Privacy Breach
A Guide to Incident Response

February 11, 2016
Companies in the United States experience an annual loss of more than $525 million due to cyber crime.

<table>
<thead>
<tr>
<th>Event</th>
<th>Annual Losses (in Millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire</td>
<td>$2,600</td>
</tr>
<tr>
<td>Cyber Crime</td>
<td>$525</td>
</tr>
<tr>
<td>Tornadoes</td>
<td>$400</td>
</tr>
<tr>
<td>Securities Lawsuits</td>
<td>$182</td>
</tr>
</tbody>
</table>
Cyber crime can be divided into two categories: the first comprises direct attacks on computer systems; the second focuses on using computer systems as a tool or mechanism to perform criminal acts.

### Direct Attack
- Denial of Service Attack
- Hacktivism
- Malicious Code

### Tool to Criminal Act
- Social Engineering
- Cyber Bullying and Slander
- Copyright Infringement

Direct attacks can result in a general security incident or a data breach.

### Security Incident
- Property Destruction
- Theft of Money

### Data Breach
- Theft of Data
- Loss of Data (Employee Error)
Anatomy of a Data Breach

- Customers
- Regulators
- Shareholders
- Media
- Attorney General/Law Enforcement

DATA BREACHED
Anatomy of a Data Breach – Claims by the Numbers

- Median claim payout = $144,000; average claim payout = $733,109
- Median cost per record = $20; average cost per record = $956
- Median cost per breach response expense = $110,594; average cost for breach response services = $366,484
- Median cost for legal defense = $283,300; average cost for legal defense = $698,797
- Median cost for legal settlement = $150,000; average cost for legal settlement = $588,520
- Median number of records lost = 3,500; average number of records lost was 2.4 million
- Personally Identifiable Information was the most frequently exposed data
- Hackers were the most frequent cause of data loss, followed by employee mistakes
- Insiders were involved in 32% of claims submitted

Source: NetDiligence 2014 Claims Study
Survey of 2013 claims filed with major cyber insurers across all industries
Incident Response Planning

Before the Crisis Occurs

Establish the Inside Response Team
- Identify the individuals that would be key in managing a data breach at your bank and engage them in developing your breach response plan.
## Incident Response Planning

### Before the Crisis Occurs

**Establish the Outside Response Team**

- Identify your expertise gaps within your Inside Team and search for qualified parties to fill them.
- Negotiate rates where possible.
- Determine if you need or want a Breach Coach.

<table>
<thead>
<tr>
<th>Forensic Expert</th>
<th>Privacy Lawyer</th>
<th>Public Relations Firm</th>
<th>Notification Mailers</th>
<th>Breach Coach</th>
</tr>
</thead>
</table>


In the wake of an actual or suspected breach, a Breach Coach will establish a triage process designed to immediately curtail exposure. Actions may include:

- Evaluating exposed information and determining whether forensic assistance is needed.
- Supervising forensic investigations by working with both the bank and outside forensic experts to prioritize the investigation so that the forensic results are delivered in such a manner so as to enable the client to meet its statutory, regulatory, or contractual reporting requirements.
- Analyzing the exposed information and determining which notification laws are triggered.
- Preparing notification letters.
- Coordinating with call center/notification vendors.
- Identifying and recommending appropriate service offerings for the breached population.
- Developing and deploying public relations strategies.
- Engaging with law enforcement.
- Identifying and assisting with appropriate remedial measures.
- Defending the bank in regulatory investigations.
Incident Response Planning

Benefits of a Breach Coach?

- Experience
- Attorney-Client Privilege
- Quarterback
- Relationships
Incident Response Planning

Evaluate Your Digital Assets

- Focus on what data a company has and what data is important to protect.
- Considerations should include the risk, vulnerability and consequence of exposed data.

- What data might hackers be interested in?
- How is such data safeguarded?
- How will you know if the data has been exposed?
- Who will be impacted by the loss or unauthorized access of the data?
Phase 1 – Incident Discovery

- Prepare to document everything (for Forensics, FBI, and Funds)
  - Document all known facts about the breach including who discovered it, when it was discovered, the type of breach, the type of data stolen, the type of devices impacted, etc. Include interviews of all those involved in the discovery

- Establish methods of communications for your Inside and Outside Response Team

- Contact your breach coach

- Notify law enforcement

- Don’t forget your insurance carrier
Phase 2 – Remediation

*Bring on the Forensic Team*

Goal: Secure the premises to stop additional data loss and preserve evidence

- Delete inserted malware and hacking tools
- Identify and address other security gaps
- Replace infected machines
- Interview those involved
- Document how the breach was contained and remediated
- Identify the extent and type of data compromised
- Determine if more in-depth investigations are required
Incident Response Planning

Developing the Plan

Phase 3 – Resolution

Next up: the Legal Team (Privacy Law and General Counsel)

Goal: Understand and act upon your obligations under common and statutory law

- Determine which parties need to be notified of exposed data
- Provide direction, or draft the content of notifications. Privacy laws vary widely by state and some states have very specific language requirements that will need to be followed.
- Provide direction as to the timeframes required for such notifications. In some cases, sixty days may be all you have by law to get the notices out the door.
- Assess potential claims against culpable third parties.
- Manage related litigation and regulatory defense for the bank.
Phase 3 – Resolution, continued

On Deck: the Full Team

Goal: Reputation restoration

- Determine the necessity and value of providing credit and identity monitoring services for impacted individuals
- Determine the necessity of employing a public relations firm
- Begin the notification process
- Establish a procedure to response to manage customer and press inquiries
- Evaluate shareholder exposure and develop response
## Incident Response Planning

### Documentation and Execution

Communicate and test the plan!
Breach Response Expense coverage is part of a liability insurance policy that covers the costs incurred to remediate a system breach.

Covers

- Reasonable and necessary expenses incurred in connection with a data breach including:
  - Forensic investigations, privacy attorney consultations, costs of issuing notifications, credit/identity monitoring services, and public relations expenses.
- Does not cover costs to remediate (patches, new software/equipment).
- Coverage may include access to an experienced Breach Coach. But you probably want one who uses an attorney with attorney-client privilege.
Thanks for your participation.

Contact information:

lmicciche@abais.com
216-220-1297

Visit abais.com
**IMMEDIATE ACTION ITEMS**

- Secure premises to stop additional data loss, and preserve evidence.
- Engaging a forensics expert or additional IT expertise may be necessary.
- Activate your Inside and Outside Response Teams and promptly investigate the incident.
- Limit access into affected areas, as necessary, and take steps to promptly investigate the incident.
- Determine steps necessary to eliminate system weaknesses and patch vulnerabilities, if any, then notify law enforcement.
- Determine what parties, if any, must be notified of exposed data.
- Determine if credit and similar monitoring services are necessary to provide to the affected parties.
- In consultation with counsel or data breach coach.

**DOCUMENTATION CHECKLIST**

- Document all known facts.
- Engage your internal audit department or outside forensic experts to determine if additional data loss, and preserve evidence.
- Secure premises to stop additional data loss, and preserve evidence.
- Document breach containment and remediation.
- Request internal measures.
- Identify and address security gaps.
- Document and address security gaps.
- Analyze the extent and type of data compromised and who is affected.
- Notify the data breach.

**DATA BREACH COACH/LEGAL COUNSEL CHECKLIST**

- Consult your data breach coach and/or legal counsel on notifying law enforcement and regulators. Notify as required.
- Contact your insurance agent/company to ensure timely notification of circumstances which may lead to a claim.

**IT AND FORENSICS EXPERTS CHECKLIST**

- Manage related litigation and regulatory defense for the bank.
- Assist counsel and address security gaps.
- Provide direction on developing timelines required for notifications. In some cases, only up to 60 days is allowed by regulations that must be followed.
- Provide direction on developing timelines required for notifications. Privacy laws vary by state. Some states have specific language.
- Determine what parties, if any, must be notified of exposed data.
- Determine what parties, if any, must be notified of exposed data.
- Engage outside auditors, if applicable.
- Analyze possible legal implications of the breach.
- Determine additional legal implications of the breach.
- Provide direction or develop content for notifications. Privacy laws vary by state. Some states have specific language.
- Provide direction or develop content for notifications. Privacy laws vary by state. Some states have specific language.
- Assess potential claims against culpable third parties.
- Manage related litigation and regulatory defense for the bank.
- Manage related litigation and regulatory defense for the bank.
- Manage related litigation and regulatory defense for the bank.
- Manage related litigation and regulatory defense for the bank.

**COMPANY ACTION ITEMS**

- In consultation with counsel or data breach coach.
- Determine if credit and similar monitoring services are necessary to provide to the affected parties.
- Determine if credit and similar monitoring services are necessary to provide to the affected parties.
- Determine if credit and similar monitoring services are necessary to provide to the affected parties.
- Determine if credit and similar monitoring services are necessary to provide to the affected parties.

**REMEDIATION AND RESOLUTION**

- Circumstances which may lead to a claim.
- Consult your insurance agent/company to ensure timely notification of circumstances which may lead to a claim.
- Contact your insurance agent/company to ensure timely notification of circumstances which may lead to a claim.
- In consultation with counsel or data breach coach.
- Determine if credit and similar monitoring services are necessary to provide to the affected parties.
- Document breach containment and remediation.
- Request internal measures.
- Identify and address security gaps.
- Document and address security gaps.
- Analyze the extent and type of data compromised and who is affected.
- Notify the data breach.

**INCIDENT RESPONSE PLAN**

**ENHANCE BREACH RESPONSE PLAN**

**STEPS TO CONSIDER AFTER A BREACH**

- Document all known facts.
- Engage your internal audit department or outside forensic experts to determine if additional data loss, and preserve evidence.
- Secure premises to stop additional data loss, and preserve evidence.
- Document breach containment and remediation.
- Request internal measures.
- Identify and address security gaps.
- Document and address security gaps.
- Analyze the extent and type of data compromised and who is affected.
- Notify the data breach.

- Circumstances which may lead to a claim.
- Consult your insurance agent/company to ensure timely notification of circumstances which may lead to a claim.
- Contact your insurance agent/company to ensure timely notification of circumstances which may lead to a claim.
- In consultation with counsel or data breach coach.
- Determine if credit and similar monitoring services are necessary to provide to the affected parties.
- Document breach containment and remediation.
- Request internal measures.
- Identify and address security gaps.
- Document and address security gaps.
- Analyze the extent and type of data compromised and who is affected.
- Notify the data breach.