

Public Entity Cybersecurity Risks, Mitigation & Breach Response



May 16, 2017

James Giszczak | Dominic Paluzzi
McDonald Hopkins

McDonald Hopkins
A business advisory and advocacy law firm®

Chicago Cleveland Columbus Detroit Miami West Palm Beach

agrip
ASSOCIATION OF
GOVERNMENTAL RISK POOLS

Overview of Topics

- What Data Must Be Protected?
- Types of Privacy Incidents
- Defining a Data Breach & Breach Notification Laws
- Proactive Measures to Minimize the Risk of a Data Breach
- Cyber Trends within Public Entities
- Real-World Data Breach Examples
- Incident Response Process
- Q & A

McDonald Hopkins
A business advisory and advocacy law firm®

Chicago Cleveland Columbus Detroit Miami West Palm Beach

agrip
ASSOCIATION OF
GOVERNMENTAL RISK POOLS

What Data Must Be Protected?

■ Personally Identifiable Information (PII)

- Social Security number
- Drivers license number
- Credit/debit card numbers
- Passport number
- Bank Account Information
- Date of Birth
- Medical Information
- Mother's maiden name
- Biometric data (i.e., fingerprint)
- E-mail/username in combination with password/security question & answer

In combination with name
(either First Name & Last Name
or First Initial & Last Name)



What Data Must Be Protected?

■ Protected Health Information (PHI)

- Medical records
- Health status
- Provision of health care
- Payment for health care

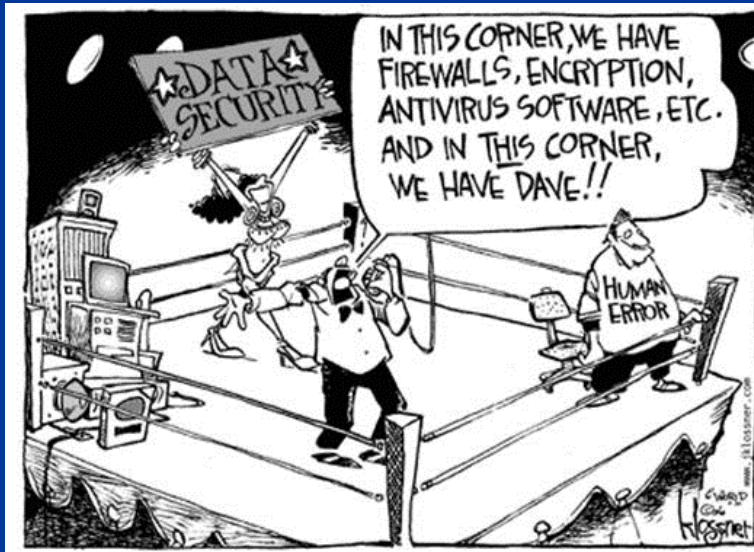
■ HIPAA



What Data Must Be Protected?

■ Payment Card Information (PCI)

- Primary Account Number (PAN)
- Cardholder Name
- Expiration Date
- Service Code (3 or 4 digit code)
- PIN



Top 10 Passwords Discovered in Data Breaches in 2016


1. 123456	6. 123456789
2. password	7. football
3. 12345678	8. 1234
4. qwerty	9. 1234567
5. 12345	10. baseball

McDonald Hopkins Chicago Cleveland Columbus Detroit Miami West Palm Beach
A business advisory and advocacy law firm®

agrip ASSOCIATION OF GOVERNMENTAL RISK POOLS

Primary Types of Privacy Incidents

- **Physical loss:** Stolen or lost laptop, PDA, thumb drive, or other portable media containing PII or other sensitive data
 - Mitigation
 - Encrypt
 - Prohibit / minimize / block saving PII on portable media
 - Records management



McDonald Hopkins Chicago Cleveland Columbus Detroit Miami West Palm Beach
A business advisory and advocacy law firm®

agrip ASSOCIATION OF GOVERNMENTAL RISK POOLS

Primary Types of Privacy Incidents

- **Hardcopies:** Mis-mail, Misplaced, Stolen, or “Disposal Fail”

- Mitigation

- Handling policy and training
- Disposal policy and training
- Diligence/contracts with records management/disposal vendors



Primary Types of Privacy Incidents

- **Unintended Disclosures**

- “Computer Glitch”
- Incorrect Permission Settings
- Misdirected Email / Fax

- Mitigation

- Regular systems and/or vulnerability testing
- Encrypt or password-protect files
- Outlook delay



Primary Types of Privacy Incidents

- **Vendors:** Negligence, physical loss, database/server breach or stolen data at a vendor's location or server
 - Increases response costs about 20%
 - Mitigation
 - Vendor contract provisions
 - Appropriate review of vendors to confirm safeguards are in place



Primary Types of Privacy Incidents

- **Stolen Data by Otherwise Authorized Users:** Rogue Employee or other malicious insider with access downloads or sends personal or sensitive data to another unauthorized location for an improper purpose
 - Mitigation
 - Systems activity review – logging and periodic monitoring
 - Access reviews

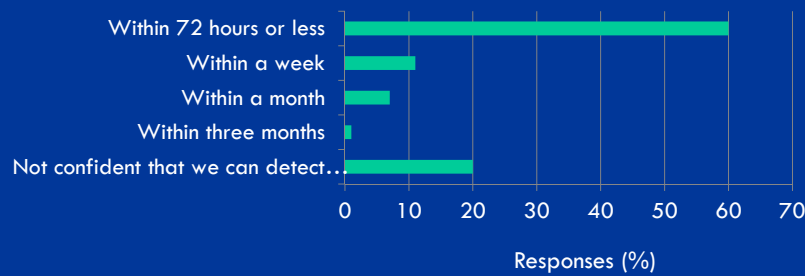


Primary Types of Privacy Incidents

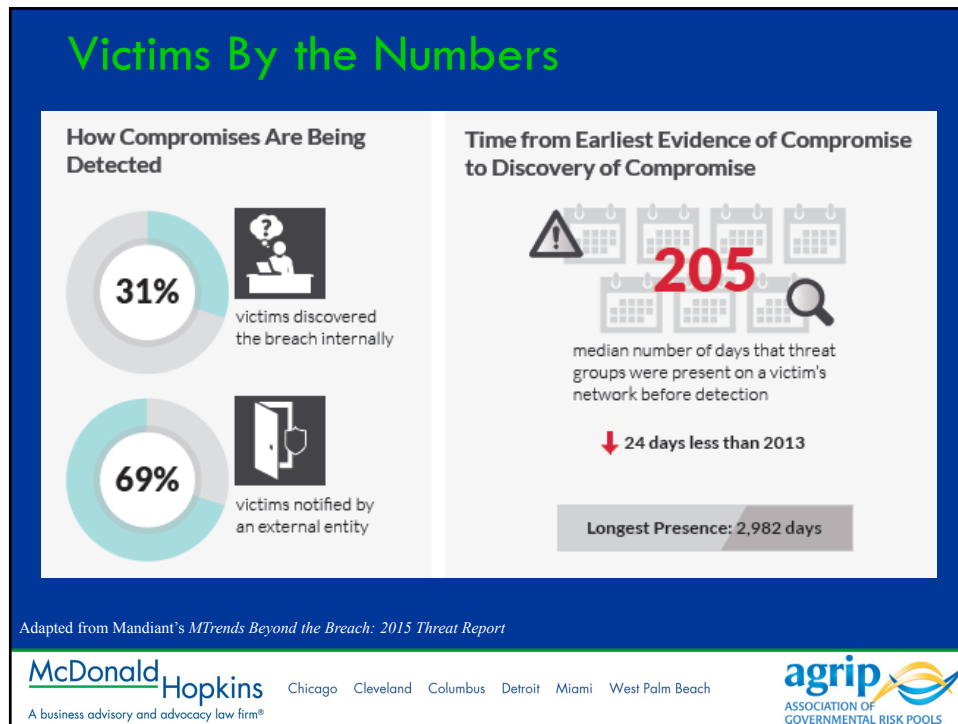
- **Database/server breach:** Unauthorized person accesses or hacks into a data server that stores personal or other sensitive data
 - Malware; Hackers; Phishing; Ransomware
 - Mitigation
 - Penetration testing, firewalls, intrusion detection, etc.
 - Systems activity review – logging and periodic monitoring
 - Training of employees



Companies are Still Too Optimistic About Ability to Detect an Attack



*Information from Tripwire Breach Detection Survey,
<http://www.tripwire.com/company/research/us-retail-survey/>.



Reputational Harm

- Consumer Study on Data Breach Notification
 - 62% said breach notification decreased trust and confidence in the organization
 - 15% would terminate their relationship with the notifying company (39% would consider terminating)
 - 94% believe reporting organization is solely to blame for breach
 - 72% thought organizations do a poor job communicating and handling a data breach

(Source: Ponemon Institute & Experian Data Breach Resolution)

Chicago Cleveland Columbus Detroit Miami West Palm Beach

ASSOCIATION OF GOVERNMENTAL RISK POOLS

What is a Data Breach?

- Definition varies from state to state, but typically includes:
 - Unauthorized acquisition / access / use
 - of Personally Identifiable Information (PII)
 - Unencrypted
 - Compromising the security, confidentiality or integrity of PII
 - Does not include good faith acquisition of PII

What is a Data Breach? (That may trigger state notification laws)

- Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII . . .
 - *that results or could result in identity theft or fraud (OH)*
 - *unless PII is not used or subject to further unauthorized disclosure (NE)*
 - *unless no misuse of PII has occurred or is not reasonably likely to occur (NJ)*
 - *unless no reasonable likelihood of harm to consumer whose PII was acquired has resulted or will result (CT)*

What is a Data Breach? (That may trigger state notification laws)

- Unauthorized acquisition of PII that compromises the security, confidentiality or integrity of PII . . .
 - *that has caused or is likely to cause loss or injury to resident (MI)*
 - *that causes or is reasonably likely to cause substantial economic loss to the individual (AZ)*
 - *unless no reasonable likelihood of financial harm to consumer whose PII was acquired has resulted or will result (IA)*

Why we should be careful with the word "breach"

- Using "breach" to describe a data-privacy related incident assumes the incident meets the definition of a security breach which triggers various notification requirements
- An "incident" does not always rise to the level of "breach" (i.e., encryption safe harbor)
- "Incident" is better received by the public than "breach"

Breach Notification Laws

- State laws *differ* with respect to:
 - Deadline for notifying (14, 30, 45 days; reasonable time)
 - Notification to Attorney General
 - Notification to other State Agencies
 - Including Attorney General contact information
 - Substitute notice (email, website, media)
 - Specific facts of incident and type of PI compromised
 - Maintaining records of incident (for 3-5 years)
- Countries also differ with notice requirements

PCI DSS

(Payment Card Industry Data Security Standard)

- Established in 2004 by major credit card companies
- Requires merchants accepting credit, debit & other payment cards to safeguard cardholder data
 - Primary Account Number (PAN)
 - Cardholder Name
 - Expiration Date
 - Service Code (3 or 4 digit code)
- All merchants (anyone accepting credit card payments) are required, under merchant banking agreements, to comply with PCI standards.



PCI DSS

- Self-regulated
- The enforcement arm is the card brands via the acquiring banks/processors
- Penalties = fines and increased interchange rates imposed by acquirers/processors
- Data Security Standard (DSS) is well defined (288 requirements) but still open for interpretation
- PCI Compliant merchants are still breached (Target)
- Compliance ≠ Security

Proactive Measures

- A Written Information Security Program (WISP)
 - Required by Massachusetts law, GLBA and FTC Red Flags Rule
- Incident Response Plan
 - Required by PCI DSS, GLBA and HIPAA
- Carefully drafted Confidentiality Agreements for employees, vendors and visitors
- Proper and ongoing training of employees on entity's data security programs & cyber awareness
- Perform a data privacy review & risk assessment, including penetration testing
- Review your employee exit process

PII Destruction/Disposal Laws & Document Retention Issues

- 32 States have data disposal / destruction laws
- A business that maintains records which contain PII concerning customers and employees of the business shall take reasonable measures to ensure the destruction of those records when the entity decides that it ***no longer has a legitimate business reason to maintain***
- **Destruction** = Shredding of the record containing PII or erasing the PII from the records
- The failure to destroy unnecessarily increases the number of records in a breach
- AG can impose fines/penalties



Who Should Be On Your Incident Response Team?

- Because the issue impacts almost every component of the organization, and failure to properly manage can result in both long and short term consequences, the team should include “C” level decision makers in the following areas:
 - Legal
 - IT
 - Risk Management/Insurance
 - HR
 - Marketing
 - Public Relations
 - Compliance & Internal Audit
 - Physical security
 - Other executives, as appropriate
 - 3rd party response services (e.g., forensics, privacy counsel, notification)



Incident Response Plan

- The “go to” document
- Identifies the Incident Response Team
 - Roles & Responsibilities
 - Internal & External Capabilities
 - Contact Info (work, cell, home)
 - Alternates
- Decision Trees
- Notification/Escalation Process
- Incident Reports for Gathering Evidence
- Test IRP & IRT

Other Privacy Policies

- Computer and electronic devices usage
- Document retention and destruction
- BYOD
- Telecommuting
- Social media
- Website privacy policy & terms of use
- Physical and logical access security

Vendor Agreements

- Compliance with data privacy standards for the protection of PII, PHI and/or PCI
- Return or destruction of PII, PHI and/or PCI
- Use of subcontractors with access to PII, PHI and/or PCI
- Notice of security and/or privacy incident within _____ hours
- Indemnification
- Cyber liability insurance

Cyber Trends within Public Entities

- Common Misconceptions
- Use of unsecured wireless connections to internal network
- Lack of encryption (laptops, desktops, smartphones, USB storage = > 40% data breaches)
- Ineffective password policies (complexity, length, age)
- Weak Physical Security
- Inadequate Network Security
- Lack of Vendor controls



Public Entity Breach Examples

▪ Wisconsin Dept. of Revenue

- An annual sales report contained the Social Security and tax identification numbers of people and businesses who sold property in Wisconsin.
- The report was available online between for 3 months and meant for real estate professionals.
- The report was accessed a total of 138 times before being taken down.
- A total of 110,795 sales were made in Wisconsin during time period, but not everyone who made a sale provided their Social Security or tax identification number for the paperwork.

Public Entity Breach Examples

▪ New Hampshire Dept. of Corrections

- A staff member found that a cable line hooked to the computers used by inmates had been connected to a line connecting to the entire Concord prison computer system.
- Allowed one or more prisoners to view, steal, or change sensitive records, including staff member information and sentencing and parole dates.
- Information from the offender management database system "Corrections Offender Records and Information System" may have been compromised as well.

Public Entity Breach Examples

▪ Baltimore County, MD

- A contractor who worked for Baltimore County was found to have saved the personal information of 12,000 county employees to computers for reasons unrelated to work.
- Employees who had their paychecks direct deposited were affected and the bank account information of 6,633 employees was exposed.
- Baltimore county employees are no longer allowed to download personal information to county computers and more than 5,000 county hard drives will be cleared of related data.

Other Real World Examples

- Donation of CDs
- Hack of Database of Checks
- Inadvertent Email to “All” Users
- Compromise of log-in credentials (targeting DoD projects)
- Theft by HR employees
- Shared Drive Incorrect Permission Settings

Other Real World Examples

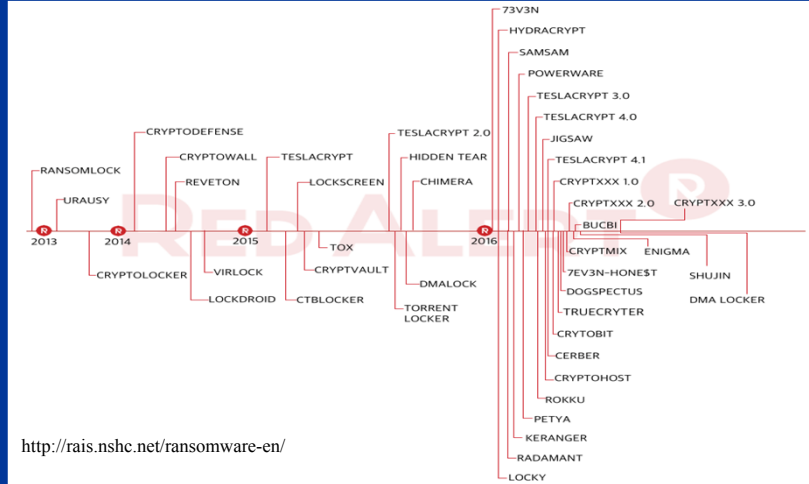
- Stolen Laptop / Unnecessary Media Notification
- Thumb Drive Bowl
- Card Skimmers
- Payroll Vendor
- Phishing scams (CEO W2s)
- Ransomware Attacks



Impact of Ransomware

- FBI reported that extortion attempts cost companies \$209 million in Q1 of 2016
 - Expected to be a billion dollar industry in 2016
 - Easy money for cyber criminals
- Untold amount of ransomware variants
 - Capabilities will vary based on the variant
- Stakes are getting higher for companies
 - Bigger business impact, greater losses

Evolution of Ransomware



<http://rais.nshc.net/ransomware-en/>

Phishing Attacks

From: <Name of executive / CEO / CFO> <corporate email address>
Reply-To: <Name of executive / CEO / CFO> <non-corporate email address>
To: <Targeted victim in HR / Finance>
Subject: SALARY REVIEW

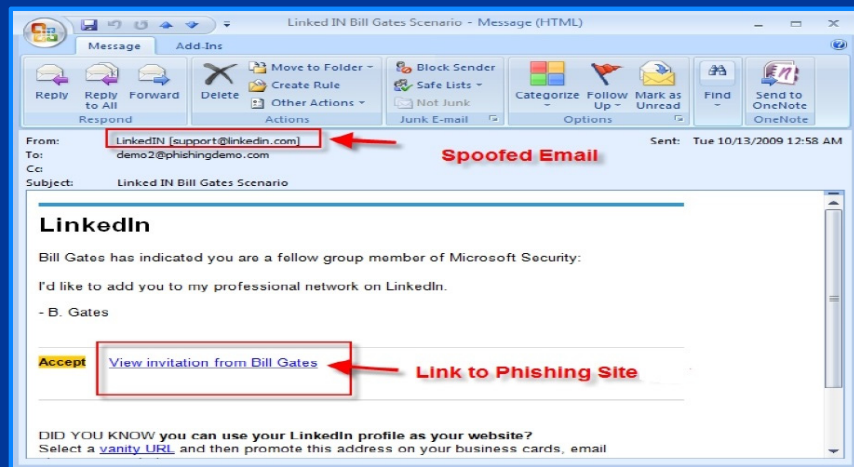
Hello

Kindly send me the 2015 W-2 (PDF) of all our company staffs for a quick review

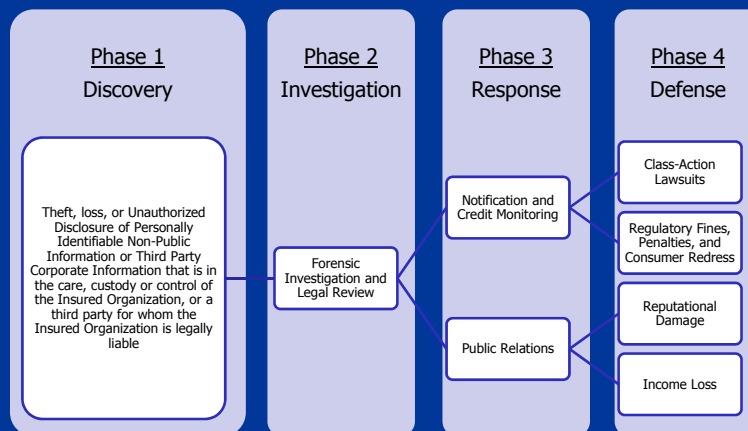
Thanks



Phishing Attacks



A Simplified View of a Data Breach Response Methodology



Once an “Incident” Occurs, What Should the Entity Do Next?

- Put **cyber insurance carrier/broker/pool** on notice of the incident
- Engage **privacy attorney** (breach coach) to maintain all communications as Privileged
- Gather members of Incident Response Team (IT, HR, legal, communications, risk, finance etc.)
 - Determine & assign an **IRT Leader**

Once an “Incident” Occurs, What Should the Entity Do Next?

- Immediately **gather and preserve all evidence** of the potential breach and secure the systems to prevent additional exposure
- **Take notes** and document each step of your response
- Engage a **forensic specialist** (through privacy attorney) to determine the breadth and scope of the incident, contain the breach, and quantify the records comprised
- Consider contacting **law enforcement** agencies about the incident, if appropriate

Once an "Incident" Occurs, What Should the Entity Do Next?

- Determine if notice must be provided by law (or whether there is a business reason to notify)
- Work with an experienced breach coach to craft notifications in compliance with the numerous state, federal, international, and industry-specific breach notice laws
 - **Residence** of affected individuals determines applicable notice law
 - **Encryption or Redaction** may provide exception (i.e., MI, OH)

Once an "Incident" Occurs, What Should the Entity Do Next?

- Work with your breach coach to **notify** appropriate parties, including:
 - Affected individuals (utilizing a notification vendor as necessary)
 - State attorneys general
 - Other state agencies (i.e., state police, Office of Cybersecurity, Office of Consumer Protection)
 - Federal agencies
 - Industry-specific organizations
 - Credit card brands, processors and acquiring banks
 - Credit reporting agencies
 - Media

Once an "Incident" Occurs, What Should the Entity Do Next?

- Coordinate with your breach coach and **crisis communication firm** to manage public relations issues and respond promptly, earnestly and with honesty, utilizing tailored **media statements** and **Frequently Asked Questions (FAQs)**
 - Internal & external communications
- Provide dedicated **call center** support, explaining the steps callers can take to reduce their risk of harm, and monitor **escalated** questions from callers

Once an "Incident" Occurs, What Should the Entity Do Next?

- Offer appropriate remedy to affected individuals
 - Credit monitoring
 - SSN breaches
 - NOT appropriate for credit card breaches
 - Identity theft restoration/repair services
 - Identity theft monitoring
 - Fraud Alerts
 - Security Freezes
- What about Minors? Deceased?

Notification Content Requirements

- Must be written in plain language
- The name and contact information of the reporting organization
- The date of the breach
- The date of discovery of the breach
- A list of the types of PII that were or are reasonably believed to have been the subject of the breach
- Whether notification was delayed as a result of a law enforcement investigation
- A general description of the breach incident
- Toll-free telephone numbers and addresses of the major credit reporting agencies
- Information about what the organization has done to protect individuals whose information has been breached
- Advice on steps that the person whose information has been breached may take to protect himself or herself.

What Do State Regulators Expect?

- Number of state residents affected
- Specific details about incident
- Redacted copy of notification letter sent to affected individuals
- Time of Notification to AGs
 - NY: *at time* of notification to affected individuals
 - NJ: *before* notifications to affected individuals
 - VT: 1st letter - within 14 days of discovery; 2nd letter - at or before time of notification to affected individuals
- Names of residents (in Louisiana)

What Do All Regulators Dislike?

- Unencrypted backup tapes
- Unencrypted portable devices
- Slow incident detection and notification
- Default configurations/passwords
- Absence of appropriate policies
- Insufficient employee training/awareness
- Insufficient sanctions for employee(s) responsible for breach
- Insufficient dedicated security roles
- Failure to address issues identified by risk assessments

Helpful Reminders for Incident Response

- From the first date of discovery of the incident, always keep in mind there is a high likelihood that litigation (single plaintiff and/or class actions) and regulatory investigations will result
 - Avoid the “B” word
 - Pick up the phone! Don’t email.
 - All correspondence directed to counsel



Thank you for your time!


 Chicago Cleveland Columbus Detroit Miami West Palm Beach
 
 ASSOCIATION OF GOVERNMENTAL RISK POOLS 51



James J. Giszczak
248.220.1354
jgiszczak@mcdonaldhopkins.com



Dominic A. Paluzzi
248.220.1356
dpaluzzi@mcdonaldhopkins.com



A business advisory and advocacy law firm®

*Proactive Compliance • Training • Breach Response Workshops
Breach Coaching • Litigation & Class Action • Regulatory Response*



We live data privacy law 24/7.