Data Security:
The Problem and Solutions

Association of Corporate Counsel

Veronica D. Jackson | Marietta, PA | April 23, 2018

MILES & STOCKBRIDGE

About the Speaker

vjackson@milesstockbridge.com
Direct Dial: 410-385-3499

Veronica is a Senior Associate at Miles & Stockbridge. She is a member of the Labor and Employment practice group at Miles & Stockbridge, P.C.

Veronica concentrates her practice on employment litigation and data privacy and security.

She routinely advises clients on data privacy and security issues and counsels clients through data breaches and other cyber incidents.

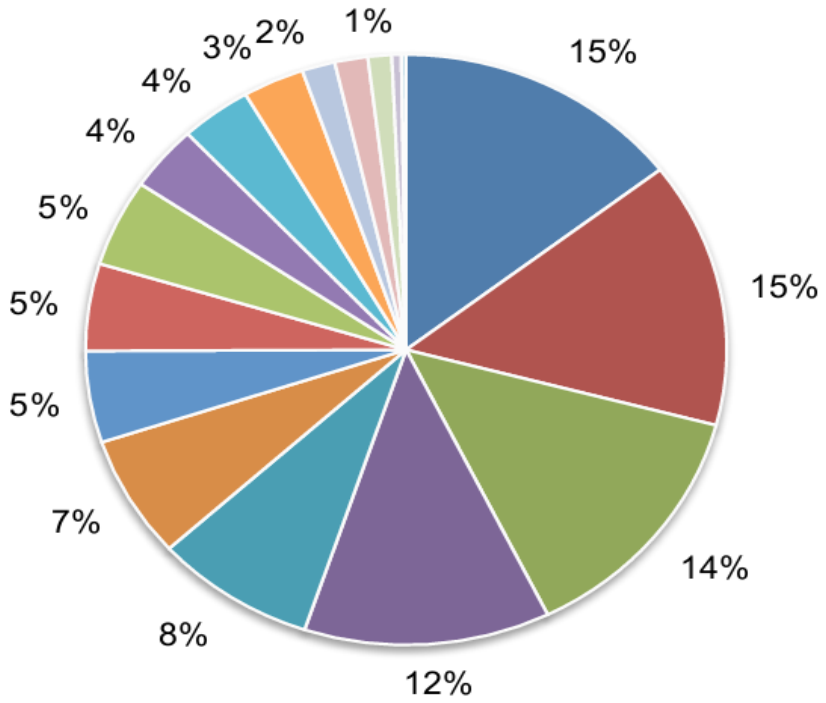
In addition to her law degree, Veronica is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals (IAPP).

MILES & STOCKBRIDGE

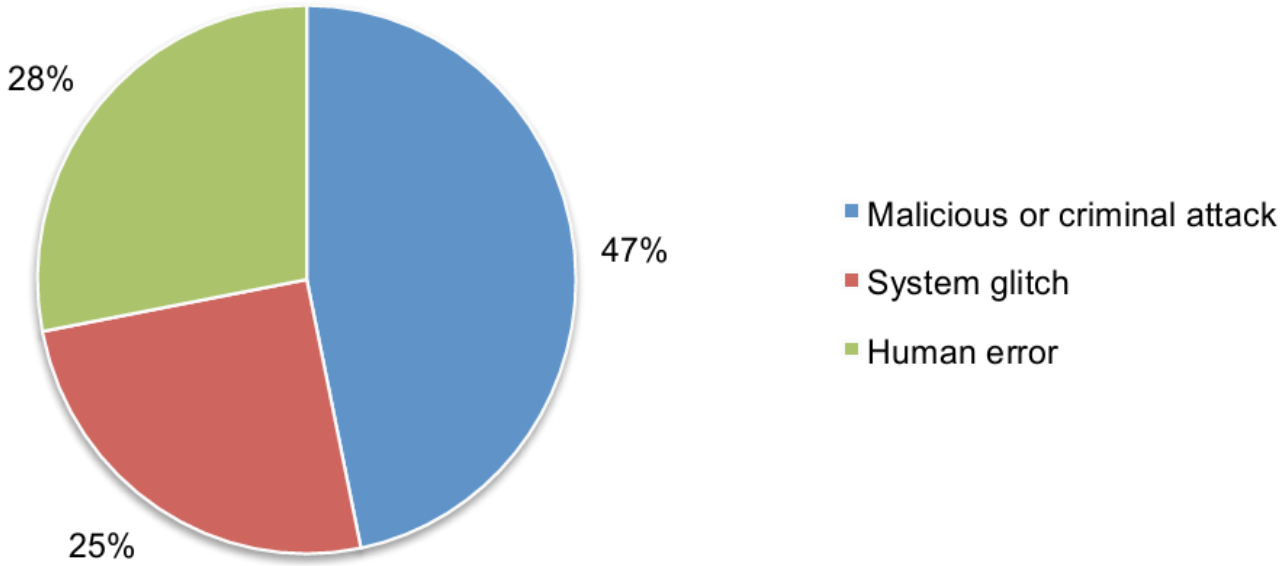
The Problem: Common Data Security Scenarios

DEEP RELATIONSHIPS, FORWARD THINKING. AND NOT JUST A LAWYER, A TEAM.

2017 Data Breach Statistics by Industry



Data Security:
Internal Defense Is Key



Source: 2017 Ponemon Institute Study, Costs of Data Breaches in United States, sponsored by IBM

Hot Trends in Cybersecurity

MILES & STOCKBRIDGE

- Trends are industry-specific
- It is not an accident anymore – "Inevitable"
- Cyber Espionage
- Business Email Compromises (BEC) and other phishing schemes. (*e.g.*, W2 Breaches)

Real or Not?

UPS.com <tracking@ups.com>

NOTIFICATION - Package delivery confirmation

To [redacted]

Dear client,
Your package has been delivered to the local UPS office.
The tracking# is: **1Z12Y6169096771351** and can be used at :
http://wwwapps.ups.com/WebTracking/track?loc=en_US

The shipping invoice can be downloaded, in PDF format, from :
http://wwwapps.ups.com/WebTracking/trackinginvoicedownload.aspx?package_id=820919

In order, to claim your item, visit our office with a printed copy of the shipping invoice.
Thank you,

***Do not reply to this e-mail. UPS and GRD GROUPON GOODS WAREHOUSE will not receive your reply.

At the request of GRD GROUPON GOODS WAREHOUSE, this notice alerts you that the shipment listed below has been delivered.

Important Delivery Information

Tracking Number:	927899999855335730229013 94
Alternate Tracking Number:	061251218151868351
Delivery Date/Time:	12/23/2015 / 11:10 AM
Status:	DELIVERED

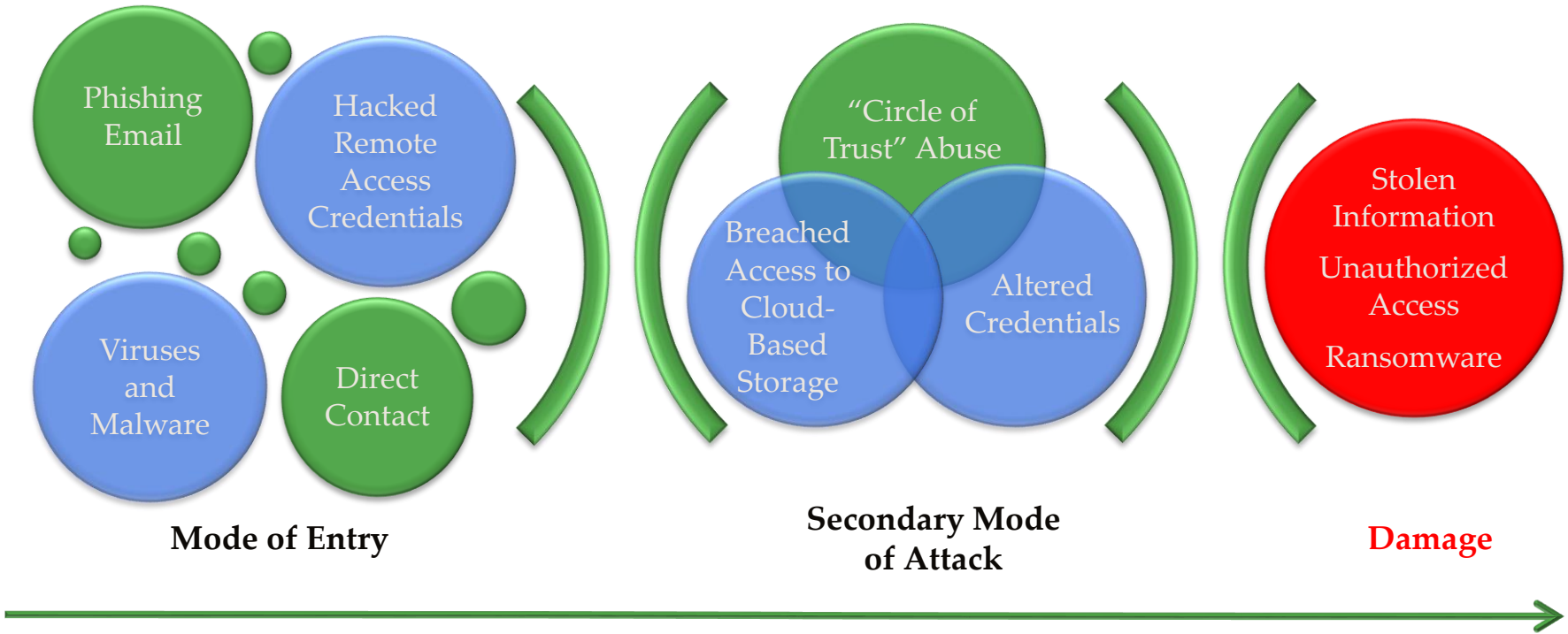
Shipment Detail

Ship To:

[redacted]

Number of Packages:	1
UPS Service:	UPS Mail Innovations Expedited
Weight:	0.2 LBS
Tracking Number:	927899999855335730229013 94
Package ID:	00000999990045302731
ShipmentCostCenter:	GROUND

Life Cycle of a Hack: Some Examples



MILES & STOCKBRIDGE

Ethical Concerns
Data Security & Confidentiality

DEEP RELATIONSHIPS, FORWARD THINKING. AND NOT JUST A LAWYER, A TEAM.

ABA Rule 1.1

"To maintain the ***requisite knowledge and skill***, a lawyer should keep abreast of change sin the law and its practice, including the ***benefits and risks associated to relevant technology***, engage in continuing study and education and comply with all continuing legal education and requirements to which the lawyer is subject."

ABA Commission explained … "***These tasks now require lawyers to have a firm grasp on how electronic information is created, stored, and retrieved***… 'notable developments' in technology that have impacted the practice of law to include electronic communication; mobile electronic storage; third-party servers; how clients find lawyers; virtual offices; and online practice management."

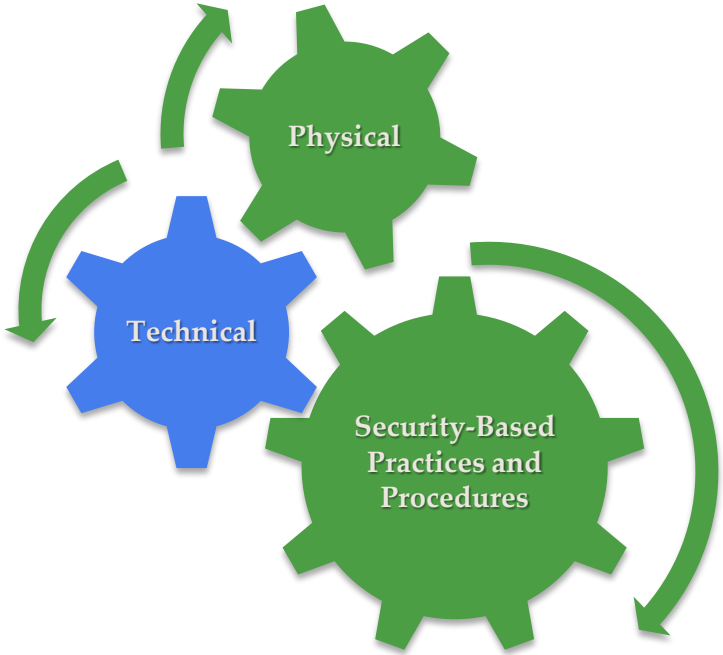
Data Security is a Fiduciary Duty

- Protection of confidential information is a fiduciary duty
- Duties of officers and directors
- Duty of Care
  - Duty to exercise adequate oversight
- Duty of Loyalty
  - Includes Duty of Confidentiality
- Liability for breach

The Solution:
Best Practices for Data Security

DEEP RELATIONSHIPS, FORWARD THINKING. AND NOT JUST A LAWYER, A TEAM.

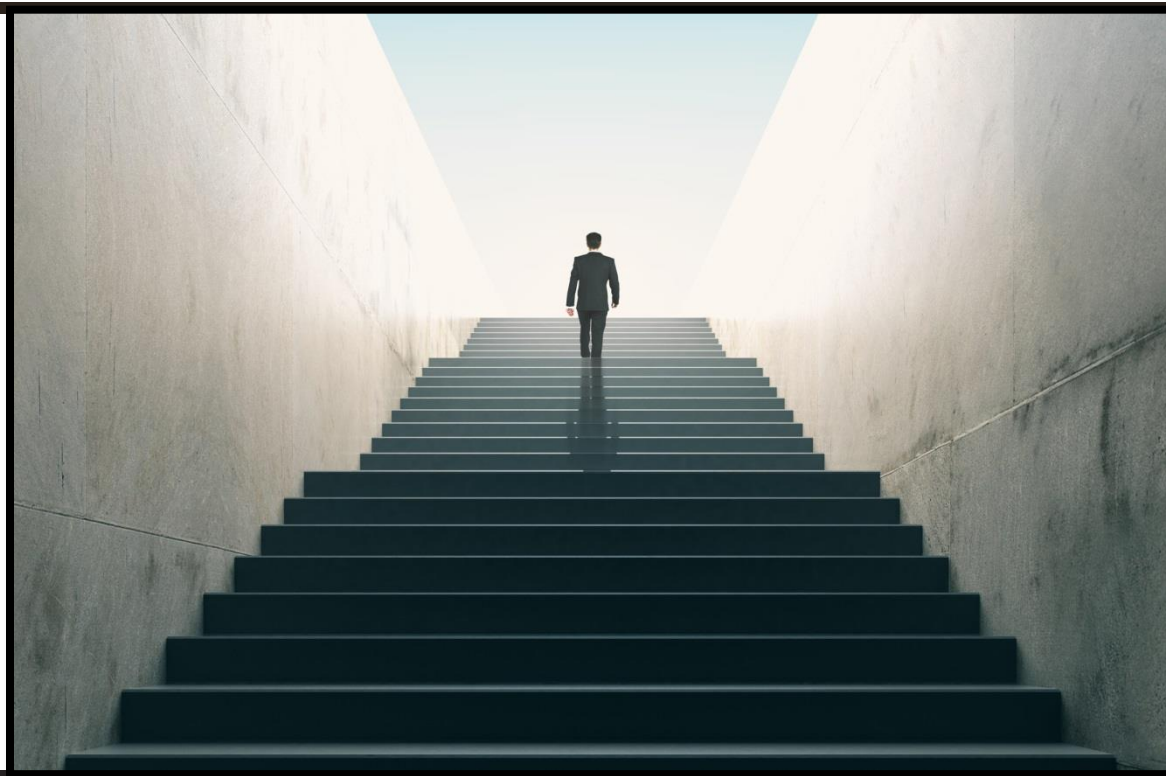
Data Security Tools



Anatomy of Data Security

Three stages:

1. Pre-breach
2. Breach response
3. Post-breach



Pre-Breach

Written Information Security Program (WISP)

- A living program – not just policies – that defines security practices & exposures
- Best defense to litigation & regulatory actions
- Required by SEC, GLB, FED, FDIC, OCC, FISMA, HIPAA, Massachusetts, GDPR, PCI – DSS
- Defines current regulatory & liability environment
- Identifies IRT members, including IT, Security, Legal, Compliance, Communications
  - Outside counsel/privilege considerations
- ***Training is essential!***

Pre-Breach

MILES & STOCKBRIDGE

Steps to take <u>before</u> a breach occurs:

- Identify most critical cyber assets and risks
- Audit data flows within organization; assess vulnerabilities
- Assess applicable data security and breach notification laws
  - (Note: state notification laws apply based on the state of residence of the data subject.)
- Written information security program
- Incident response team and plan
- Penetration testing and breach response drills
- Know your local FBI cyber crimes specialist

Employees as First Line of Defense

Tips to promote data security compliance and early reporting:

- Clear and accessible policies
- Training
- Limited access
- "See something, say something."
- Reporting incentives?
- Violation consequences?

Contract Considerations

- Pre-Contract Considerations
  - Criticality of the relationship
  - Internal practices, policies and protocols
  - Determine extent of due diligence and develop the due diligence process
- The Contract and On-Going Relationship Management
  - Operational concerns
  - Legal/Risk management issues
  - Communications needs
- Exiting the Vendor Relationship
  - Return of information
  - Transition needs
  - Post-relationship dealings

Insurance Do's and Don'ts

- **Do** consider that you have coverage under your CGL, despite recent narrowed definitions and cyber exclusions.
  - *Travelers Indemnity v. Portal Healthcare Solutions* (4th Circuit, 3/24/2016): Upheld duty to defend under CGL policy because data breach was a "publication."
  - *But see Zurich Am. Ins. v. Sony*, (N.Y. Sup. Ct., 2/21/2014): Held no coverage, ruling that there was no publication when third party hackers caused data exposure.
- **Don't** forget: the duty to defend is broader than liability coverage.
- **Do** your homework before purchasing a cyber liability policy.
- **Don't** void your policy by failing to implement basic data security measures or for untimely notice of incident to carrier.

The Solution:
Best Practices – Responding to a Breach

DEEP RELATIONSHIPS, FORWARD THINKING. AND NOT JUST A LAWYER, A TEAM.

And Then the Phone Rings…

Files and Lockbridge, an *unrelated* firm client, calls you frantically because they have a problem. F&L is a government contractor based in Maryland that exclusively does business with the federal government. They just learned that Abby Whelan, F&L's former head of HR who was recently fired, had apparently been saving company personnel records onto her personal cloud-based Carbonite account. They tell you that, while she had a written agreement with the CEO, Fitz Grant, allowing her to use a company laptop for both business and personal use, she was *not* authorized to save company files onto Carbonite. F&L retrieved the company laptop but it had been wiped clean. Huck, the IT guy, was able to restore the laptop so that they know what files were on it and therefore uploaded to Carbonite. You call Carbonite and they confirm someone, the day after Abby was fired, "restored" the backups onto a new computer.

The files include the SS#s of F&L employees, past and present, home contact info, bank account #s (for those that set up direct deposit), and SS#s for some spouses and children that were named as beneficiaries for F&L's life insurance policies. Grant wrote Abby a threatening letter already but is otherwise clueless on what to do next.

A day later you get a call from Olivia Pope, Abby's lawyer, and she wants you to know that there "is no issue here" because Abby has no interest in the files and wants to confirm that you aren't calling the police. ***What do you do?***

Breach Response – Initial Questions

MILES & STOCKBRIDGE

Evaluating Scope and Cause

- When did the breach occur?
- How did it occur?
- Who/what was the unauthorized access?
- What systems and locations were involved/impacted?
- What users were impacted?
- Was the data acquired or viewed?
- Was the information encrypted?
- Employee data, customer data, or both?
- Is the breach ongoing?

Breach Response

MILES & STOCKBRIDGE

- Evaluating Scope
  - Is it PII under any state statute?
  - Is it PHI under HIPAA?
  - Is Gramm-Leach-Bliley-Act implicated?
  - Payment card breach? (One day to notify merchant bank or payment processor)
  - How many states impacted? Any international impact?
  - If notification is required in some jurisdictions, but not others, make decision about voluntary notification
  - Identify and assemble key agreements with clients and subcontractors to determine any contractual obligations
  - Any internal policies/procedures violated?

Breach Response

MILES & STOCKBRIDGE

What is a Data Breach?

- CA: "***unauthorized acquisition*** of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business." Cal. Civ. Code § 1798.82
- FL: "***unauthorized access*** of data in electronic form containing personal information." Fla. Stat. § 501.171
- NC: "an incident of ***unauthorized access to and acquisition of*** unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer." N.C. Gen. Stat. § 75-61

Breach Response

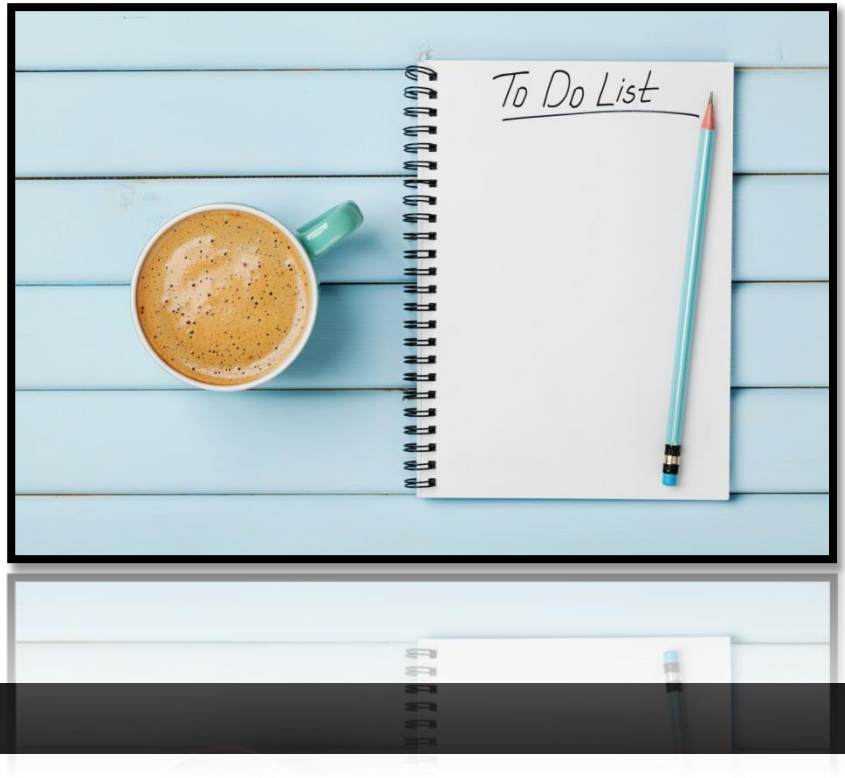
Maryland (Md. Code Ann., § 14-305 *et seq.*)

"***Personal information***" means an individual's first name or first initial and last name in combination with any one or more of the following that is not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable:

- SSN;
- Driver's license number;
- Financial account number (credit or debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's financial account); or
- Tax identification number.

Breach Response

- Liability Mitigation
- Law Enforcement
- Data Breach Notifications
- Other required notifications
- Strategic Communications



MILES & STOCKBRIDGE

ANY QUESTIONS