CYBER READINESS FOR FINANCIAL INSTITUTIONS

Are You Prepared for Your Eventual Cyber Breach?

April 15, 2015
Section one

STRENGTHENING CYBER RISK MANAGEMENT

Earl Crane, PhD, CISSP
ecrane@promontory.com
www.linkedin.com/in/earlcrane
How We Got Here

- By relying on crisis response, rather than front-end prevention investments
- As a result of ambiguous lines of authority and accountability
- Using risk management frameworks that do not capture the full range of cyber risks

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Sector Attacks (2012-2014)</td>
<td>Financial, Retail, Entertainment and other sector attacks with increasingly public profile and impact</td>
</tr>
<tr>
<td>Heightened Expectations (Today)</td>
<td>“Good enough” to meet expectations and combat threats several years ago are no longer sufficient</td>
</tr>
</tbody>
</table>
Heightened Expectations: Information Security

Processes good enough to meet expectations several years ago are no longer sufficient

- Changes in examination policies and expectations have rendered former best practices insufficient
- Increased threats require new practices and resources be dedicated to strengthen cyber risk management
- Customer expectations for companies are increasing due to public cyber risk events

**FRB**

“The Federal Reserve requires the financial institutions it regulates to develop and maintain effective information security programs that are tailored to the complexity of each institution's operations and that include steps to protect the security and confidentiality of customer information.”
– Governor Tarullo, February 6, 2014

**SEC**

“Corporate boards that ignore cybersecurity "do so at their own peril." A board's failure to manage cyber risks could create a threat of litigation against a company or lead shareholder groups to advocate the ouster of board members.”
– Commissioner Aguilar, June 10, 2014

**OCC**

“We expect the board and management to ensure that appropriate risk management practices are in place, that clear accountability for day-to-day management of these relationships is established, and that independent reviews of these relationships will be conducted periodically.”
– Comptroller Curry, April 16, 2014

**CFTC**

“[Cybersecurity] is perhaps the single most important new risk to financial stability, and it is an area we are very focused on... We require clearinghouses, exchanges, and other market infrastructures to implement safeguards, and we are focusing on this issue in our examinations. Among other things, we want to make sure the board of directors and top management are making this a priority.”
– Chairman Massad, January 21, 2015
Where do We Start?

- For risk managers, the very first place to start is to reduce the impact of a cyber-event.
- Reducing the impact of a breach begins with better cybersecurity hygiene.
- Multiple resources to help improve cyber hygiene:
  - NIST Voluntary Cybersecurity Framework
  - Center for Internet Security Cyber Hygiene Campaign
  - Council for Cybersecurity Top 20 Controls
What do I do while Strengthening my Cyber Risk Management?

- A mature cyber risk management program takes time to build, but the risks and impact is real today

- Use risk management controls like cyber insurance to transfer risk and fill in the gaps that your cyber risk management can not or will never meet

  - Caution to consider cyber insurance as a risk transfer component of your cyber risk response, appetite, threat mitigation, regulatory requirements, and resources
Steps to Mitigate Cyber Impact

Steps to take to improve cyber hygiene and mitigate impact from breach:

- Strengthen cyber hygiene (1) can help reduce impact of a cyber breach (2)
- Strengthen cyber risk management (3) to sustain better hygiene (1)
- Stronger cyber risk management (3) reduces cyber impact (2)
- Supplement weak cyber risk management (3) with cyber risk transfer (4)
Where do We Start?

- Stronger cyber hygiene can reduce the impact of an incident, but change doesn’t happen overnight, and the change must be sustained.

- The second part of this challenge is to sustain strong cyber risk management.

- Promontory’s six principles of a cyber risk management program:
  1. Cyber Risk Culture
  2. Cyber Risk Management Appetite
  3. Cyber Threats
  4. Cyber Risk Reporting
  5. Cyber Resources
  6. Cyber Response
# What Level of Threats Are Targeting Your Organization?

<table>
<thead>
<tr>
<th>Tier</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Script Kiddies</td>
<td>Practitioners who rely on others to develop the malicious code, use known exploits.</td>
</tr>
<tr>
<td>II</td>
<td>Amateurs</td>
<td>Practitioners with a greater depth of experience, with the ability to develop their own tools (from publically known vulnerabilities).</td>
</tr>
<tr>
<td>III</td>
<td>Hackers</td>
<td>Practitioners who focus on the discovery and use of unknown malicious code, target corporate executives and key government and industry officials to sell the information.</td>
</tr>
<tr>
<td>IV</td>
<td>Criminals</td>
<td>Criminal or state actors who are organized, highly technical, proficient, well funded professionals working in teams to discover new vulnerabilities and develop exploits.</td>
</tr>
<tr>
<td>V</td>
<td>Professional</td>
<td>State actors who create vulnerabilities through active programs to “influence” or impact commercial products during design, development or manufacturing.</td>
</tr>
<tr>
<td>VI</td>
<td>Elite</td>
<td>States with the ability to successfully execute full spectrum cyber operations to achieve a specific outcome in political, military, economic, etc. domains and apply at scale.</td>
</tr>
</tbody>
</table>
Cyber Risk Management Reporting

**Current State**
- **Data**: Put risk data into context to inform management decisions but does not incorporate any further insight.
- **Information**: Define risk tolerance but does not communicate its risk appetite across business units.

**Desired State**
- **Knowledge**: Execute information security knowledge-based decisions by communicating potential risk impact across business units more effectively.

**Long Term Goal**
- **Wisdom**: Information Security Wisdom incorporates risk decisions with business units and operational risk.
# How do I Strengthen my Cyber Risk Management?

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I Cyber Risk Culture</td>
<td>Set the tone from the top</td>
</tr>
<tr>
<td>II Cyber Risk Management Appetite</td>
<td>Information security must be embodied by the organization. Information security is a journey not a destination.</td>
</tr>
<tr>
<td>III Cyber Threats</td>
<td>Respond as adversaries continue to raise the bar. Integration is key.</td>
</tr>
<tr>
<td>IV Cyber Risk Reporting</td>
<td>An information security program is not built on compliance.</td>
</tr>
<tr>
<td>V Cyber Resources</td>
<td>Significant changes are required. Develop in-house information security professionals.</td>
</tr>
<tr>
<td>VI Cyber Response</td>
<td>Expect a breach, and work backwards.</td>
</tr>
</tbody>
</table>
## How do I strengthen my cyber risk management?

<table>
<thead>
<tr>
<th></th>
<th>Cyber Risk Culture</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td></td>
<td>Set the tone from the top</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Cyber Risk Mgmt. Appetite</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>II</td>
<td></td>
<td>Information security must be embodied by the organization.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Cyber Threats</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>III</td>
<td></td>
<td>Information security is a journey not a destination.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Cyber Risk Reporting</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IV</td>
<td></td>
<td>Respond as adversaries continue to raise the bar.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Cyber Resources</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>V</td>
<td></td>
<td>Integration is key.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Cyber Response</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VI</td>
<td></td>
<td>An information security program is not built on compliance.</td>
</tr>
</tbody>
</table>

|   |   | Significant changes are required. | A bank’s infrastructure, third party engagement, culture of trust, monitoring, and organizational structure will need enhancement to integrate information security. |

|   |   | Develop in-house information security professionals. | A bank should consider developing an information security career track. Security controls must be rigorous enough to ensure consistent information system security capabilities across all organizational systems (corporate and third party). |

|   |   | Expect a breach, and work backwards. | There are two types of organizations, those who have been breached, and those who have but don’t yet know it. |
Questions?
Section two

DATA BREACH RESPONSE

Michael L. Yaeger
Schulte Roth & Zabel
+1 212.756.2290 | michael.yaeger@srz.com
Overview

- First steps
- Evidence preservation and collection
- Reporting
- Working with law enforcement
Communications

- Set up a secure channel to email
- Dig out emergency phone list (paper)
Privilege

- This is an investigation done at the urging of the company’s lawyer
What happened when

What the decision-making process was

What happened next:

- Screenshots, pen and paper notebooks, collaborative software tools, etc.

- Showing that the ultimate solution wasn’t the only reasonable assumption
Preserve Evidence

- Think forensically from the start:
  - Bring in an outside team
  - Incident response can alter evidence
Some Lawyer Questions

- Any insurance that may apply?
- Have the bad guys stolen something that was subject to a non-disclosure agreement?
Notification

It’s a big country, and you have to comply with all of it
Notification (cont’d)

- Realistically, how much will your response differ for customers in different states?
- 30 days has September, April, June, and . . . Florida
- Encryption
- Working with law enforcement delays some notification requirements
Working with Law Enforcement

- What you say won’t be privileged
- LE has tools you don’t, but has no magic wand
- If you have to disclose, it’s nice to be able to say that you’ve done everything you could
Disclaimer

This information and any presentation accompanying it (the “Content”) has been prepared by Schulte Roth & Zabel LLP (“SRZ”) for general informational purposes only. It is not intended as and should not be regarded or relied upon as legal advice or opinion, or as a substitute for the advice of counsel. You should not rely on, take any action or fail to take any action based upon the Content.

As between SRZ and you, SRZ at all times owns and retains all right, title and interest in and to the Content. You may only use and copy the Content, or portions of the Content, for your personal, non-commercial use, provided that you place all copyright and any other notices applicable to such Content in a form and place that you believe complies with the requirements of the United States’ Copyright and all other applicable law. Except as granted in the foregoing limited license with respect to the Content, you may not otherwise use, make available or disclose the Content, or portions of the Content, or mention SRZ in connection with the Content, or portions of the Content, in any review, report, public announcement, transmission, presentation, distribution, republication or other similar communication, whether in whole or in part, without the express prior written consent of SRZ in each instance.

This information or your use or reliance upon the Content does not establish a lawyer-client relationship between you and SRZ. If you would like more information or specific advice on matters of interest to you please contact us directly.
Section three

CYBER READINESS FOR FINANCIAL INSTITUTIONS

Peter Foster
Willis North America
+1 617.351.7480 | peter.foster@willis.com
Threat Environment

- Growing incentive for insiders to abuse access to sensitive data for financial gain
- Disgruntled current and former employees exploit back-doors
- Theft of Intellectual Property
- Security compromise – loss of sensitive client data
- Infrastructure downtime may lead to Dependent Business Interruption claim
- Intent is to disrupt and/or embarrass a target
- Motivations are fickle and unpredictable
- Massive DDoS attack

Malicious Insider

Exposures that lead to a potential Data Breach

Cloud or 3rd party Compromise

Negligent Insider

• Access controls and behavior monitoring insufficient to detect insider threats
- Unwary insiders susceptible to attacks that exploit traditional security controls (e.g. spear phishing)

Hacktivists

Criminal Hackers

• Users who fail to embrace “culture of security” will find ways to circumvent ‘inconvenient’ security controls

- Patience is a virtue. Tactics have evolved from “hit and run” to “infiltrate and stay.”
- Industrialization - Black markets exist for all types of personal information
- Proliferation of mobile platforms and BYOD policies creates new vectors
After suffering an intrusion or breach, an entity may become aware of the situation through a number of different ways. Some are more preferable than others.

**Discovery:**
1. Self Discovery
2. Customer Inquiry or Vendor Awareness
3. Notification and Communication from Law Enforcement or Regulators

Upon becoming aware of the situation, the breached entity will put their internal incident response plan into action. The key individuals on the Internal Response Team will actively address their designated responsibilities in an attempt to mitigate negative consequences.

Outside Legal and Forensics may be determined necessary:
1. Forensics to determine the extent of the event
2. Legal / Data Breach Coaching (Obligations/Options etc)

**Notification** (Obligatory and/or Voluntary)

**Credit Monitoring and Identity Theft related Offerings**

**Public Relations and Media Facing**

**Income Loss and Damage to Brand Reputation**

**Regulatory Actions and Fines/Penalties, PCI Fines and Penalties, Consumer Redress**

**Civil Litigation**
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 company’s data security programs

- Data Privacy & Network Security Review

- Contract with vendors to perform Incident Response prior to the incident
  - Legal Counsel, who will hire:
    - Forensic engineers
    - Crisis Management (Notification, credit monitoring, call center
    - Public relations
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
- Other executives, as appropriate
- Third-party security services (e.g., forensic investigation)
Incident Response Plan

- The “go to” document

- Notification/Escalation
  - Establish a team

- A good place to document incident
  - Incident Reports
  - Computer Logs

- Identify resources
  - Internal capabilities
  - External vendors

- Test response
Immediate Steps Following an Incident

- Call attorney to maintain privilege
- Gather Incident Response Team
- Preserve all evidence
- Engage Forensic Experts
  - Through privacy counsel (to maintain privilege)
- Contain the breach
- Call your Insurance Broker
Broker Response

- Gather details of the incident
- Determine the insuring agreements, limits, sub-limits and retentions that will apply to the incident
- What triggers a loss or claim under the policy?
- What are the notice requirements?
- Are there issues around an upcoming policy renewal/expiring policy period that require an expedited notice?
- Do you have all third-party vendors pre-approved by the underwriters?
- Draft the notice letter to be shared with client
- Schedule regular update calls
Cyber Insurance likely applicable to an Incident

- **Privacy Liability:**
  - Provides defense and liability coverage for claims resulting from your failure to maintain the privacy of information entrusted to you. Examples of Sensitive Information: Protected Health Information; Personally Identifiable Information; or a Third Party’s Confidential Corporate Information that you are required to keep confidential.

- **Breach Event Costs:**
  - Provides coverage for costs incurred due to a breach of individuals personally identifiable information or protected health information for: public relations; notification (Voluntary notification available from some carriers) of individuals; credit monitoring; call centers; obtaining legal counsel; and forensic experts to determine what information was breached and for any other expenses approved by the insurer, to respond to a breach.

- **Regulatory Defense Fines and Penalties:**
  - Provides coverage for proceedings brought by a government agency for an alleged violation of privacy regulations resulting from a breach of personal information. Coverage includes, defense, consumer redress, fines and penalties (where allowable by law).

- **PCI Fines and Penalties:**
  - Provides coverage for a monetary assessment of a fine or penalty by a Card Association or Acquiring Bank due to insured’s non-compliance with a PCI Data Security Standard, resulting from a breach.

- **Cyber Extortion:**
  - Coverage for Costs to Investigate and terminate a threat to commit an intentional attack against your Computer System.
## Potential Costs of a Data Breach

### Willis Estimated Data Breach Cost (based on number of affected individuals compromised)

<table>
<thead>
<tr>
<th>Privacy Expense (Forensics/Crisis)</th>
<th>1,000</th>
<th>10,000</th>
<th>100,000</th>
<th>500,000</th>
<th>1,000,000</th>
<th>10,000,000</th>
<th>100,000,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Expense (Forensics/Crisis)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forensics Investigation</td>
<td>$25,000</td>
<td>$100,000</td>
<td>$200,000</td>
<td>$400,000</td>
<td>$750,000</td>
<td>$1,000,000</td>
<td>$2,000,000</td>
</tr>
<tr>
<td>Data Breach Coach</td>
<td>$10,000</td>
<td>$20,000</td>
<td>$30,000</td>
<td>$50,000</td>
<td>$100,000</td>
<td>$250,000</td>
<td>$500,000</td>
</tr>
<tr>
<td>Public Relations</td>
<td>$0</td>
<td>$20,000</td>
<td>$40,000</td>
<td>$80,000</td>
<td>$200,000</td>
<td>$500,000</td>
<td>$1,000,000</td>
</tr>
<tr>
<td>Privacy Expense (Notice/Credit Monitoring)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Notification</td>
<td>$2,000</td>
<td>$15,000</td>
<td>$150,000</td>
<td>$625,000</td>
<td>$1,000,000</td>
<td>$9,000,000</td>
<td>$50,000,000</td>
</tr>
<tr>
<td>Call Center</td>
<td>$1,000</td>
<td>$10,000</td>
<td>$100,000</td>
<td>$500,000</td>
<td>$800,000</td>
<td>$5,000,000</td>
<td>$20,000,000</td>
</tr>
<tr>
<td>Credit Monitoring</td>
<td>$4,500</td>
<td>$45,000</td>
<td>$450,000</td>
<td>$2,250,000</td>
<td>$2,500,000</td>
<td>$25,000,000</td>
<td>$250,000,000</td>
</tr>
<tr>
<td>Identity Fraud Remediation</td>
<td>$1,000</td>
<td>$10,000</td>
<td>$100,000</td>
<td>$250,000</td>
<td>$500,000</td>
<td>$1,000,000</td>
<td>$5,000,000</td>
</tr>
<tr>
<td>Customer Notification</td>
<td>$2,000</td>
<td>$15,000</td>
<td>$150,000</td>
<td>$625,000</td>
<td>$1,000,000</td>
<td>$9,000,000</td>
<td>$50,000,000</td>
</tr>
<tr>
<td>Privacy Expense Total:</td>
<td>$43,500</td>
<td>$220,000</td>
<td>$1,070,000</td>
<td>$4,155,000</td>
<td>$40,000,000</td>
<td>$325,000,000</td>
<td>$328,500,000</td>
</tr>
<tr>
<td>(Privacy Expense Cost per record)</td>
<td>$43.50</td>
<td>$22.00</td>
<td>$10.70</td>
<td>$8.31</td>
<td>$5.85</td>
<td>$4.18</td>
<td>$3.29</td>
</tr>
</tbody>
</table>

### Privacy Liability

| Regulatory Defense/Fines            |       |        |         |         |           |            |            |
| State Regulatory (AG)               | $0     | $0     | $350,000 | $750,000 | $1,500,000 | $6,000,000 | $15,000,000 |
| Federal Regulatory (FTC)            | $0     | $0     | $250,000 | $500,000 | $1,000,000 | $5,000,000 | $10,000,000 |
| PCI Fines/Penalties                 | $0     | $10,000 | $20,000 | $100,000 | $500,000 | $1,000,000 | $2,000,000 |
| Civil Liability                     | $9,000 | $180,000 | $900,000 | $3,900,000 | $7,000,000 | $45,000,000 | $330,000,000 |
| Legal Defense/Damages/Class Actions | $0     | $100,000 | $300,000 | $900,000 | $2,000,000 | $5,000,000 | $30,000,000 |
| Card Reissuance Liability           | $9,000 | $80,000 | $600,000 | $3,000,000 | $5,000,000 | $40,000,000 | $30,000,000 |
| Privacy Liability Total:            | $9,000 | $190,000 | $1,270,000 | $4,750,000 | $9,000,000 | $52,000,000 | $347,000,000 |

### Total Data Breach Cost:

<table>
<thead>
<tr>
<th>1,000</th>
<th>10,000</th>
<th>100,000</th>
<th>500,000</th>
<th>1,000,000</th>
<th>10,000,000</th>
<th>100,000,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>$52,500</td>
<td>$410,000</td>
<td>$2,340,000</td>
<td>$8,905,000</td>
<td>$14,850,000</td>
<td>$93,750,000</td>
<td>$675,500,000</td>
</tr>
<tr>
<td>Per Record Cost: Retail</td>
<td>$52.50</td>
<td>$41.00</td>
<td>$23.40</td>
<td>$17.81</td>
<td>$14.85</td>
<td>$9.38</td>
</tr>
</tbody>
</table>

Assumptions:
- Credit Monitoring: $15 per individual (10%-15% take-up rate)
- Identity Fraud Remediation: $100-$500 per affected individual (less than 1% typically require fraud remediation)