LESSONS LEARNED FROM RECENT DATA BREACH STUDIES AND 10 CRITICAL STEPS TO TAKE NOW TO REDUCE THE RISK AND COST OF DATA BREACHES

JUNE 11, 2014 PRESENTATION TO:
THE ACC, MID-AMERICA CHAPTER
LEAWOOD, KS

LAURA CLARK FEY, ESQ., CIPP/U.S.
DALEY & FEY LLP
LEAWOOD, KS
Top Ten Signs the Government is Spying on You

10. Post office wall has several photos of you sleeping

9. Your houseplant occasionally sneezes

8. Domino’s keeps delivering to unmarked van parked across the street

7. Birthday card from your mom has several words blacked out

6. You get nominated for “Outstanding Lead Performance in an NSA Surveillance Video”

Source: Late Show with David Letterman, May 16, 2006 and April 15, 2009.
Top Ten Signs the Government is Spying on You

5. Your dishwasher functions are “Wash,” “Rinse” and “Record”

4. Local news only reporting things that happen in your living room

3. Every time you say goodbye on the phone, you hear a strange voice say, “Roger that, Chico”

2. You “googled” a recipe for hummus and the FBI raided your house

1. “Girl Scout” delivering your thin mints is 6'4”, 270

Source: Late Show with David Letterman, May 16, 2006 and April 15, 2009.
Agenda

• Lessons Learned from Recent Information Security and Data Breach Studies

• 10 Critical Steps Corporations Should Take Now to Reduce Data Breach Risks and Costs

• Recommended Resources

• Questions
“The guy with the weird skin disease forgot to sign the privacy forms.”
LESSONS LEARNED FROM RECENT INFORMATION SECURITY AND DATA BREACH STUDIES
LESSONS LEARNED FROM RECENT INFORMATION SECURITY AND DATA BREACH STUDIES

1. The Current State of Information Security
2. Primary Targets and Causes of Data Breaches
3. Significant Consequences; Key Factors Impacting Overall Costs; and Post-Breach Actions
1. Lessons Learned: The Current State of Information Security
Current State: Gaps in Information Security
Perceptions and Reality

Figure 2: Confidence that organizations have instilled effective information security behaviors into their culture

- Somewhat confident: 39%
- Very confident: 29%
- Total: 68%

Figure 3: When information security becomes involved in major projects

- At project inception: 25%
- During the analysis and design phases: 24%
- During the implementation phase: 12%
- On an as-needed basis: 21%
- Do not know: 18%
Current State: Lack of Accurate Inventory and Adequate Administrative Policies and Processes

Figure 10: Data privacy safeguards in place related to process

- Privacy policy reviewed at least once a year: 39% (2011), 49% (2012)
- A written privacy policy is in place and published on our external website: 41% (2011), 53% (2012)
- Accurate inventory of where personal data for employees and customers are collected, transmitted, and stored: 33% (2011), 34% (2012)
- Require third parties (including outsourcing vendors) to comply with our privacy policies: 29% (2011), 32% (2012)
- Accurate inventory of locations or jurisdictions where data is stored: 29% (2011), 31% (2012)
- Incident response process to report and handle breaches to third parties that handle data: 27% (2011), 27% (2012)
- Inventory of all third parties that handle personal data of employees and customers: 24% (2011), 26% (2012)
- Conduct compliance audits of third parties that handle personal data of customers and employees: 29% (2011), 26% (2012)
Current State: Decline in Use of Basic Information Security Detection Technologies

Figure 8: Technology information security safeguards currently in place

- Malicious code detection tools (spyware and adware): 83% (2011) vs. 71% (2012)
- Intrusion detection tools: 62% (2011) vs. 53% (2012)
- Tools to discover unauthorized devices: 57% (2011) vs. 47% (2012)
- Vulnerability scanning tools: 59% (2011) vs. 46% (2012)
- Subscription to vulnerability alerting service(s): 49% (2011) vs. 41% (2012)
- Data loss prevention (DLP) tools: 48% (2011) vs. 39% (2012)
- Security event correlation tools: 47% (2011) vs. 36% (2012)
Current State: Technology Adoption is Moving Faster than Security
Current State: Greatest Obstacles to Improving Information Security

Figure 14: Greatest obstacles to improving the overall strategic effectiveness of the organization’s information security function

- Leadership: CEO, president, board, or equivalent
- Leadership: CIO or equivalent
- Lack of an effective information security strategy
- Lack of an actionable vision or understanding of how future business needs impact information security
- Insufficient capital expenditures
- Insufficient operating expenditures
- Absence or shortage of in-house technical expertise
- Poorly integrated or overly complex information/IT systems

2011 vs. 2012:
- Leadership: CEO, president, board, or equivalent: 23% vs. 21%
- Leadership: CIO or equivalent: 18% vs. 15%
- Lack of an effective information security strategy: 26% vs. 22%
- Insufficient capital expenditures: 27% vs. 26%
- Insufficient operating expenditures: 21% vs. 21%
- Absence or shortage of in-house technical expertise: 21% vs. 22%
- Poorly integrated or overly complex information/IT systems: 19% vs. 17%
2. Lessons Learned: Primary Targets and Causes of Data Breaches
Primary Targets: Overview of Industries with Most Security Incidents

Incident rates across monitored industries

- **Manufacturing**: 26.5%
- **Finance and insurance**: 20.9%
- **Information and communication**: 18.7%
- **Health and social services**: 7.3%
- **Retail and wholesale**: 6.6%
Primary Targets: Type of Data Lost

2013 Incidents by Data Type Exposed

- Credit Card Number: 10.4%
- Date of Birth: 12.2%
- Medical: 13.3%
- Phone Number: 13.3%
- Misc.: 15.6%
- SSN: 18.5%
- Address: 18.7%
- User Name: 37.4%
- eMail: 39.0%
- Name: 41.4%
- Password: 47.8%
Primary Targets: Attacker Motivation

- Industrial espionage, financial crime, terrorism, data theft: 23%
- Dissatisfaction with employer/job: 15%
- Social activism, civil disobedience: 7%
- Other: 6%
- Opportunistic: 49%
Primary Causes According to Ponemon Institute

- Malicious or criminal attacks (42%)
- Negligent employees or contractors (30%)
- System glitches (IT and business process failures) (29%)
The 2,861 data breaches occurring in the 95 countries analyzed by Verizon between 2011 and 2013 can be described by these patterns:

- **Point-of-Sale Intrusions** – 31%
- **Web App Attacks** – 21%
- **Cyber-Espionage** – 15%
- **Card Skimmers** – 14%
- **Insider Misuse** – 8%
- **Crimeware** – 4%
- **Physical Theft/Loss** – 1%
- **Miscellaneous Errors** – 1%
- **Denial-of-Service Attacks** – 0% *(but 3% of security incidents in 2013 were due to DoS attacks)*
- **Everything Else** – 5%
3. Lessons Learned: Significant Consequences; Key Factors Impacting Overall Costs; and Post-Breach Action
Key Consequences of a Data Breach

Figure 14: Impact of the breach
More than one response permitted

- Lost reputation, brand value and marketplace image: 45% Malicious, 39% Non-malicious
- None: 23% Malicious, 30% Non-malicious
- Cost of notification: 6% Malicious, 37% Non-malicious
- Lost time and productivity: 71% Malicious, 33% Non-malicious
- Out-of-pocket costs to prevent harm to breach victims: 14% Malicious, 32% Non-malicious
- Lost customers: 14% Malicious, 30% Non-malicious
- Regulatory fines and lawsuits: 5% Malicious, 25% Non-malicious
- Lost revenues: 20% Malicious, 16% Non-malicious
- Cost of outside consultants and attorneys: 17% Malicious, 11% Non-malicious
- Cost of purchased technologies: 0% Malicious, 35% Non-malicious
- Other: 1% Malicious, 1% Non-malicious
Nearly two thirds of U.S. adults surveyed said they would not return to a business where personal information was stolen:

- 55 percent would change banks
- 46 percent would switch insurance companies
- 42 percent would go to a different drug store/pharmacy
- 40 percent would get a new doctor or dentist
- 39 percent would get a new lawyer
- 38 percent would donate to a different charity/non-profit organization
- 35 percent would not return to their hospital
- 24 percent would no longer donate to their alma mater or another educational institution they attended
Data Breaches are Increasing in Volume and Expense

- **823 million:** Exposed records (compared to 264 million in 2012)
- **$145:** Average cost per record breached
- **$3.5 million:** Average recovery cost from a single data breach

$145: Average cost per record breached

$3.5 million: Average recovery cost from a single data breach
Certain Industries Have Higher Data Breach Costs

Figure 4. Per capita cost by industry classification
Consolidated view (n=314)

- Healthcare: $359
- Education: $294
- Pharmaceutical: $227
- Financial: $206
- Communications: $177
- Industrial: $160
- Consumer: $155
- Services: $145
- Energy: $141
- Technology: $138
- Media: $137
- Hospitality: $122
- Transportation: $121
- Research: $119
- Retail: $105
- Public: $100
Key Factors Increasing Costs

• Data breaches caused by third parties increased per record cost by $25

• Data breaches involving lost or stolen devices increased per record cost by as much as $18

• Rushing into notifying affected individuals without a thorough assessment or forensic examination increased cost by an average of $15 more per record

• Engaging forensic consultants
Key Factors Reducing Costs

- Involving business continuity management in remediation of a breach can reduce the cost by an average of $13 per compromised record.

- Having a strong organizational security posture can reduce the average cost by as much as $21 per record.

- Having a formal incident response plan in place prior to the data breach can reduce the average cost by $17 per record.

- Appointing a Corporate Information Security Officer (CISO) to lead the data breach incident response team can reduce the cost by $10 per record.
Actions Believed to be Most Helpful in Reducing the Negative Consequences of a Data Breach

- Retained outside legal counsel: 56% in 2011, 43% in 2007
- Careful assessment of the harm to victims: 50% in 2011, 45% in 2007
- Hired forensic experts to investigate the breach: 45% in 2011, 5% in 2007
- Prompt notification to regulators on voluntary basis: 19% in 2011, 6% in 2007
- Responded to all media inquiries: 15% in 2011, 3% in 2007
- Prompt notification to regulators as required by law: 12% in 2011, 3% in 2007
- Prompt notification by placing an ad in a newspaper: 8% in 2011, 2% in 2007
- Prompt notification to victims by letter: 22% in 2011, 6% in 2007
- Prompt notification to victims by telephone: 22% in 2011, 5% in 2007

*The FY 2007 survey did not contain this choice*
Steps Taken by Organizations to Address Vulnerabilities After Data Breach

- Conducting training and awareness
- Controlling endpoints to the organization’s systems
- Hiring outside counsel to provide legal advice
- Establishing incident response plan
- Investing in encryption solutions
- Investing in security event management tools (SEIM)
- Hiring in-house personnel to lead data protection efforts
- Investing in identity & access management solutions
- Conducting a post mortem
- Investing in data loss detection and prevention technology
- Hiring security consultants to help data protection efforts
- Investing in perimeter controls

2007 vs. 2011
Changes Implemented by Organizations After Data Breaches

- Our organization limits the amount of personal data collected: 49%
- Our organization limits sharing with third parties: 48%
- Our organization limits the amount of personal data stored: 42%
- Strict rules were established to limit access to data: 39%
- No affect: 31%
- Our organization limits personal information used for marketing: 27%
- Unsure: 22%
- Our organization limits social media interaction: 19%
10 CRITICAL STEPS CORPORATIONS SHOULD TAKE NOW TO REDUCE THE RISKS AND COSTS OF DATA BREACHES
Overview of 10 Critical Steps

1. Identify Data Privacy and Security Team, and Obtain Executive Buy-In

2. Conduct Regular Risk Assessments

3. Minimize Personal Data Collection, Access, and Retention

4. Adopt Policies and Procedures that Accurately Reflect Your Company’s Unique Practices

5. Develop and Implement Layered Information Security Program
6. Combat Mobile Threats

7. Develop and Implement Procedures for Securely Disposing of Personal Data

8. Train Staff to Implement Privacy and Security Programs

9. Take Steps to Help Ensure Vendors will Protect Personal Data Entrusted to Them

Step 1: Identify Data Privacy and Security Team, and Obtain Executive Buy-In

- Designate leader(s) with organization-wide responsibilities

- Select team members:
  - Internal (e.g., Legal, Compliance, IT/IS, HR and Communications)
  - External (e.g., outside counsel, electronic forensics consultants, and PR)

- Obtain executive buy-in
Step 2: Conduct Regular Risk Assessments

- Analyze stored personal data, map data flows, and determine who has access
- Evaluate risks
- Develop and implement a risk mitigation plan
Step 3: Minimize Personal Data Collection, Access, and Retention

- Only collect necessary data
- Promptly return any unneeded data
- Securely dispose of any unnecessary copies
Step 3: Minimize Personal Data Collection, Access, and Retention

- Minimize access to fullest extent possible
- Only transfer when absolutely necessary, and do so securely
- Dispose of all copies as soon as no longer needed for business or legal reasons
Step 4: Adopt Policies and Procedures that Accurately Reflect Your Company’s Unique Practices

- Data Privacy
- Information Security
“We understand you’re not happy with our privacy policy.”
Step 5: Develop and Implement Layered Information Security Program

- Strong passwords/dual-authentication procedures
- Encryption
- Anti-virus and anti-malware protection
- Firewalls
- Intrusion detection
Step 5: Develop and Implement Layered Information Security Program

- Access controls
- Limited administrative rights
- Segmentation
- Device hardening
- Data loss prevention technology
Step 5: Develop and Implement Layered Information Security Program

- Keeping equipment up-to-date
- Patching and system updates
- Vulnerability assessments and penetration testing
- Logging/monitoring for problems
- Physical security
Step 6: Combat Mobile Threats

- Institute a mobile device security policy
- Educate employees about the importance of safeguarding mobile devices
- Install hardware or software USB locks on computers, laptops or other devices to prevent unauthorized data transfer through USB ports and thumb drives
Step 6: Combat Mobile Threats

- Encrypt mobile devices and removable media (e.g., USB drives)
- Secure mobile devices from malware, viruses, and malicious applications and require users to implement anti-malware protection if available
- Consider mobile device management ("MDM") technology that creates a virtual partition in the device separating work data from personal data
Step 6: Combat Mobile Threats

- Establish protocols for reporting lost or stolen devices
- Invest in geolocation tracking software or services
- “Brick” the mobile device when it is lost or stolen
- Get ahead of the “BYOD upgrade” curve by ensuring that the devices coming offline are adequately secured and checked before disposal or donation
Step 7: Develop and Implement Procedures for Securely Disposing of Personal Data

- Completely delete or destroy all copies, locations, and formats in a confidential matter
  - Paper:
    - Secure shredding
    - Burning, pulping, or pulverizing
    - Locked, secure destruction container
  - Electronic Form: Completely Deleting
  - Media and Equipment: Physically destroying the device or over-writing the data:
    - Clearing
    - Purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains)
    - Destroying (disintegration, pulverization, melting, incinerating, or shredding) the media
Step 8: Train Staff to Implement Privacy and Security Programs

- Conduct training, including situational training
- Post FAQs
- Provide periodic tips, reminders and/or visual workplace cues
- Monitor staff awareness and compliance
Step 9: Take Steps to Help Ensure Vendors Will Protect Personal Data Entrusted to Them

- Exercise due diligence in selecting vendors
- Contractually require vendors to protect personal data
- Use the principle of “least privilege”
- Consider monitoring/audit program
Step 10: Establish Security Incident/Data Breach Response Procedures

- Identification
- Containment and recovery
- Assessment of risks
- Breach notification
- Evaluation and response
Recommended Resources

- Data Privacy Resources
- Information Security Resources
- Mobile Device Security Resources
- Cloud Computing Resources
- Data Breach Response
ANY QUESTIONS?
CONTACT INFORMATION

Laura Clark Fey, ESQ., CIPP/US
Partner, Daley & Fey LLP

Email: lfey@daleylegal.com
Direct: 913-948-6301
Mobile: 816-518-6554