BakerHostetler

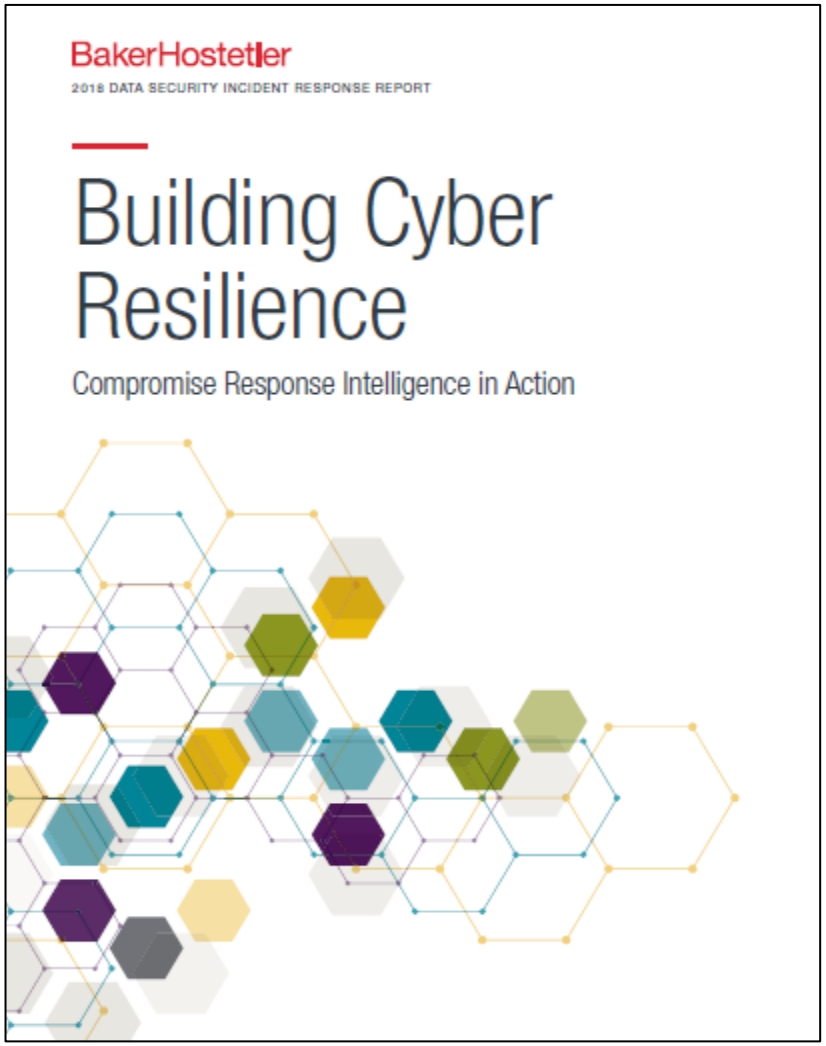
Cybersecurity Preparedness: The Legal Landscape and Incident Response Survival Guide

David M. Brown

Davidmbrown@bakerlaw.com

Blog: www.dataprivacymonitor.com

Introduction



BakerHostetler

- Chambers USA 2018 nationally ranked & Legal 500 ranked Privacy and Data Protection practice
- Privacy and Data Protection "Practice Group of the Year" by Law360 in 2013, 2014 & 2015
- Over 2,000 incidents handled (560+ in 2017 alone)
- Team includes 40+ attorneys focusing in privacy and data security law across the country

Overview & Goals

- Review current data security threats and trends
  - Ransomware, W-2 incidents, business email compromise, etc.
- Provide real-world examples of security incidents and subsequent fallout
- Review the legal landscape and discuss best practices for incident response
- Offer guidance on data security best practices and risk management and prevention

Cyber Risk Landscape

Sony Hackers Used Phishing Emails to Breach Company Networks

YAHOO!

Yahoo hack may become test case for SEC data breach disclosure rules

Neiman Marcus

The New York Times

Neiman Marcus Data Breach Worse Than First Said

Forbes

CSO FROM IDG

Ransomware As A Service Being Offered For $39 On The Dark Net

Phishing attacks targeting W-2 data hit 41 organizations in Q1 2016

Insurance giant Anthem hit by massive data breach

Anthem®

Bloomberg

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

Where are the threats?

Inside threats

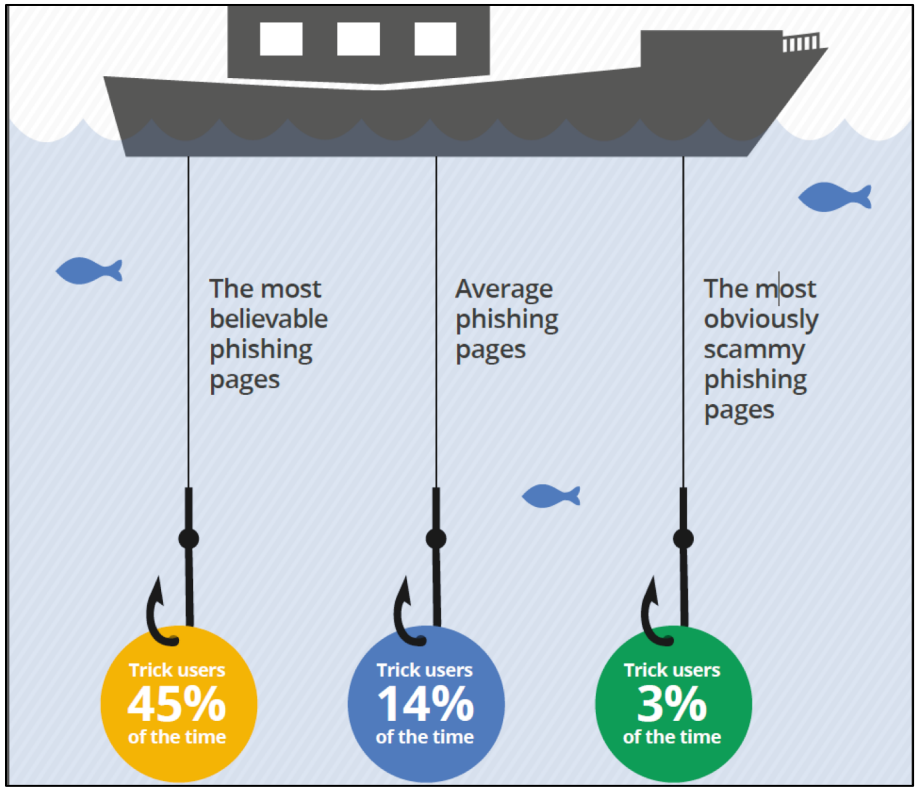
- Employee negligence
  - Security failures
  - Lost mobile devices
- Employee ignorance
  - Improper disposal of personal information (dumpsters)
  - Lack of education and awareness
- Malicious employees

Outside threats

- Hackers/hacktivists
- Malware
  - Phishing and Spear Phishing
  - Ransomware
- Vendors
- State-sponsored attacks

Beware of Phishing Threats

- **Phishing Schemes**
  - W2 / Tax Related
  - Wire Transfer Request
  - Payroll ACH Fraud
  - Credential Stealing



Fast Facts:

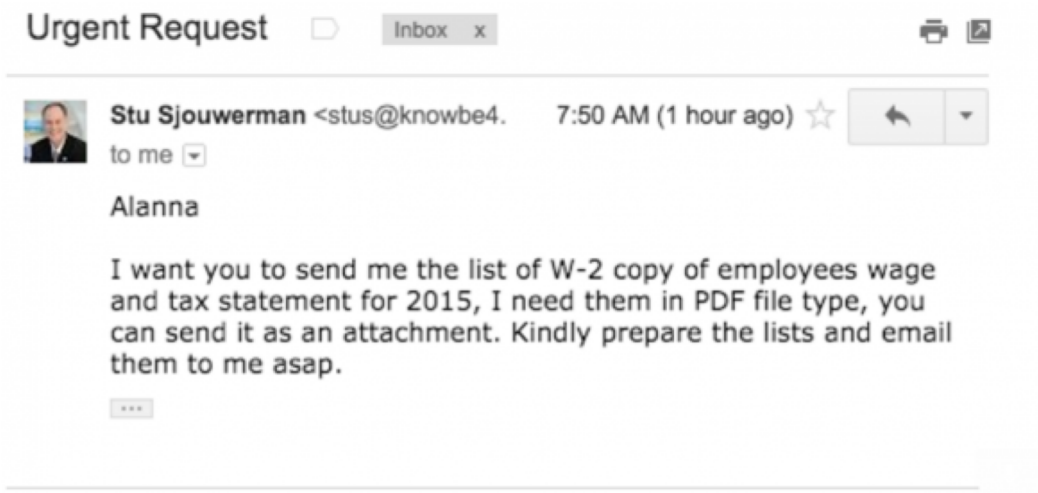
- 20% of hackers access compromised accounts within 30 minutes of obtaining credentials
- Hackers spend on average 3 minutes searching the account for valuable information, such as “wire transfer” and “bank”

Source: Google, *Behind Enemy Lines in our war against account hijackers* (Nov. 2014)

W-2 & wire transfer incidents

- Scammers use emails from a target organization's CEO, asking human resources and accounting departments for employee W-2 information.

- Scammers last year also massively phished online payroll management account credentials used by corporate HR professionals.

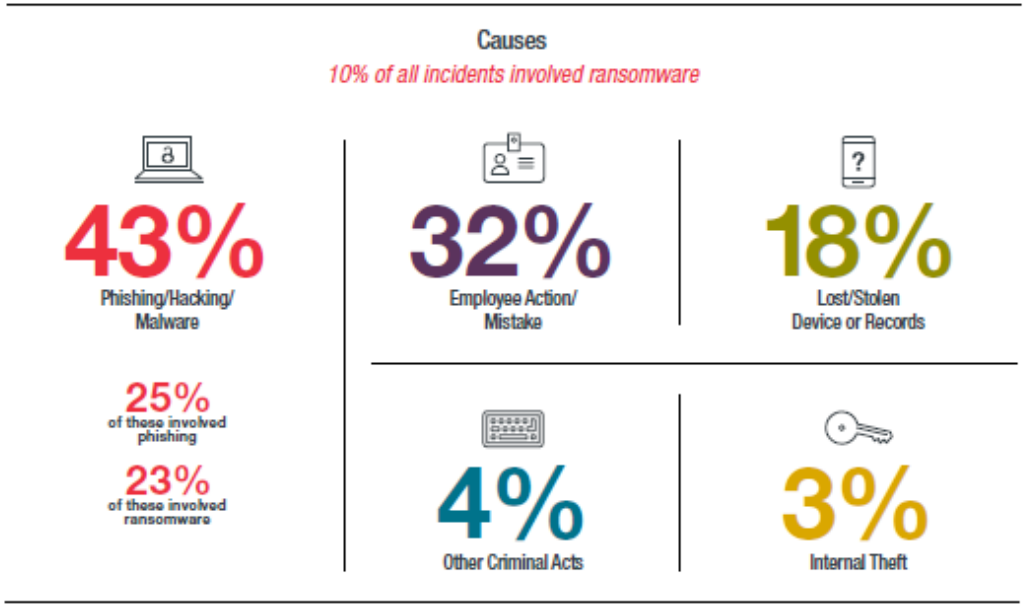


CyberExtortion (Ransomware)

- CyberExtortion can be conducted by:
  - Ransomware.
  - Distributed denial of service (DDoS) attacks.
- Cybercriminals use the ransomware to encrypt target data so that the criminal can extort money from the target institution or person, or use DDoS to shut down the website and deny service from the institution/person until ransom is fulfilled.

Ransomware on the Rise

- On April 29, 2016 - FBI issued a warning that ransomware attacks are on the rise.
- Cyber-criminals collected $209 million in the first three months of 2016 by extorting businesses and institutions to unlock computer servers.



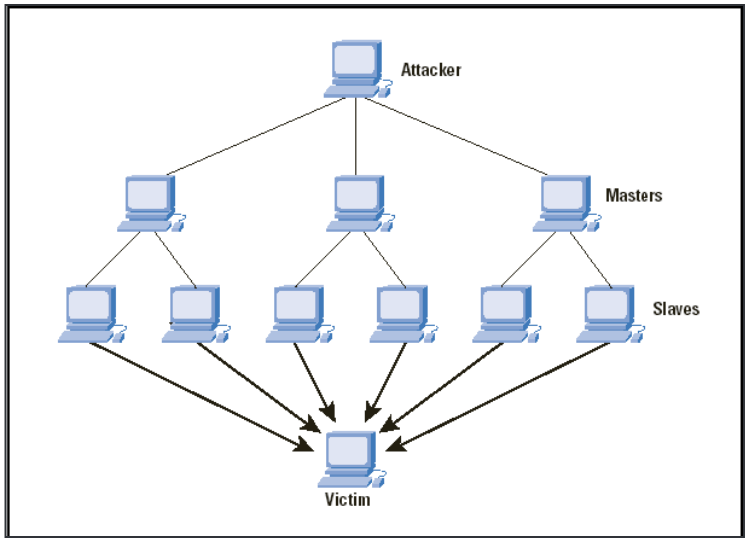
BakerHostetler Data Security Incident Response Report 2017

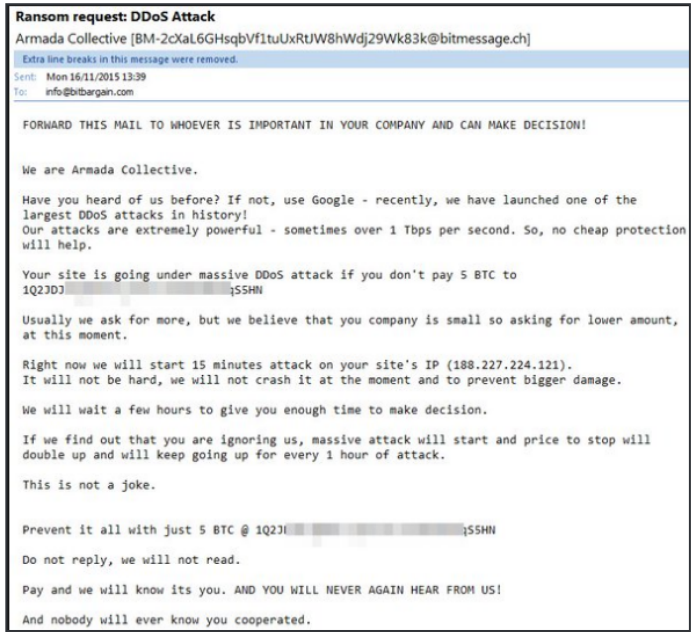
IoT DDOS Attacks

- End of 2016, major internet sites were taken down due to DDOS attack on Dyn, a company responsible for routing internet traffic.

- IoT DDOS attacks utilize multiple infected IoT devices, ranging from personal cameras to medical devices, to carry out attacks that flood a victim's server with legitimate requests thereby overloading the server's capacity and impairing functionality.

- Because open-source software, such as Mirad, is now widely available, IoT DDOS attacks will inevitably increase in 2017 and similar to ransomware will morph into more sophisticated and specialized variants.





Ransom request: DDoS Attack

Armada Collective [BM-2cXaL6GHsqbVf1tuUxRtJW8hWdj29Wk83k@bitmessage.ch]

Extra line breaks in this message were removed.

Sent: Mon 16/11/2015 13:39

To: info@bitbargain.com

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

Have you heard of us before? If not, use Google - recently, we have launched one of the largest DDoS attacks in history!
Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Your site is going under massive DDoS attack if you don't pay 5 BTC to
1Q2JDJ[redacted]iS5HN

Usually we ask for more, but we believe that you company is small so asking for lower amount, at this moment.

Right now we will start 15 minutes attack on your site's IP (188.227.224.121).
It will not be hard, we will not crash it at the moment and to prevent bigger damage.

We will wait a few hours to give you enough time to make decision.

If we find out that you are ignoring us, massive attack will start and price to stop will double up and will keep going up for every 1 hour of attack.

This is not a joke.

Prevent it all with just 5 BTC @ 1Q2JI[redacted]iS5HN

Do not reply, we will not read.

Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

And nobody will ever know you cooperated.

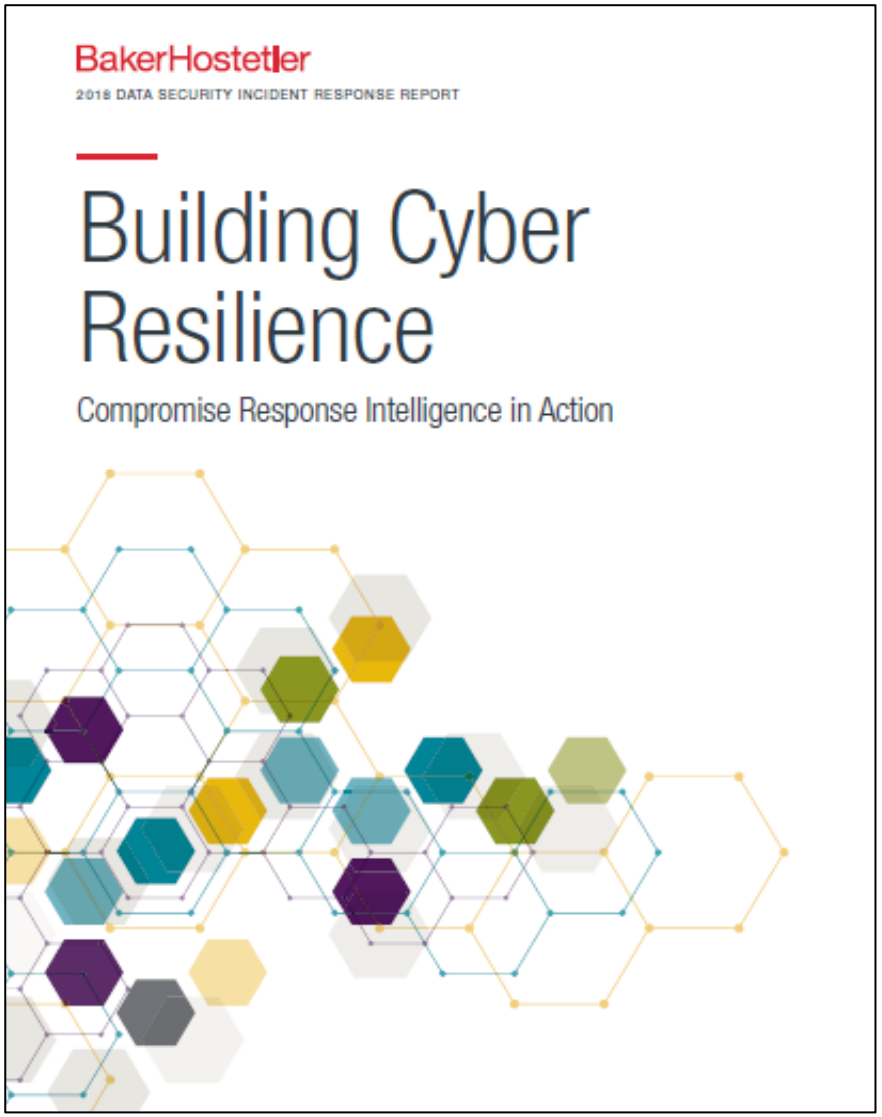
State and Local Governments Are Targets Too

- Hackers targeted Mecklenburg County, NC, with ransomware and demanded $23,000 to unlock the affected data. County officials refused to pay and said it would rebuild the applications from scratch. But hours after that announcement, the hackers struck again.
- The Darkoverlord group targets school districts in Montana and Iowa.
- Other cities and local governments targeted.
- Some states are offering cybersecurity assistance to local governments (e.g., Michigan and Virginia).

State and Local Governments Are Targets Too

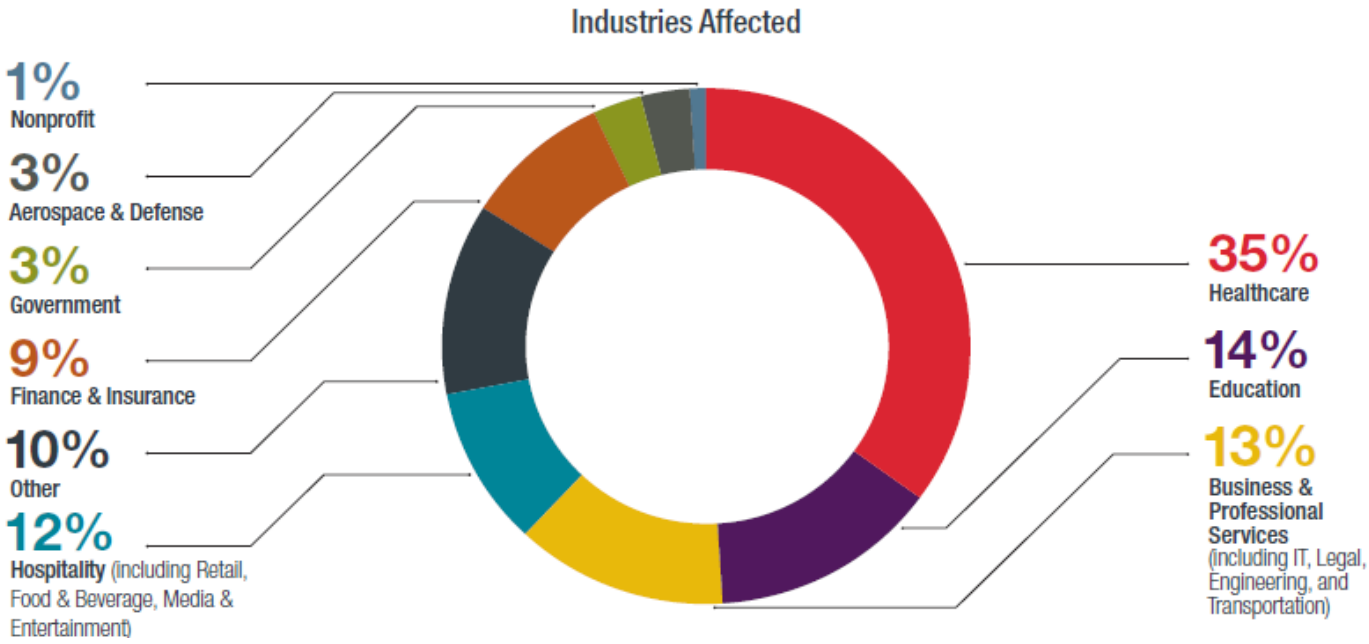
- Atlanta revealed that it had been the victim of a ransomware attack ($50,000 ransom) that took many of the city's services offline for nearly a week, forcing police to revert to taking written case notes, hampering the Atlanta's court system and preventing residents from paying water bills online.
- Atlanta spent $2,667,328 responding.
- The bulk of the expenditures relate to incident response and digital forensics, extra staffing, and Microsoft Cloud infrastructure expertise, presumably all related to clawing back the systems that the hackers had frozen. The city also spent $50,000 on crisis communications services from the firm Edelman, and $600,000 on incident response consulting from Ernst & Young.

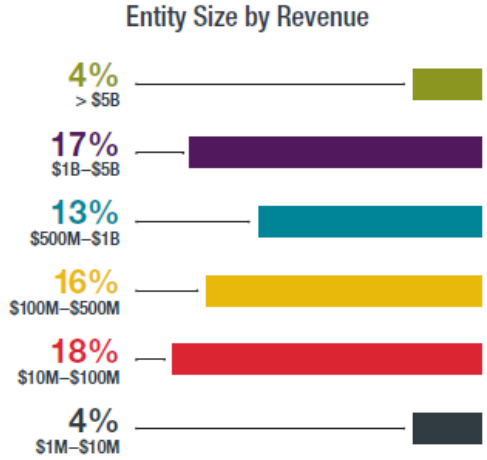
Incident Response Trends



BakerHostetler

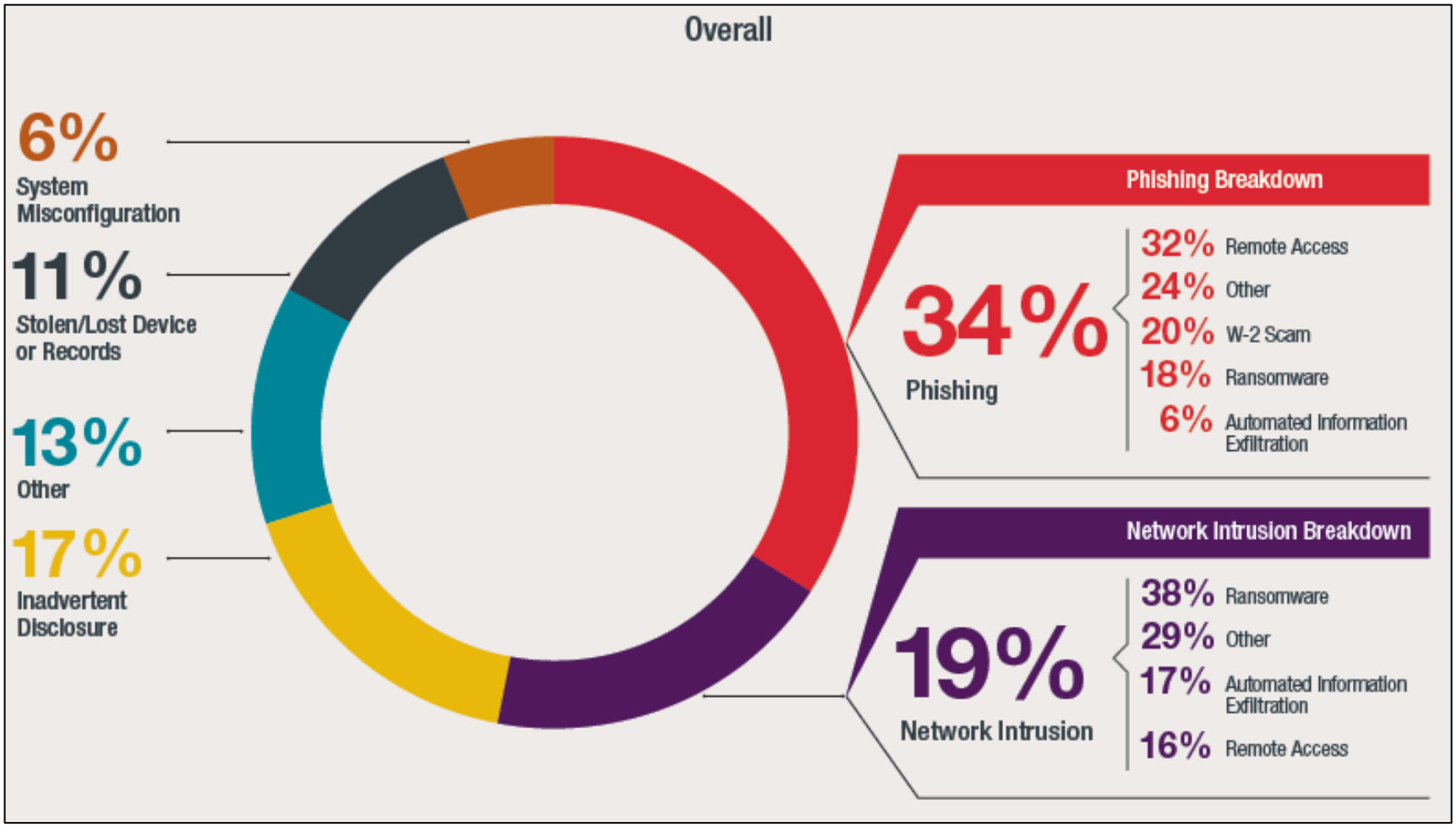
Incident Response Trends





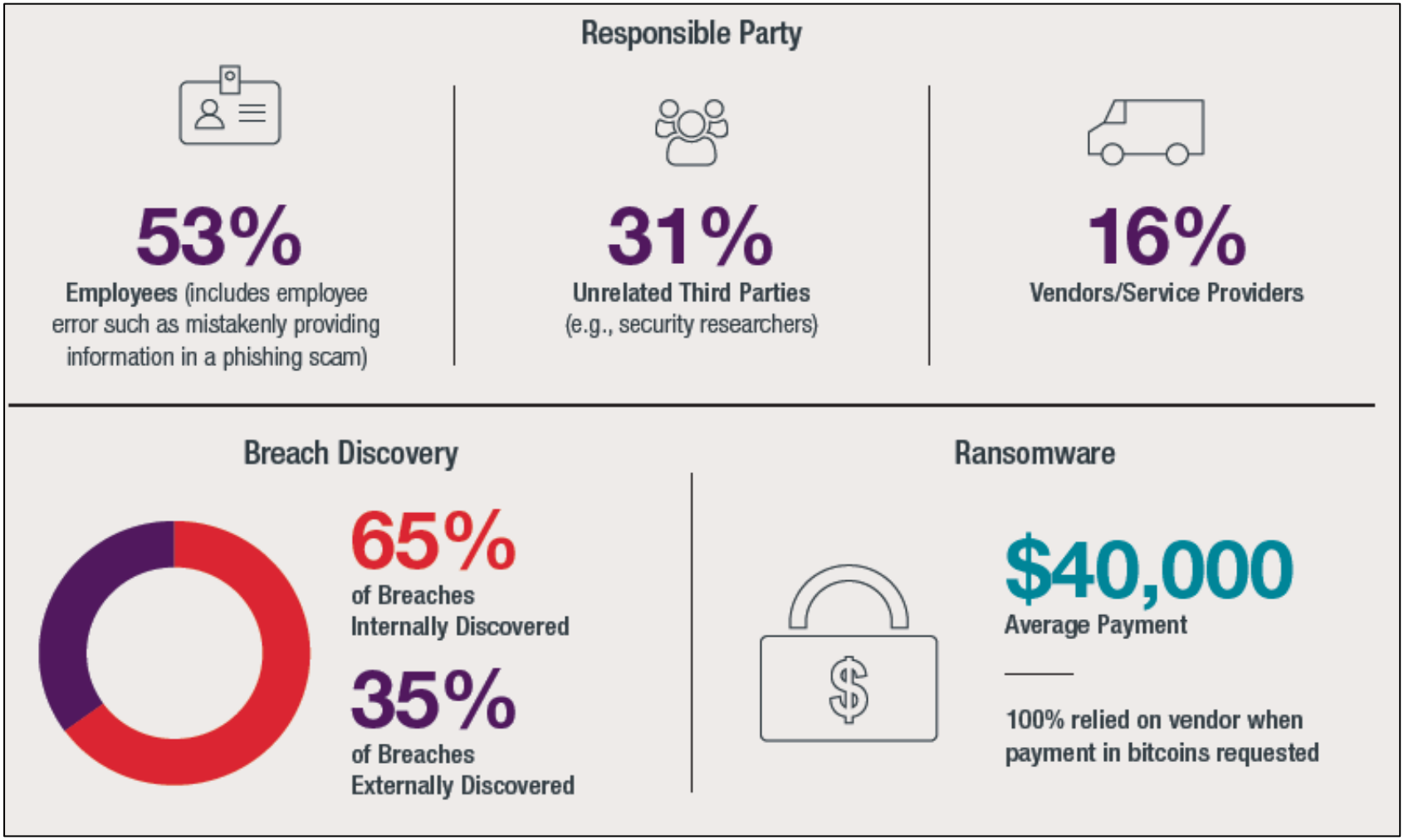
BakerHostetler Data Security Incident Response Report 2018

Why Do Incidents Occur – Most Common Causes



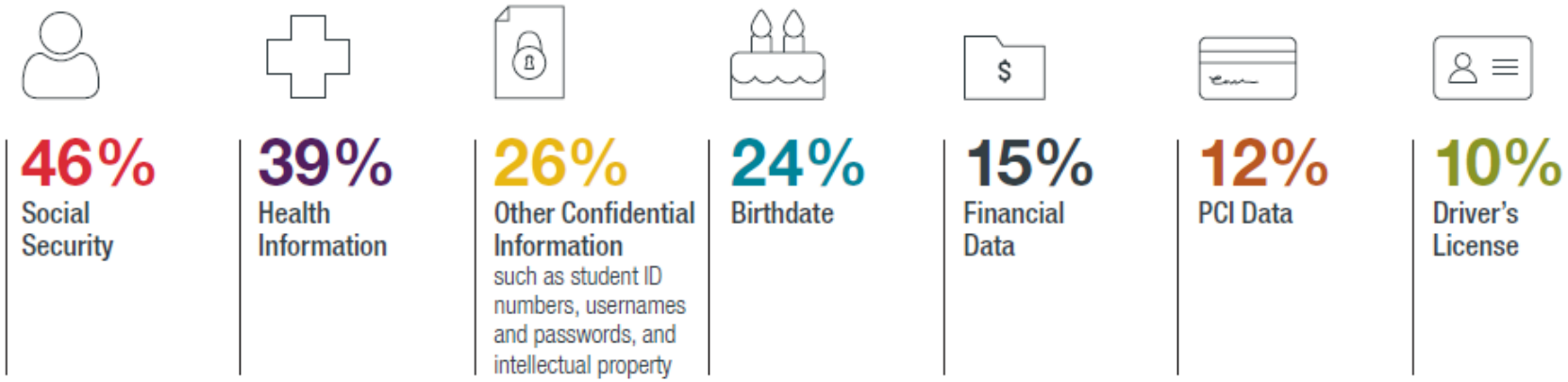
BakerHostetler Data Security Incident Response Report 2018

Incident Response Trends



BakerHostetler Data Security Incident Response Report 2018

Data at risk



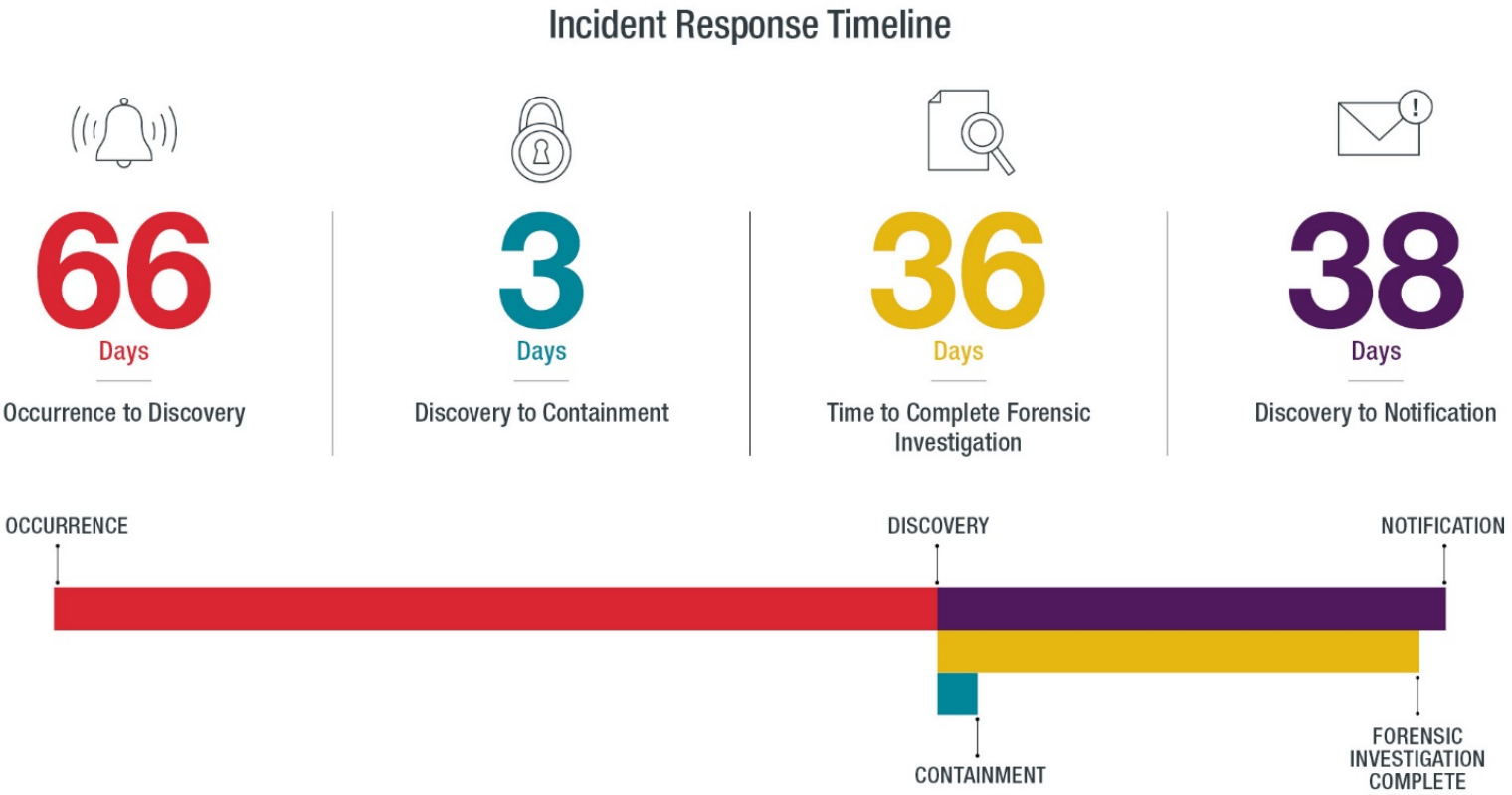
** These amounts total more than 100% because many incidents involved multiple types of data.*

BakerHostetler Data Security Incident Response Report 2018

Incident Response

- **Assess the situation with client**
- **Cyber insurance**
- **Scoping call with forensics team**
- **PR/Crisis Management firm**
- **Set up vendors for call center or mailing services**
- **Forensic report**
- **Credit monitoring decision**
- **Individual notice and regulatory notice**

Detection, Containment, Notification

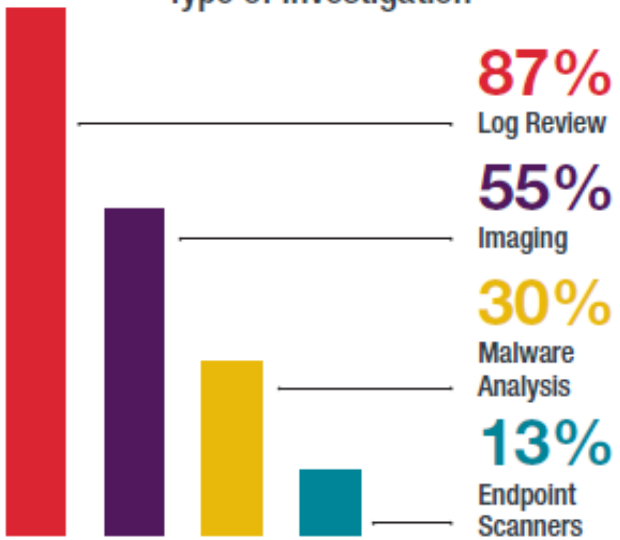


BakerHostetler Data Security Incident Response Report 2018

Responding to Security Incidents is Costly

BakerHostetler

Type of Investigation



Forensic Investigation Costs

$84,417
for All Incidents

$86,751
for Network Intrusion Incidents

$436,938
for 20 Largest Investigations

Use of Outside Forensics

65%
of Network Intrusion Incidents

41.5%
of Data Breach Incidents

36
Days

Average Completion Time for Forensic Investigation

24%
Evidence of Data Exfiltration in Network Intrusion Incidents

BakerHostetler Data Security Incident Response Report 2018

Costs of Responding to a Breach

- Forensics
- Notification costs
- Credit monitoring
- Call center
- Remediation
- Legal fees
- Defense costs/settlement expenses
- PCI fines/assessments & regulatory fines

Regulatory Scrutiny

- Expect Transparency
- Prompt and Thorough Communications
- Containment
- Remediation and Mitigation
- More Scrutiny for “Known” Issues

Incident Response Plan

Employee Training Manual

Policies and Procedures

Forensic Reports

Information on Specific Data Loss Prevention

Information on Use of MFAs

What regulators look for

Be prepared to answer questions regulators may ask:

1. Describe your network environment.
2. Do you have a network diagram?
3. What data do you process or store?
4. What logs do you maintain?
5. Are you preserving the environment, including RAM?
6. Do you have critical third-party vendors?
7. What IT resources do you have?
8. Do you have an incident response plan?
9. How did you detect the intrusion?
10. What have you done so far?

What regulators look for

More questions regulators may ask:

11. Why did it take so long to notify individuals?
12. Are you offering credit monitoring? If so, for how many years?
13. What steps did you take to investigate?
14. Did you exclude anyone from notification?
15. How are you notifying people for whom you don't have addresses?
16. Did you involve law enforcement?
17. If a vendor caused the breach:
    - What does the vendor agreement require?
    - Has the vendor experienced other breaches?
    - Do you audit the vendor?

Regulatory "Hot Buttons"

- Encryption of Portable Devices
- Patching
- Security Awareness and Training
- Two-Factor Authentication for Remote Access
- Ignoring Risk Assessments
- Slow Detection
- Slow Notification
- Repeat Offenders

The Legal Landscape

The Privacy "Patchwork"

- Federal & state laws govern the handling of PII/PHI
  - Laws covering SSNs / disposal of PII
  - Employment-related laws (e.g. FMLA, ADA, GINA)
  - Other federal and state regulations (e.g. FTC Act)
- HIPAA
  - Applies to Covered Entities and Business Associates
  - Preempts except where state law is "more stringent"
- State breach notification laws
- State medical information breach reporting laws
- International data protection regulations

State Laws

- 50 states, D.C., & U.S. territories
- Laws vary between jurisdictions
- Varying levels of enforcement by state attorneys general
- Limited precedent
  - What does “access” mean?
  - What is a reasonable notice time?

Montana Breach Notice & Data Protection Statutes

- **Breach of security** is the "unauthorized acquisition of **computerized data** that: (a) materially compromises the security, confidentiality, or integrity of the personal information maintained by a state agency or by a third party on behalf of a state agency; and (b) causes or is reasonably believed to cause loss or injury to a person."
- **Notice to individuals**: Upon discovery or notification of a breach of the security of a data system, a state agency that maintains computerized data containing personal information in the data system shall make reasonable efforts to notify any person whose unencrypted personal information was or is reasonably believed to have been ***acquired*** by an unauthorized person.
- **Personal information** is a first name or first initial and last name in combination with any one or more
- of the following data elements when the name and data elements are not encrypted:

  - (A) social security number;
  - (B) driver's license number, state identification card number, or tribal identification card number;
  - (C) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
  - (D) medical record information;
  - (E) a taxpayer identification number; or
  - (F) an identity protection personal identification number issued by the United States internal revenue service.

- **Notice** notification must be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.
- If notice is required, also notify the **state's CIO** and to the **state AG**.
- All state agencies and third parties to whom personal information is disclosed by a state agency shall **develop and maintain**: (a) an information security policy designed to safeguard personal information; and (b) breach notification procedures.

Montana – guidance on protection of personal information (MCA 2-6-1502)

- Each state agency that maintains the personal information of an individual shall develop procedures to protect the personal information while enabling the state agency to use the personal information as necessary for the performance of its duties under federal or state law.

- The procedures must include measures to:
  - (a) eliminate the unnecessary use of personal information;
  - (b) identify the person or state agency authorized to have access to personal information;
  - (c) restrict access to personal information by unauthorized persons or state agencies;
  - (d) identify circumstances in which redaction of personal information is appropriate;
  - (e) dispose of documents that contain personal information in a manner consistent with other record retention requirements applicable to the state agency;
  - (f) eliminate the unnecessary storage of personal information on portable devices; and
  - (g) protect data containing personal information if that data is on a portable device.

The Notification Process

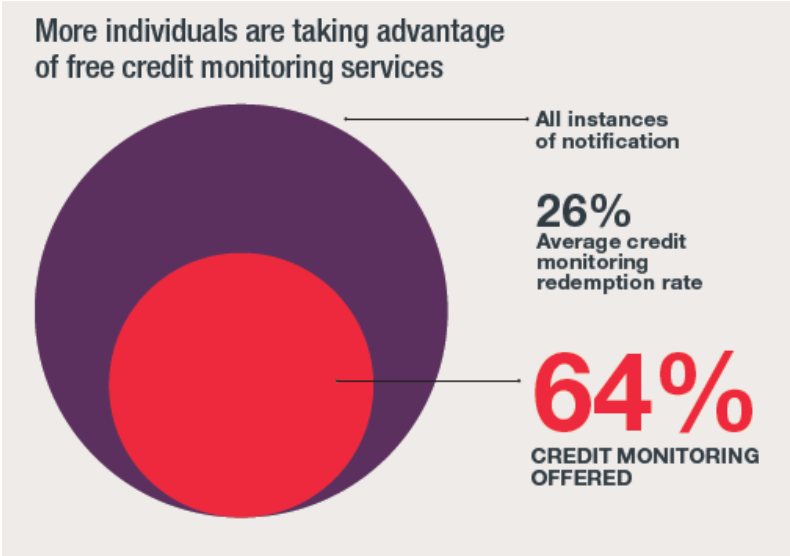
Who needs to be notified?

- Employees/Residents
- Government Agencies
- Attorney General/CIO
- Law Enforcement
  - FBI
  - Secret Service
  - Local Police
- Credit Reporting Agencies (CRAs)

Offer of Credit Monitoring?

Why Offer

- To mitigate harm
- Affected individuals' expectations
- Regulators' expectations



Why Not to Offer

- Does not prevent fraudulent charges on payment cards
- May impact litigation position
- Low redemption rate

BakerHostetler Data Security Incident Response Report 2017

The Importance of Messaging

Messaging Goals and Risks

Goals

- Comply with all applicable laws and regulations.
- Be thorough and descriptive without causing unnecessary concern.
- Provide reassurance without overpromising.
- Strive for openness and transparency without creating unnecessary risk.

Risks

- Complaints
- Negligence, Invasion of Privacy Lawsuits
- Class Action Lawsuits
- Regulatory Action
- Damage to Trust

Using the Word “Breach”

- "Breach" has legal significance
- "Breach" suggests something bad happened or is going to happen
- Use “Breach" too frequently and individuals or regulators may think you are subject to numerous breaches
- *“Incident”?*
- *“Event”?*

Communications Strategy

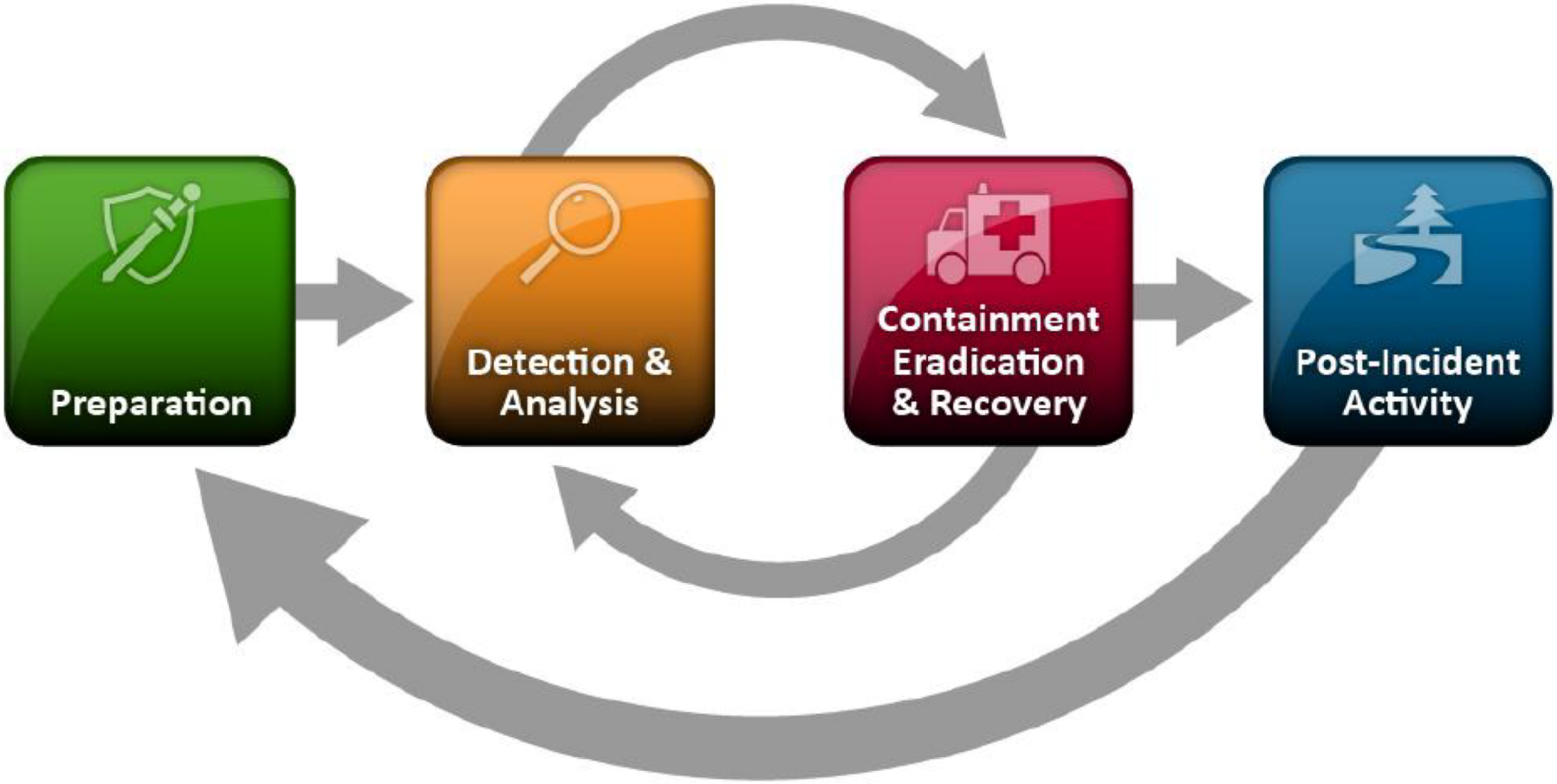
Speaking too soon and on the fly

- Dec. 20, 2013: Initial notice indicated that the breach affected card data (no PINs) of 40 million
- Dec. 27, 2013: PIN numbers captured
- Jan. 10, 2014: Personal information of 70 million customers taken

Communication Don'ts

- Speak too early and on the fly
- Use a misleading initial holding statement
- Fall victim to saying too much, being too reassuring
- Make logistical mistakes (e.g., call center)
- Assume you have to answer all media inquiries
- Over-apologize
- Leave out helpful evidence
- Call yourself a victim
- Overstate the security measures you had in place
- Overstate new security measures
- Ignore regulators

Developing an Effective Incident Response Plan ("IRP")



Source: NIST 800-61, Incident Response

Incident Response Team

- The Incident Response Team (IRT) manages and coordinates the event investigation, response, reporting and corrective action activities
- The IRT should be activated upon learning of an event
- The IRT should be authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident

Incident Response Team Members

- IRT leader/coordinator
- Privacy officer
- Legal
- Risk management
- Others as appropriate
  - IT/Information security
  - HR, employee relations
  - Public relations
  - Fulfillment vendor
  - Insurer/Broker
  - Outside legal counsel
  - Crisis management firm

Team Leader

- **IRT Leader**: may be any qualified senior-level individual
- Team leader's responsibilities include:
  - Implementing the response plan, overseeing all response and recovery activities
  - Providing guidance and assistance in determining the appropriate action taken
  - Developing a timeline for compliance with any notification requirements under federal or state law (e.g., 60 days under HIPAA)
  - Updating the appropriate officers of incident investigation findings (Information Security Officer? Director of Privacy & Compliance?)
  - Specifying the "Threat Level" of an incident, and updating the threat level as needed

Incident Response Team Training

- Explain Incident Response Plan
- Discuss each role and the responsibilities associated with that role
- Establish/explain the IRT's internal communications plan security events
  - Think group communication (e.g. email distribution lists, conference calls)
  - Avoid ad hoc communications among members by telephone, SMS text, email
- Conduct tabletop breach response exercises

Post-Event IRT Review

- Review all events with incident response team
  - IRT's internal communications plan, ID problems & correct
  - Review information security systems, policies and procedures, workflows
  - Review physical security systems, policies and procedures, workflows
  - Update training program accordingly
- Update incident response plan

Risk Management & Prevention

Prevention = Protection

- Vendor Management
- Security Awareness/Education
- Basic Data Security Good Practices
- Risk Assessment
- Policies and Procedures
- Consistent Enforcement of Policies and Procedures
- Practice breach response initiative
- Delete data when no longer needed

Basic Data Security Best Practices

- Data identification & classification
- Data hygiene (don't collect what you don't need)
- Access restrictions
  - Is there a need for this employee to handle PII?
  - Backups and Network mapping
- Education
  - Does the workforce know how to identify and safeguard personal information?
  - Does workforce understand the importance of data security compliance?
- Document retention/destruction

Security Awareness and Education

Initial training at time of hiring

- How do employees spot security problems?
- What is the reporting procedure?
- Are leaders trained to handle reports from staff?

Regular and continued training and awareness

- What does your training program include for security issues and procedures? Annual?
- Formal online training course vs. in-person?
- Monthly staff meetings?
- Newsletters?

Risk Assessment

- Periodic Review of Administrative Safeguards
- Periodic Review of Physical Safeguards
- Periodic Review of Technical Safeguards
- Periodic Review of Data Flows – has the quantity/nature/sensitivity of the data changed?

Policies & Procedures

- **Security Incident Response Plan**
- **BYOD Policy and Social Media Policy**
- **Information Security and User Policies**
  - What users can and must do to use network and organization's computer equipment
  - Define limitations on users to keep the network secure (password policies, use of proprietary information, internet usage, system use, remote access)
- **IT Policies**
  - Virus incident and security incident
  - Logs
  - Backup policies
  - Server configuration, patch update, modification policies
  - Firewall policies
  - Wireless, VPN, router, and switch security
  - Email retention

Policies & Procedures (cont.)

- General Policies
  - Program Policy
  - Crisis Management Plan
  - Disaster Recovery
    - Server Recovery
    - Data Recovery
    - End-user Recovery
    - Phone System Recovery
    - Emergency Response Plan
    - Workplace Recovery

Be “Compromise Ready”

- Threat information gathering
- Technology – preventative & detective
- Personnel – awareness & training
- Security assessments
  - Understand where assets and sensitive data are located
  - Implement reasonable safeguards
  - Increase detection capabilities
- Vendor management
- Incident response plan and tabletop exercises
- Insurance
- Ongoing diligence and oversight

Questions

- David M. Brown
- Davidmbrown@bakerlaw.com

BakerHostetler

Atlanta
Chicago
Cincinnati
Cleveland
Columbus
Costa Mesa
Denver
Houston
Los Angeles
New York
Orlando
Philadelphia
Seattle
Washington, DC

www.bakerlaw.com