protected information or to cond security investigations. It should be noted that both detection of and response to unauthoriz access are included. Information security includes response plans and measures to minimize a losses.

Fifth, the FTC alleged the NTA respondents had failed to provide reasonable oversi for the handling of protected information by service providers. The management of contract is a critical component of information security programs.

(11) ***In the Matter of CardSystems Solutions Inc. (FTC File No. 05223148 – September 5, 2006).***

The FTC Consent Order in this matter applies to CardSystems Solutions, Inc. and i successor Solidus Networks, Inc., doing business as Pay By Touch Solutions.

CardSystems provides merchants with products and services used to obtain authorizati for credit and debit card purchases from banks issuing credit cards. CardSystems provid

authorization processing for card purchases in 2005 totaling at least $15 billion for approximately 119,000 merchants. In providing these services, CardSystems used the Internet and a web application program to provide information to client merchants.

The FTC alleged that a number of practices engaged in by CardSystems, when taken together, failed to provide reasonable and appropriate security for personal information stored on its computer network.

First, the FTC alleged that CardSystems created unnecessary risks to the information by storing it in a "vulnerable" format for up to 30 days. The FTC probably would not have challenged CardSystems' information storage practices if CardSystems had stored the information in encrypted form. This FTC allegation supports the general principle that information should be retained for only so long as the information is needed or legally required. To the extent protectable information is stored and retained, it should be encrypted.

Second, the FTC alleged that CardSystems had failed to assess adequately the vulnerability of its web application and computer network to "commonly known" or "reasonably foreseeable attacks", including, but not limited to "Structured Query Language" (or SQL) injection attacks. The FTC noted that in 2004 a hacker had exploited CardSystems' web application and website using an SQL injection attack to install common hacking programs on computers on CardSystems' computer network. In November 2004, these hacker programs were set up to collect and transmit magnetic stripe credit and debit card data stored on the network to computers located outside the network every four days. As a result, the hacker obtained unauthorized access to magnetic stripe data for tens of millions of credit and debit cards.

Third, the FTC alleged that CardSystems had failed to implement "simple, low-cost, and readily available defenses" to the SQL injection attacks. Simple, low-cost and readily available control measures need, at a minimum, to be implemented when risks are foreseeable. Liability

for inadequate information security practices is more likely to be assessed where cost-effective solutions were readily available but not implemented.

Fourth, the FTC alleged that CardSystems had failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network. Password policies are a very important part of information security programs, including the use of strong passwords that are frequently changed.

Fifth, the FTC alleged that CardSystems did not use "readily available security measures to limit access between computers on its network and between such computers and the Internet".

Sixth, the FTC alleged that CardSystems failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.

(12) ***In the Matter of DSW Inc. (FTC File No. 052-3096 – March 14, 2006).***

DSW is a footwear retailer selling footwear for men and women at approximately 190 stores in 32 states. DSW collects customer information at the cash register and wirelessly transmits the information, formatted as an authorization request, to a computer network located in the store and then transmitted to the appropriate bank or check processor. DSW operates wireless access points through which the cash registers connect to in-store computer networks.

The FTC alleged based on a number of shortcomings that DSW had failed to provide reasonable and appropriate security for personal information collected at its stores. First, the FTC alleged DSW created unnecessary risks to the information by storing personal information in multiple files when it no longer had a business need to keep the business information.

Second, the FTC alleged DSW did not use readily available security measures to limit access to its computer networks through wireless access points on the networks.

Third, the FTC alleged DSW had stored information in unencrypted files that could be accessed easily by using a commonly known user ID and password. Not only is encryption

desired to protect the confidentiality of information that is accessed without authorization, it also is desired to protect the integrity of information so that it is not altered improperly.

Fourth, the FTC alleged DSW did not limit sufficiently the ability of computers on one store's network to connect to computers on other in-store and corporate networks and failed to employ sufficient measures to detect unauthorized access. As a result, a hacker could use the wireless access points on one in-store computer network to connect to, and access personal information on, the other in-store and corporate networks.

(13) ***In the Matter of Superior Mortgage Corp. (FTC File No. 0523136 – September 28, 2005).***

Superior Mortgage Corp. is a direct lender of residential mortgage loans. It conducts business through 40 branch offices in 10 different states, as well as through six separate websites.

The FTC alleged that Superior Mortgage violated the Safeguards Rule requiring financial institutions to protect the security, confidentiality and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical and physical safeguards. The comprehensive information security program requirements follow the requirements contained in other FTC information security cases.

In the *Superior Mortgage* matter, the FTC emphasized the need for "regular" testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems and procedures. With respect to service providers, the FTC emphasized the need to "oversee" service providers and to require them by contract to protect the security and confidentiality of customer information. Information security needs to be considered in most service provider contracts and other contracts.

The FTC alleged that Superior Mortgage had violated the Safeguards Rule issue pursuant to the Gramm-Leach-Bliley Act for a number of reasons. The FTC alleged tha Superior Mortgage had failed to assess risks to its customer information until more than one yea after the Safeguards Rule's effective date.

Second, the FTC alleged that Superior Mortgage had failed to institute appropriat password policies to control access to company systems and documents containing sensitiv customer information.

Third, the FTC alleged that Superior Mortgage had failed to encrypt or otherwise prote sensitive customer information sending it by email. The FTC noted that while Superi Mortgage encrypted information while it was being transmitted between a visitor's web brows and the website's server (using SSL), once the information reached the server, it was decrypt and emailed to respondent's headquarters and branch offices in clear, readable text.

Fourth, the FTC alleged that Superior Mortgage had failed to take reasonable steps ensure that its service providers were providing appropriate security for customer informat and addressing known security risks in a timely fashion. In some circumstances, the need overseeing information security compliance by service providers will require monitoring possibly an information security audit.

(14) ***In the Matter of BJ's Wholesale Club, Inc. (FTC File No. 042-3160 – June 16, 200***

In the FTC case against BJ's Wholesale Club, Inc. ("BJ's"), the FTC found that BJ's computer networks to request and obtain authorization for credit card and debit card purchas its stores, and that BJ's collected personal information to authorize these purchases. The alleged that BJ's failed to employ reasonable and appropriate measures to secure pers information collected at its stores.

Among other things, the FTC alleged that BJ's failed to encrypt the personal information while in transit or when stored on the in-store computer networks. Encryption has become a required practice when it comes to personal information. Cases like ChoicePoint dictate that encryption be used for all personal information and other sensitive or confidential information.

The FTC also alleged that BJ's stored personal information in files that could be accessed anonymously – that is, using a common known default user ID and password. Reasonable access controls were not implemented by BJ's.

The FTC further alleged that BJ's did not use readily available security measures to limit access to its computer networks through wireless access points on the networks. Where security measures are "readily available", companies should be aware of their availability and use them.

The FTC also claimed that BJ's failed to employ sufficient measures to detect unauthorized access or conduct security investigations. Detection and security investigations need to be an integral part of information security programs.

The FTC further found that BJ's had created unnecessary risks to the personal information by storing it for up to 30 days when it no longer had a business need to keep the information. Storing this information under these circumstances also violated bank rules. It is important for companies to recognize the risks associated with storing information that is not needed. Record retention policies should reflect the risk of maintaining information longer than it is needed.

Under these circumstances, the FTC found that hackers could have used the wireless access points on an in-store computer network to connect to the network and, without authorization, access personal information on the network.

Problems with BJ's information security practices were discovered by the banks who had issued credit cards to BJ's customers. During 2003 and 2004, banks began discovering

fraudulent purchases that were made using counterfeit copies of credit and debit cards the banl had issued to customers. Counterfeit copies of cards were used to make millions of dollars (fraudulent purchases. According to BJ's SEC filing, as of May 2005, the amount of outstandir claims against BJ's from banks and credit unions was approximately $13 million.

BJ's inadequate information security practices have resulted not only in the FTC actic but also in cases by banks and credit unions seeking to recover the return of the millions (dollars in fraudulent purchases and operating expenses. These operating expenses related in pa to the cancellation and reissuance of thousands of credit and debit cards that had been used ; BJ's stores.

(15) ***In the Matter of Petco Animal Supplies, Inc. (FTC File No. 032-3221 – November 17, 2004).***

Petco sells pet food, supplies and services. It has marketed and sold pet food an supplies to consumers through its website since February 2001. Most customers who mak purchases through the Petco website pay using a credit card.

The FTC Complaint states that Petco's website and application have been vulnerable t attack from third parties attempting to obtain access to personal information about consumer stored in Petco's database. These attacks include web application attacks such as "Structure Query Language" injection attacks, permitting the attackers to gain access, in clear readable text to tables in databases that support or connect to the Petco website.

This Petco case emphasizes the need for encrypting personal information and protectin against known risks.

(16) ***In the Matter of MTS, Inc., d/b/a Tower Records/Books/video (FTC File No. 032-3209 – April 21, 2004).***

Tower Records marketed and sold music, video recordings, books and other entertainment products through their website and the Internet. Tower Records collects personal information from consumers who visit the Tower website and purchase Tower products online.

The incident that gave rise to the FTC complaint occurred in November and December 2002, when Tower Records redesigned the "check out" portion of their website and rewrote the software code for the Order Status application. In rewriting the code, Tower Records failed to ensure that all of the code from the original version had been rewritten and included, as appropriate, in the new version. As a result, the new version failed to include any "authentication code" to insure that the consumer viewing purchase history was in fact the consumer to whom such information related.

Due to the omission of the authentication code in this application, any visitor to the Tower website who entered a valid order number in the Order Status URL could view certain personal information relating to other Tower customers.

This vulnerability in the Tower Records website and Order Status application lasted for eight days and was exploited by a number of visitors to the site. In December 2002, personal information relating to approximately 5,225 consumers was accessed by unauthorized users, and at least two Internet chat rooms contained postings about the vulnerability as well as comments about some consumer purchases.

The FTC complaint asserted that Tower Records failed to implement procedures that were reasonable to detect and prevent vulnerabilities in their website applications, including reasonable and appropriate procedures for writing and revising web-application code. The FTC further noted that Tower Records failed to adopt and implement policies and procedures

regarding security tests for its web applications, and failed to provide appropriate training and oversight for their employees regarding web application vulnerabilities and security testing.

Like other FTC cases, here again the FTC notes that the security risks associated with broken account and session management are widely known in the information technology industry and there are simple, publicly available measures to prevent such vulnerabilities. The FTC further noted that security experts have been warning the industry about these vulnerabilities since at last 2000.

The Tower case suggests a number of lessons learned. Software changes can have adverse effects to other portions of the software. The effect on security should be considered fully. Software testing needs to include security testing. Companies need to be aware of known security risks and adopt publicly available measures to prevent such vulnerabilities.

(17) ***In the Matter of Guess?, Inc. (FTC File No. 022-3260 – July 30, 2003).***

Guess? designs and produces men's, women's and children's clothing and accessory products. Guess? has sold Guess-branded clothing and accessories online through its website since June 1998.

The FTC complaint states that Guess?'s application and website have been vulnerable to commonly known or reasonably foreseeable attacks from third parties attempting to obtain access to customer information stored in Guess?'s databases. The FTC further notes that these attacks include web-based application attacks such as "Structured Query Language" injection attacks. These SQL attacks were said to occur when an attacker enters certain characters in the address (or URL) bar of a standard web browser to direct the application to obtain information from the databases that support or connect to the website. Through this type of attack, the attacker can gain access in clear text to tables containing credit card information supplied by

purchasers. The FTC noted that the risk of web-based application attacks is commonly known and simple, publicly available measures to prevent such attacks can be implemented.

Companies need to implement measures that are available to prevent access to systems and personal information. Personal information should be stored in an unreadable, encrypted format at all times. In the Guess? case, commonly known attacks could be employed to manipulate the web application and gain access, in clear readable text, to sensitive personal information about consumers, including credit card information.

(18) ***In the Matter of Microsoft Corporation (FTC File No. 012-3240 – August 8, 2002).***

The FTC case against Microsoft arose because of concerns related to Microsoft's Passport and Passport Express Purchase online wallet services that were available through Microsoft's website at www.passport.com and elsewhere on the Internet. Microsoft claimed that it maintained a high level of online security in connection with its Passport and Passport Wallet services.

The FTC's complaint asserted that Microsoft had failed to implement and document procedures that were reasonable and appropriate to: (1) prevent possible unauthorized access to the Passport system; (2) detect possible unauthorized access to the Passport system; (3) monitor the Passport System for potential vulnerabilities; and (4) record and retain system information sufficient to perform security audits and investigations.

(19) ***In the Matter of Eli Lilly and Company (FTC File No. 012-3214 – May 8, 2002).***

The FTC case against Eli Lilly was the first case where the FTC challenged a company's information security practices. The case concerned Eli Lilly's email reminder service known as "Medi-messenger". Consumers who used the Medi-messenger service could design and receive personal email reminder messages from Eli Lilly concerning their medication or other matters. Once someone registered for the Medi-messenger service, the remainder messages were

automatically emailed from Prozac.com to the subscriber at their designated email address according to the schedule established by the subscriber.

Subscribers for the Medi-messenger service registered by providing an email address, a password, the text of the reminder message they wanted to receive, and the schedule for sending the reminder messages.

Eli Lilly promoted the security and privacy protection of its websites. Among other statements, Eli Lilly represented its "websites have security measures in place, including the use of industry standard secure socket layer encryption (SSL), to protect the confidentiality of any ... of Your Information that you volunteer; however, to take advantage of this your browser must support encryption protection (found in Internet Explorer Release 3.0 and above".

The security breach that precipitated the FTC action occurred on June 27, 2001. On this date, Eli Lilly sent an email to Medi-messenger subscribers announcing the termination of the Medi-messenger service. The email disclosed the email addresses of all 669 Medi-messenger subscribers to each individual subscriber by including all of the recipients' email addresses. By this email, Eli Lilly unintentionally disclosed personal information provided to it by consumers in connection with their use of the Prozac.com web site.

The FTC complaint states that this incident resulted from Eli Lilly's failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information. The FTC further noted that Eli Lilly had failed to provide appropriate training for its employees regarding consumer privacy and information security and had failed to provide appropriate oversight and assistance for the employee who sent out the email, who had no prior experience in creating, testing or implementing the computer program used. Also, the FTC complaint stated that Eli Lilly had failed to implement appropriate checks and controls on the

process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the email.

The Eli Lilly case stresses the importance of employee training and management supervision. People are an integral part of information systems. Information security programs need to recognize the importance of people in security oversight.

IV. PEER-TO-PEER FILE SHARING

The FTC has also expressed concern about companies that collect and store sensitive information using Peer-to-Peer (P2P) file sharing software. P2P technology enables computers using compatible P2P programs to share digital files with other computers on the network. If P2P file sharing software is not configured properly, anyone on the P2P network may be able to access files that are not intended to sharing.[10] Furthermore, if there are security flaws or vulnerabilities in the P2P file sharing software, these flaws in the P2P file sharing software could be used to attack other computers on the network.[11]

The FTC recommends that these steps be taken:

- Delete sensitive information you don't need, and restrict where files with sensitive information can be saved.
- Minimize or eliminate the use of P2P file sharing programs on computers used to store or access sensitive information.
- Use appropriate file-naming conventions.
- Monitor your network to detect unapproved P2P file sharing programs.

[10] Peer-to-Peer File Sharing: A Guide for Business, Federal Trade Commission at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus46.shtm (last visited July 31, 2010).

[11] Id.

- Block traffic associated with unapproved P2P file sharing programs at the network perimeter or network firewalls.

- Training employees and others who access your network about the security risks inherent in using P2P file sharing programs.[12]

Whether companies decide to ban P2P file sharing programs or allow them, it is important to create a policy respecting P2P file sharing programs to reduce the risk that any information will be shared unintentionally.

V. MASSACHUSETTS REGULATION

Massachusetts issued regulation 201 CMR 17.00 *et seq.* entitled "Standards for the Protection of Personal Information of Residents of the Commonwealth." This regulation provides standards that must be "met by persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." 201 CMR 17.01(1). The regulation applies to "all persons that own, license or maintain personal information about a resident of the Commonwealth." 201 CMR 17.01(2). The scope of this regulation is much broader than Massachusetts-based companies. It applies to any company that owns, licenses or maintains personal information about a Massachusetts resident without regard to where the company is located or the information stored.

This Massachusetts regulation establishes "minimum standards" to be met in connection with the safeguarding of personal information contained in both paper and electronic records. 201 CMR 17.01(1). This regulation also seeks to "(i) ensure the security and confidentiality of such information in a manner consistent with industry standards, (ii) protect against anticipated threats or hazards to the security or integrity of such information, and (iii) protect against

[12] Id.

unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud against such residents." 201 CMR 17.01(1).

These regulations use the terminology used in the FTC consent orders of "comprehensive information security program". These regulations require "[e]very person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth ... develop, implement, maintain and monitor a comprehensive, written information security program containing such personal information." 201 CMR 17.03(1) (emphasis added). Massachusetts requires a written information security program by every company that maintains personal information on Massachusetts residents. 201 CMR 17.03(1). This written comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records. 201 CMR 17.03(1). Furthermore, "the safeguards contained in such program must be consistent with the safeguards for protection of personal information and information of a similar character set forth in any state or federal regulations by which the person who owns, licenses, stores or maintains such information may be regulated." 201 CMR 17.03(1). As such Massachusetts arguably seeks to apply any Federal standards that are more specific or demanding. It also seeks to apply industry standards.

The regulations contains specific guidance to determine whether a comprehensive information security program is in compliance with the Massachusetts regulations. The security program is to be evaluated taking into account:

(a) the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program;
(b) the amount of resources available to such person;
(c) the amount of stored data;
(d) the need for security and confidentiality of both consumer and employee information.

201 CMR 17.03(2).

The Massachusetts regulation also specifies what "every comprehensive information security program shall include". In this regard the Massachusetts regulation is much more detailed that the FTC consent orders though many of the components required by FTC consent orders are required in the regulation. The regulation requires, but is not limited to those elements:

"1. Designating one or more employees to maintain the comprehensive information security program:

2. Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting of such risks, including but not limited to:
   a. ongoing employee (including temporary and contract employee) training;
   b. employee compliance with policies and procedures; and
   c. means for detecting and preventing security system failures.

3. Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.

4. Imposing disciplinary measures for violations of the comprehensive information security program rules.

5. Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.

6. Taking all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00; and taking all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00.

7. Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.

8. Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.

9. Reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers.

10. Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

11. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.

12. Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information."

201 CMR 17.03(3).

The Massachusetts regulation also specifies certain computer system security requirements. It requires every person that owns, licenses, stores or maintains personal information about a Massachusetts resident to include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system. The information security program must, at a minimum, including the following elements:

(1) Secure user authentication protocols including:
   (a) control of user IDs and other identifiers;
   (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;
   (c) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect;
   (d) restricting access to active users and active user accounts only; and
   (e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

(2) Secure access control measures that:
   (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and
   (b) assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

(3) To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

(4) Reasonably monitoring of systems, for unauthorized use of or access to personal information;

(5) Encryption of all personal information stored on laptops or other portable devices;

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.

(8) Education and training on the proper use of the computer security system and the importance of personal information security."

201 CMR 17.04

Massachusetts has also issued a "Small Business Guide for Formulating a Comprehensive Written Information Security Program." Under this Guide the "Data Security Coordinator" is designated to implement, supervise and maintain the Plan, and is responsible for implementing the Plan, training of the Plan's safeguards, and evaluating third party service providers, reviewing the scope of the security measures at least annually or wherever there is a change in material business practices and conducting annual training.

Internal risks also need to be addressed. Employment contracts should require all employees to comply with the Plan and mandatory disciplinary action should be taken for violation of the security provisions of the Plan.

The Guide also provides the following regarding internal threats:

- The amount of personal information collected must be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or necessary to us to comply with other state or federal regulations.
- Access to records containing personal information shall be limited to those persons who are reasonably required to know such information in order to accomplish your legitimate business purpose or to enable us to comply with other state or federal regulations.
- Electronic access to user identification after multiple unsuccessful attempts to gain access must be blocked.
- All security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing personal information. The Data Security Coordinate shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.
- Terminated employees must return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
- A terminated employee's physical and electronic access to personal information must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be validated. The Data Security Coordinator shall maintain a highly secured master list of all lock combinations, passwords and keys.

- Current employees' user-ID's and passwords must be changed periodically.
- Access to personal information shall be restricted to active users and active use accounts only.

To combat external threats the Guide recommends the following:

- There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information.
- There must be reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information.
- To the extent technically feasible, all personal information stored on laptops or other portable devices must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible. Encryption here means the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation.
- All computer systems must be monitored for unauthorized use of or access to personal information.
- There must be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect; (4) restriction of access to active users and active user accounts only; and (5) blocking of access to user identification after multiple unsuccessful attempts to gain access.
- The secure access control measures in place must include assigning unique identifications plus passwords, which are not vendor-supplied default passwords, to each person with computer access to personal information.
- Employees are encouraged to report any suspicious or unauthorized use of customer information.
- Whenever there is an incident that requires notification under M.G.L. c. 93H, § 3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible.
- Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.
- At the end of the work day, all files and other records containing personal information must be secured in a manner that is consistent with the Plan's rules for protecting the security of personal information.

- Each department shall develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access in records containing personal information are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers.
- Access to electronically stored personal information shall be electronically limited to those employees having a unique log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes.
- Visitors' access must be restricted to one entry point for each building in which personal information is stored, and visitors shall be required to present a photo ID, sign-in and wear a plainly visible "GUEST" badge or tag. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.
- Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that complies with M.G.L. section 93I.

VI. DUTY TO DISCLOSE BREACHES

Identity theft has been reported to be the fastest growing crime. New laws and regulations focused not on imposing an obligation to implement security measures but rather on imposing an obligation to disclose security breaches are having a significant impact.

These disclosure or notification laws seek to provide notice to persons who may be adversely affected by a security breach (*e.g.*, persons whose compromised personal information may be used to facilitate identity theft). By requiring notice, these laws seek to provide such persons with a warning that their personal information has been compromised, and an opportunity to take steps to protect themselves against the consequences of identity theft.

The California Security Breach Information Act (the "**SBIA**"), SB 1386, became effective July 2003. This was the first law in the United States to impose a legal obligation on companies to inform individuals of incidents involving unauthorized access to their personal information. This California SBIA has become a model statute for laws adopted in various jurisdictions. At least 46 states and the District of Columbia, Puerto Rico and the Virgin Islands have now adopted "notification" statutes imposing a notification obligation to disclose

information about security breaches. Only Alabama, Kentucky, New Mexico and South Dakota have not enacted security breach laws. While these statutes place a burden on businesses, the risks of identity theft warrant their adoption.[13] Notification allows the subject of a security breach to take action to avoid or mitigate potential identity theft losses. Federal breach notification legislation is pending.

The California law requires disclosure to all persons whose personal information was compromised, and anyone who is injured by a company's failure to do so can sue to recover damages.

A. Virginia Breach Notification Statute.

By way of example, Virginia law requires business and state government agencies that own or license computerized data that includes personal information to disclose any breach of security of the system to any resident whose unencrypted and unredacted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Notice must also be provided if encrypted information is accessed and acquired in an unencrypted form, or if the breach involves a person with access to the encryption key and individual or entity reasonably believes that the breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth. In 2010, Virginia amended its breach notification statute to cover personal medical information specifically. This provision becomes effective January 1, 2011.

The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures

[13] In COMPUTERWORLD Gartner's John Pescatore is quoted as saying that :[a]n incident where information on 100,000 customers is exposed typically costs an enterprise $10 million to $15 million to fix, excluding damage to the brand name. But preventing a data leak costs $3 million to $5 million. COMPUTERWORLD at p. 18 (January 11, 2009).

necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Notice must also be made to the Office of the Commonwealth's Attorney General.

Personal information is defined as an individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the data elements are neither encrypted nor redacted: Social Security number; driver's license number; or a financial account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to the individual's financial account. It does not include publicly available information that is lawfully made available to the public from federal, state, or local government records.

Notification can be provided by mail, e-mail, or telephone. If the cost of providing regular notice would exceed $50,000, the amount of people to be notified exceeds 100,000, or the entity does not have sufficient contact information to provide written or electronic notice, substitute notice may be provided. When substitute notice is used, it must consist of the following: e-mail notice, conspicuous posting on the entity's web site, and notification to major statewide media. Notice must include a description of the following: the incident in general terms; the type of personal information that was subject to the unauthorized access and acquisition; the general acts of the individual or entity to protect the personal information from further unauthorized access; a telephone number that the person may call for further information and assistance, if one exists; and advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.[14]

B. DC Breach Notification Statute.

The DC Consumer Personal Information Security Breach Notification Act was effective July 1, 2007. DC Code §§ 28-3851 et seq. The DC statute covers personal information and the

unauthorized acquisition of computerized or other electronic data, or any equipment or de storing such data, that compromises the security, confidentiality, or integrity of pers information maintained by the person or business. The DC statute does not refer to encryp specifically but does exclude data "that has been rendered secure, so as to be unusable by unauthorized third party."

The DC statute requires notice promptly to any DC resident whose personal informat was included in the breach. notice can be accomplished by written notice, electronic not where the consumer has consented to such notice under ESIGN, or substitute notice. If m than 1000 persons are required to be notified then all consumer reporting agencies as defined § 1681(a) of the Fair Credit Reporting Act.

One of the interesting aspects of the DC statute is that if the entity has its o information security policy or procedure that requires notification consistent with this law th that procedure may be invoked in place of this law. Furthermore, if the entity main communicates by email as the primary method of communication, then email may be used f purposes of notification.

C. Maryland Breach Notification Statute

The Maryland Personal Information Protection Act, MD Code Com. Law, §§ 14-350 et seq., as amended, took effect January 1, 2008. Businesses that own or license persona information of an individual residing in Maryland must implement and maintain reasonabl security procedures and practices that are appropriate to the nature of the personal informatio owned or licensed and the nature and size of the business and its operations.

Maryland defines a "breach of the security of a system" simply as the "unauthorize acquisition of computerized data that compromises the security, confidentiality of the personal

[14] Virginia Code § 59.1-442.2: http://legal.state.vaus/cgi-bin/legp504.exe?)))+cod+59.1-4442.2

information by a business." The key word is "compromises". Maryland no longer requires that the unauthorized acquisition likely result in a material risk of identity theft.

Maryland requires that any business discovering or notified or a breach of the security "conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach." "If after the investigation is concluded, the business determines that misuse of the individual's personal information has occurred or is reasonably likely to occur as the result of a breach of the security of a system, the business shall notify the individual of the breach." If notice is required notice must be given "as soon as reasonably practicable after the business conducts the investigation. If notice is determined not to be required the business must maintain records of its determination for three years after the determination.

Notification may be delayed based on a criminal investigation, homeland or national security. Notice may be made by mail, e-mail, telephone or by substitute notice. The Maryland statute specifies certain information that must be included in the notice. The statute also requires that the business give notice of a breach to the Office of the Maryland Attorney General prior to giving notice to the affected Maryland residents.

D. Contents of Breach Notification.

These "breach notification" statutes are not uniform which can make compliance very challenging. The definition of sensitive personal information is longer in some states. The state breach notification statutes differ on the definition of breach, who must be notified, when notice is required, the form of notice that is acceptable and substitute notice options. Generally, any business in possession of computerized sensitive personal information about an individual must disclose a breach of the security of such information to the individual affected. If the individuals are citizens of different states this may require compliance with different state laws. Data

breaches are becoming increasingly more costly. It was recently reported that organizations experiencing a data breach in 2008 paid an average of $6.6 million to rebuild their brand image and retain customers.[15]

Early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information.[16] Law enforcement should also be notified. You need to make sure the timing of your notice does not impede the investigation.

The individual breach notice letters will often recommend that the individual place a fraud alert on their credit file with one of the three major credit bureaus: Equifax, Experian and TransUnion Corp.

The FTC recommends that the breach notice:

- describes clearly what you know about the compromise. Include how it happened; what information was taken, and, if you know, how the thieves have used the information; and what actions you have taken already to remedy the situation. Explain how to reach the contact person in your organization. Consult with your law enforcement contact on exactly what information to include so your notice does not hamper the investigation.
- explains what responses may be appropriate for the type of information taken. For example, people whose Social Security numbers have been stolen should contact the credit bureaus to ask that fraud alerts be placed on their credit reports. See www.ftc.gov/idtheft for more complete information on appropriate follow-up after a compromise.

[15] B. Krebs, "Data Breaches are More Costly Than Ever." WASHINGTON POST, p. D3, February 3, 2009.

[16] Compliance with the applicable breach notification statute may have the salutary effect of capping the notifying company's liability respecting the breach. *See, e.g., Piscotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007).

- includes current information about identity theft. The FTC's website at www.ftc.gov/idtheft has information to help individuals guard against and deal with identity theft.
- provides contact information for the law enforcement officer working on the case (as well as your case report number, if applicable) for victims to use. Be sure to alert the law enforcement officer working your case that you are sharing this contact information. Identity theft victims often can provide important information to law enforcement. Victims should request a copy of the police report and make copies for creditors who have accepted unauthorized charges. The police report is important evidence that can help absolve a victim of fraudulent debts.
- encourages those who discover that their information has been misused to file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Information entered into the Identity Theft Data Clearinghouse, the FTC's database, is made available to law enforcement.

These breach notification requirements apply to breaches of sensitive personal information about residents of the state (usually first and last name in combination with a social security number, driver's license number, or state id number, or financial account number) that result in the acquisition of the sensitive information by an unauthorized person. They usually contain exceptions for encrypted information, and in some cases for other methods of masking the sensitive information under the theory that those breaches do not present a risk of identity theft. Usually only the individual whose data has been acquired needs to be notified, although some state laws require notice to state authorities and to credit bureaus. In the case of a breach of security of sensitive information held by a third party service provider, the state laws typically

require that the service provider immediately notify the owner or licensee of the data, who in turn notifies the affected individual.

Many of the state laws give greater latitude with respect to how notice needs to be provided to businesses that include provisions regarding breach notification in their information security policies. Because breaches, such as thefts of laptops, lost data files and intrusions into computer systems by former employees, occur with surprising frequency, it is worth planning in advance how to mitigate and respond to these incidents.

Thefts of credit card information and other personal information are being reported almost every day. One of the largest involved a data breach at TJX Companies that implicated at least 46 million credit and debit cards. BNA reported that TJX Companies reached a tentative settlement agreement to resolve a consolidated class action (*In re TJX Companies Retail Security Breach Litigation*, D. Mass., No. 07-10162). The settlement was subject to court approval.

Key features of the tentative settlement included up to three years of credit monitoring and identity theft insurance, reimbursement for costs incurred in obtaining new drivers' licenses, reimbursement for losses incurred in connection with persons whose social security numbers were on their drivers' licenses, and $30 vouchers to be used in TJX stores for those who suffered other losses.

Another aspect of the settlement is the security improvements TJX took to enhance the security of TJX's computer system. These security improvements will be evaluated by plaintiff's independent expert to determine whether such actions are a prudent and good faith attempt to minimize the likelihood of intrusions in the future.

The TJX data theft involved unauthorized individuals hacking into a portion of TJX's computer network that handles consumer transactions for 2500 stores (T.J. Maxx, Marshals,

HomeGoods and other stores) and stealing personal credit, debit and drivers' information from TJX's system.

The class action filed January 29, 2007 alleged that TJX failed to adhere to credit card industry data security measures known as the Payment Card Industry Data Security Standard (PCI-DSS). There were at least 18 consumer and bank class action complaints filed against TJX. The estimated cost of the settlement exceeded $100 million dollars and involves 450,000 customers.

VII. RECOMMENDED SECURITY PRACTICES

A. Better Business Bureau Checklist.

A checklist developed by the Better Business Bureau, the National Cyber Security Alliance and the Federal Trade Commission recommends a detailed computer security audit twice a year and routine checks throughout the year.[17] The checklist includes the following recommendations:

1. Maintain a password protection program using cryptic passwords that are changed at least every 90 days.

2. Use virus protection software on all computers, ideally software that updates itself each week.

3. Install firewalls at every point where the computer system is connected to other networks.

4. Install software security patches upon release. Check software vendor sites for security patches or use automated patching programs.

5. Back up all computer data at least weekly, including work done on individual computers.

6. Check routinely for suspicious activity reported on firewall, encryption and password logs.

7. Recognize the risks from file-sharing. Consider turning off the file-sharing function and barring employees from installing file-sharing software.

8. Consider using encryption software to protect data even if someone cracks the firewalls.

9. Educate employees on wise e-mail practices and backup procedures, and advise them to disconnect from the Internet when not using it.[18]

In addition, for larger enterprises, more elaborate security standards, such as ISO IEC 27002 (17799), may be appropriate.

Today, every company should adopt a reasonable standard for protecting customer, employee, partner and proprietary information. This protection needs to consider access controls, encryption in storage and transmission, physical security, disaster recovery and auditing.

Access controls include requiring unique accounts for individual users, disabling anonymous logic, enforcing strong password requirements and adhering to access review and revocation policies. In addition, logging account access and usage, and conducting periodic audits also contribute to a strong access control policy.

Encryption should be used both with respect to storage and transmission of personal information, confidential information and sensitive information. Encryption is becoming increasingly more important for various legal reasons.

[17] "Network Security", *Electronic Commerce & Law Rep.* (BNA) (April 21, 2004) at pp. 382-383.

[18] *Id.*

Physical security should also be considered in helping to ensure that data is not accessed by unauthorized individuals.

Protecting against data losses and losses in data integrity by ensuring the ability to recover from system failure, natural disasters, or other emergencies is another aspect of information security. Disaster recovery planning, testing and implementation are key to information security.

Industry security standards and practices are continually updated based on changes in technology and in methods of attack. Information security programs must be constantly reviewed and updated to stay ahead of evolving threats.

Implementation of an information security program must consider all aspects essential to protecting critical business and personal information from compromise and loss.

B. Payment Card Requirements.

Through a cooperative effort between Visa and Mastercard, the credit card industry developed the Payment Card Industry Data Security Standard (PCI-DSS) referenced above. This PCI-DSS offers a single approach to safeguarding sensitive data for all card brands. The PCI-DSS consists of the following requirements.

(1) Build and Maintain a Secure Network. This requirement includes installing and maintaining a firewall configuration to protect data and not using vendor supplied defaults for system passwords and other security parameters. Firewalls are a key protection mechanism for any computer network.

(2) Protect Cardholder Data. Encryption is a critical component of cardholder data protection in this requirement. You need to use strong encryption of cardholder data in transmission across open, public networks.

(3) Maintain a Vulnerability Management Program. You need to use and regularly update anti-virus software programs. You also need to develop and maintain secure systems and applications. Part of this vulnerability program is a commitment to install security patches promptly.

(4) Implement Strong Access Control Measures. This requirement ensures critical data can only be accessed by authorized personnel. Each person with computer access needs to be assigned a unique ID. Passwords, token devices or biometrics should be used to authenticate all Users. In addition, any physical access to data or systems that house cardholder data needs to be appropriately restricted.

(5) Regularly Monitor and Test Networks. This requirement provides for tracking and monitoring all access to network resources and cardholder data. Logging mechanisms are critical to this tracking and monitoring. The requirement also includes regular test security systems and processes.

(6) Maintain an Information Security Policy. The policy should address information security for employees and contractors, and set the security tone for the whole company.

These PCI-DSS are becoming quite significant. In May 2007, Minnesota became the first state to codify one aspect of PCI-DSS by prohibiting entities conducting business in Minnesota from retaining credit card or debit card security code data, Pin verification codes, or the full contents of any track of magnetic stripe data for more than 48 hours after the authorization of the transaction. These credit and debit card data retention provisions became effective August 1, 2007, with the retailer liability provisions becoming effective on August 1, 2008. Similar bills are being considered in other states.[19]

[19] H. Salow, J. Halpert and D. Lieber, "New Liability Under State Law Stresses Need for Strong Data Security for Payment Card Data," THE PRIVACY ADVISOR at p. 25 (September 2007).

VIII. CONTRACT PROTECTION

Information security needs to be contemplated fully in IT service provider contracts, software development contracts, outsourcing contracts and other IT contracts. Special security and application anti-hacking protection clauses should be considered. Furthermore, employment agreements need to reference security plans and policies.

A. Software Development.

SANS Institute and MITRE Corporation have published a list of the top 25 programming errors that cause the most security problems. Many security vulnerabilities in program code are the result of bad computer code. This list of top 25 programming errors can be used in drafting performance requirements, acceptance test provisions and warranties.

B. Top 25 Software Errors.

SANS Institute and MITRE Corporation have published a list of the "Top 25 Most Dangerous Software Errors". This list contains the most widespread and critical programming errors that can lead to serious software security vulnerabilities. They are dangerous because the errors are easy to find and exploit, and frequently permit attackers to take over the software completely as well as steal data or prevent the software from working at all.

MITRE maintains the Common Weakness Enumeration (CWE) Website presenting detailed descriptions of the top 25 programming errors along with authoritative guidance for mitigating and avoiding these errors, as well as data on more than 800 programming errors, design errors, and architecture errors that can lead to exploitable vulnerabilities. The 2010 list of Top 25 programming errors represents a substantial improvement of the 2009 list. The listing has been prioritized based on an evaluation of each weakness based on its prevalence and importance.

Cross-site scripting and SQL injection are the major security weaknesses identified. Both of these weaknesses were identified in several of the FTC consent order cases. Below is a listing of the 2010 top 25 programming errors:

2010 TOP 25 ERRORS

1. Improper Neutralization of Input During Web Page Generation ("Cross-Site Scripting").
2. Improper Naturalization of Special Elements Used in an SQL Command ("SQL Injection:").
3. Buffer Copy without Checking Size of Input ("Classic Buffer Overflow").
4. Cross-Site Request Forgery (CSRF).
5. Improper Access Control (Authorization).
6. Reliance on Untrusted Inputs in a Security Decision.
7. Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal").
8. Unrestricted Upload of File with Dangerous Type.
9. Improper Neutralization of Special Elements use in an OS Command ('OS Command Injection').
10. Missing Encryption of Sensitive Data.
11. Use of Hard-coded Credentials.
12. Buffer Access with Incorrect Length Value.
13. Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion').
14. Improper Validation of Array Index.
15. Improper Check for Unusual or Exceptional Conditions.
16. Information Exposure Through an Error Message.
17. Integer Overflow or Wraparound.
18. Incorrect Calculation of Buffer Size.
19. Missing Authentication for Critical Function.
20. Download of Code Without Integrity Check.

21. Incorrect Permission Assignment for Critical Resource.
22. Allocation of Resources Without Limits or Throttling.
23. URL Redirection to Untrusted Site ('Open Redirect').
24. Use of a Broken or Risky Cryptographic Algorithm.
25. Race Condition.

There is extensive information at MITRE's CWE - Common Weakness Enumeration - A Community - Developed Dictionary of Software Weakness Types at http://cwe.mitre.org/top25/ (last visited 7/19/2010).

The Top 25 can be used in procurement software development projects and other IT contracts to improve information security. The Top 25 may be used to help set minimum expectations for due care by software vendors.

C. Security Training.

The development team should be well-trained and knowledgeable in information security issues affecting the development, including avoiding unsafe library function calls and cross-site scripting errors.

D. Defining Security Requirements.

Security requirements should be defined during the early stages of software development.

E. Secure Design.

Potential threats should be identified in the early design phase.

F. Background Checks.

In some situations it may be desirable to perform or require the vender to perform. background investigations of development team members and require the vendor to certify that all personnel involved in a contract have cleared a background investigation.

G. Risk Assessments.

Vendors may be required to conduct risk assessments to determine and prioritize risks, identify vulnerabilities and understand the impact that particular attacks might have on a system.

H. Mitigation of Errors.

Warrant that the top 25 most common programming errors have been mitigated.

I. Performance.

Warrant that the software meets applicable contractual obligations, regulatory requirements and security best practices and standards.

J. Vulnerability Tests.

Permit vulnerability and penetration testing.

K. Patches and Updates.

Ensure security patches and updates are installed in a timely manner.

L. No Malicious Code.

Warrant that the software does not contain any code that does not support a software requirement and weakens the security of the application including all forms of malicious code.

M. No Disabling Mechanisms.

Warrant that the software does not contain any disabling mechanisms.

IX. LEGAL BATTLE PLANS

Effective information security programs include effective incident response plans. Legal battle plans are rapidly becoming an important part of a comprehensive information security program. These battle plans should be viewed as a critical component of your incident response plans.

In today's information security environment, you need to react quickly and thoroughly to security breaches. Companies need to establish procedures to ensure a quick, effective and

orderly response to such incidents. When an adverse event occurs, you are not going to have time to study your options. You will already be in trouble. You should prepare yourselves well ahead of any possible incidents so you can respond quickly to minimize damage and legal exposure. Legal battle plans help to address this need. They are "off-the-shelf" plans that can be quickly adapted and executed to combat and otherwise defend against security incidents. These plans seek to take full advantage of legal rights and remedies to control, manage, avoid, and mitigate losses and disruptions and comply with all legal obligations, including any notice requirements, contractual or regulatory obligations, and forensically sound evidentiary collection procedures.

Legal battle plans should be prepared for the security incidents that would have the greatest adverse effect on the company. A battle plan should spell out in advance the defenses and counterattacks the company can deploy rapidly. These include legal notices that must be provided to customers and contracting parties under affected contracts, as well as any necessary actions you will need to take regarding other matters, including insurance coverage, civil and criminal claims that may be applicable, evidence that should be collected, and points of contact that need to be notified.

By fully considering potential claims applicable to security incidents, you should be in a better position to make sure that the necessary evidence is collected in a forensically sound manner. You need to make sure that you put in place sufficient audit procedures and controls to provide a strong evidentiary trail consistent with the requirements applicable to the production of admissible evidence. The legal battle plan should consider the quality and completeness of the evidence. As the European Convention on Cybercrime has noted, "effective collection of evidence in electronic form requires very rapid response". Consider using forensic software tools to provide accurate, relevant, and timely information about security incidents.

Because the legal battle plan is meant to increase your company's ability to respond to security incidents, it should include the tools to identify and analyze the incident, including the capability of successfully identifying and prosecuting a perpetrator, even an anonymous one. The plan also should include consumer notices required by law, applicable contract notices, and regulatory notices. Further, it should provide for limiting damages, recouping losses, and reducing regulatory, contractual, and other legal exposures. Also, the battle plan should be sufficiently flexible to be adapted readily to the circumstances of specific incidents and should coordinate with a company's public relations response and other incident response plans. This coordination ensures that the company is well prepared to limit damage to its reputation and to answer public or media queries about any incidents. A key objective of response plans, including the legal battle plans that are a part of these response plans, should be to maintain public confidence and trust in the company.

Legal battle plans will detail legal responses to a security incident. However, although not all incidents will be amenable to a legal counterattack, in most situations legal strategies may be deployed to keep damages to a minimum. With proper planning, you should be able to prevent damages from continuing to accrue after an incident has occurred. For example, the battle plan should provide contingencies for rapidly escalating your response, if such response is deemed appropriate.

Once you create a legal battle plan, don't neglect it. Legal battle plans need to be monitored and adapted based on changing external and internal threats and any evolution or change within your company and its information security risk environment. Like all response plans, legal battle plans need to be tested periodically. Management and employee training on information security responses should include training on the company's legal battle plans.

Today, legal battle plans have become an essential part of comprehensive information security planning as a matter of prudent risk management. Make sure your battle plans are combat ready.

X. FORENSIC SOFTWARE TOOLS

Companies must establish incident response capabilities. Forensic software tools need to be considered to preserve, authenticate and analyze computer data consistent with proper computer forensics.

For example, Guidance Software, Inc.'s EnCase computer forensic tool is being widely used in computer investigations. Guidance Software claims its EnCase Enterprise Edition software is a powerful network-enabled, multi-platform enterprise computer investigation and incident response system that provides rapid and thorough analysis and collection of static and volatile data residing on servers and work stations anywhere on the network, without disrupting operations. Guidance Software represents that EnCase Enterprise dramatically reduces the cost and improves the effectiveness of information security professionals, computer incident response teams, eDiscovery auditors and forensic examiners. Guidance Software claims that its EnCase computer forensic tool has been validated by several courts at trial and on appeal. This software tool is used to identify, contain and control an incident, and to authenticate, search, recover and preserve relevant computer evidence. It is likely that software tools like EnCase Enterprise and EnCase Forensic will become an integral part of information security programs. The availability of these software tools requires that they be considered in analyzing risks and developing effective responses.

XI. ETHICAL CONSIDERATIONS

Information security has become a very important ethics consideration. This point was emphasized in a recent Opinion by the Arizona State Bar Committee on the Rules of

Professional Conduct.[20] In this Opinion, the Arizona Committee advises that compliance with the ethical rules relating to the client's electronic files or communications requires attorneys and law firms "to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence", including taking "reasonable and competent steps to assure that the client's electronic information is not lost or destroyed".[21] The Arizona Opinion further advises that in order to meet this information security requirement "an attorney must be competent to evaluate the nature of the potential threat to client electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end".[22] Most importantly, the Arizona Opinion provides that "[a]n attorney who lacks or cannot reasonably obtain that confidence is ethically required to obtain an expert consultant who does have such competence".[23] In connection with this Opinion, the Arizona Committee observes that the modern rule is that precautions must be taken to prevent the theft of confidential communications to preserve the privilege.

The Arizona Committee observes that precautions must be taken with regard to protecting electronic communications and notes that "[a] panoply of electronic and other

[20] Arizona State Bar Committee on the Rules of Professional Conduct Opinion No. 05-04 (July 2005).

[21] *Id.* In a recent Nevada Standing Committee on Ethics and Professional Responsibility, the Committee observed that lawyers can use third party providers to store confidential client information as long as the lawyers act competently and reasonably to safeguard confidential information and communications from inadvertent and unauthorized disclosure. This involves competence and reasonable care (1) in the selection of the third party contractor and (2) an express contractual requirements that the contractor and its employees keep the information confidential and protected from unauthorized access or disclosure. Nevada Opinion No. 33, Feb. 9, 2006. In a related opinion, Virginia addressed the issue whether the client's file may contain only electronic documents with no paper copies retained. Virginia Legal Ethics Opinion No. 188.

[22] *Id.*

[23] *Id.*

measures are available to assist an attorney in maintaining client confidences".[24] Further, the Arizona Opinion advises:

> ""Firewalls" – electronic devices and programs which prevent unauthorized entry into a computer system from outside that system – are readily available. Recent upgrades in Microsoft operating systems incorporate such software systems automatically. A host of companies, including Microsoft, Symantec, McAfee and many others, provide security software that helps prevent both destructive intrusions (such as viruses and "worms") and the more malicious intrusions which allow outsiders access to computer files (sometimes called "adware" or "spyware").
>
> Software systems are also readily available to protect individual electronic files. Passwords can be added to files which prevent viewing of such files unless a password is first known and entered. The files themselves can also be encrypted so that, even if the password protection is compromised, the files cannot be read without knowing the encryption key – something that is extremely difficult to break."[25]

Lawyers need to keep abreast of the legal developments relating to information security. For example, the Federal Trade Commission has filed complaints against many companies on the grounds that the companies failed to provide adequate information security for consumer information. In all of these "information security" cases, the FTC entered into a Consent Order with the respondent company requiring the company to establish, implement and thereafter maintain a "comprehensive information security program" that is "reasonably designed to protect

[24] *Id.*

[25] *Id.*

the security, confidentiality and integrity of personal information collected from or abo consumers." These rules may be applied to client confidential information.

Information security risks apply to both online and offline collection and storage, a include the secure disposal of information. Lawyers need to be very sensitive to the risks disposing of old computers containing confidential client information.

Lawyers also need to employ strong passwords and reasonable access controls to preve a hacker from gaining access to the lawyer's computer systems and network. If protection c be obtained at a reasonable cost, it should be obtained. Lawyers also need to employ reasonab measures to detect and respond to unauthorized access to protected information and condu security investigations. Lawyers should provide for reasonable oversight over service provide who have access to confidential information. The management of contractors is a critic component of information security programs for lawyers. Today, incident response processe consistent with best practices, need to be implemented as part of an overall security pla Lawyers need to be able to respond quickly to manage, contain and minimize problems arisi from unexpected events affecting the confidentiality of client information.

XII. CONCLUSION

Information security is becoming a very serious legal issue. The duty to provide securi to information and communications is expanding. The requirement to develop and maintain "comprehensive information security program" is becoming a legal requirement. "Reasonab Security" is evolving in the law. The duty to warn individuals of information security breach has become quite significant and is required by law in most states. In all likelihood the leg issues relating to information security will continue to grow in importance.

Additional Reference Links
ACC's 2010 Annual Meeting
Session 410 Data Breach Preparedness & Prevention

http://www.privacyrights.org/data-breach

http://datalossdb.org/

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.htmlA

http://securityblog.verizonbusiness.com/2010/09/21/arriving-soon-new-study-on-pci-dss/

http://www.bbc.co.uk/news/technology-11388018

Extras from ACC

We are providing you with an index of all our InfoPAKs, Leading Practices Profiles, QuickCounsels and Top Tens, by substantive areas. We have also indexed for you those resources that are applicable to Canada and Europe.

Click on the link to index above or visit http://www.acc.com/annualmeetingextras.

The resources listed are just the tip of the iceberg! We have many more, including ACC Docket articles, sample forms and policies, and webcasts at http://www.acc.com/LegalResources.