Credit Unions in the Crosshairs: Cybersecurity | Research Colloquium

Best Practices to Prepare for and Respond to Data Security Incidents
You’ve heard the risks

• What can you do
  – To detect and reduce the impact of security incidents?
  – To respond appropriately if your credit union experiences a security incident?
Become “compromise–ready”

• Deploy prevention and detection tools;
• Use threat intelligence services;
• Train managers and employees;
• Conduct risk assessments focused on identifying and protecting sensitive data;
Become “compromise–ready” (cont’d)

- Manage the security of vendors;
- Understand regulators’ “hot buttons”;
- Develop, update, and practice incident response plans; and
- Evaluate your cyber liability insurance.
Deploy prevention and detection tools

Deploy an intrusion detection system (IDS) and an intrusion prevention system (IPS) that aggregate logs to a Security Information and Event Management (SIEM) tool that sends real-time alerts.
Deploy prevention and detection tools

• Ensure that servers that store sensitive data have logging enabled.
• Collect logs elsewhere than only on the server, and retain the logs for at least a year, preferably longer.
Deploy prevention and detection tools

Use multi-factor authentication for remote access and for administrator access to key servers.

Insight Enterprise Intelligence tool. Used with permission.
Deploy prevention and detection tools

Deploy data loss prevention software on the network and on USB ports to help prevent insider data thefts.
Deploy prevention and detection tools

These tools will enable you to

– Detect incidents sooner;
– Contain them more quickly; and
– Help a forensic investigator better determine what occurred before the attack was stopped.
Use threat intelligence

Utilize threat intelligence and endpoint protection that use reputational searching

– to identify artifacts of malware that anti-virus tools cannot identify, and

– to monitor how executables and binaries behave on computers.

Examples include FireEye, Cylance “Protect,” CrowdStrike Falcon, SNORT, FireAmp, Black Ice Defender, TripWire, White Hat’s Sentinel, and Bit9/Carbon Black.
Use threat intelligence

Ponemon Institute, *Advanced Threats in Retail Companies: A Study of North America & EMEA*, 7 (May 2015)
Use threat intelligence

**Figure 11. The most promising technologies to stop or minimize ATs**
Three responses permitted

<table>
<thead>
<tr>
<th>Technology</th>
<th>Response Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technologies that provide intelligence about networks and traffic</td>
<td>64%</td>
</tr>
<tr>
<td>Technologies that isolate or sandbox malware infections</td>
<td>55%</td>
</tr>
<tr>
<td>Technologies that secure information assets</td>
<td>55%</td>
</tr>
<tr>
<td>Technologies that secure the perimeter</td>
<td>42%</td>
</tr>
<tr>
<td>Technologies that provide intelligence about attackers’ motivation and weak spots</td>
<td>40%</td>
</tr>
<tr>
<td>Technologies that secure endpoints including mobile-connected devices</td>
<td>26%</td>
</tr>
<tr>
<td>Technologies that simplify the reporting of threats</td>
<td>13%</td>
</tr>
<tr>
<td>Technologies that minimize insider threats (including negligence)</td>
<td>5%</td>
</tr>
</tbody>
</table>

Ponemon Institute, *Advanced Threats in Retail Companies*, 11.
Train managers and employees

- Recognize threats to different services and technologies, e.g., ACH transfers and ATMs;
- Regularly discuss cybersecurity at Board and senior management meetings; and
- Regularly provide employee cybersecurity awareness and training.
Train managers and employees

Provide threat awareness training to enable employees to identify anomalous behavior. For example, the following incident was stopped by an alert credit union teller –
Credit union incident

- Thieves downloaded malware onto a teller’s computer
- Stole the teller’s credentials
- Used the credentials to add account holders to existing accounts and to create new accounts
- Made illusory electronic fund transfers into the accounts
- Sent mules with IDs for the new account holders to withdraw the funds
- Cost the credit union $510,119 in uninsured expenses.
Train managers and employees

The incident was thwarted when a teller noticed that a fraudulent “deposit” into a new “member’s” account was supposedly made with assistance of another teller – after the pertinent branch was closed.
Train managers and employees

Train (or hire) staff to provide continuous network security monitoring

– to respond to alerts from IDS/IPS, analytics, and endpoint protection tools; and

– to prevent exfiltration of data at one of the points on the “kill chain” when malware is found on the network.
Train managers and employees

- **Initial Training at Time of Hiring**
  - Spotting security problems
  - Avoiding inadvertent disclosures through mistaken emails, faxes, and paper records mishandling
  - Reporting procedures
  - Supervisors trained to handle reports

- **Regular and Continued Training**
  - Formal online training vs. in person
  - Staff meetings
  - Newsletters
  - PhishMe or other anti-phishing training
Hi, Sir/Madam,

For the company’s network security, we have upgraded the Citrix Virtual Workplace System. Please login to the Citrix Virtual Workplace System to activate your Account. You should install the Citrix Secure Input IE ActiveX Control before you type in your password.

Citrix Login: https://poccitrix.[companyname].com/vpn/index.html

For more information, please contact me.

Best regards,

[Actual name]
[Correct title] Systems Administration
Phone: [correct phone number]
Email: [correct email address]
Local Address: [correct address]
[Company name]
[Company address]
Train managers and employees

Who clicks on Malicious Messages: IT or Sales?

*Click rate by department*

Volume of malicious messages by department

Proofpoint, The Human Factor 2015, 10
Train managers and employees

Source: Dept. of Homeland Security

- Phishing: 71%
- Unpatched vulnerabilities: 50%
- DDoS: 42%
- SQL injection: 32%
- Cross site scripting: 21%
- Hacktivist-originated attacks: 21%
- APTs: 18%

(Advanced Persistent Threats, i.e., sophisticated network attacks)
Conduct risk assessments

Use security firms to conduct

• Periodic, credentialed vulnerability scans and correct vulnerabilities discovered;

• Penetration tests on
  – Internet-facing applications that contain sensitive data or provide access to internal networks, and
  – Internally-accessible applications that contain sensitive data.

• Security program reviews.
Manage vendors’ security

Target Timeline

- Target certified as PCI-DSS compliant
- First FireEye alerts triggered
- More FireEye alerts triggered
- DOJ notifies Target
- Target publicly announces 40 million credit and debit card records stolen after story broken on 12/18

Attacker Timeline

- Attackers first breach Target network
- Attackers steal Fazio credentials
- Attacker test malware on Target POS
- Attackers install malware on Target POS
- POS malware fully installed
- Attackers install upgraded versions of exfiltration malware - begin exfiltrating data
- Attackers install data exfiltration malware
- Attackers lose foothold in Target network

Source: U.S. Senate Committee on Commerce
Understand regulators’ “hot buttons”

Including:

– Failure to encrypt sensitive data;
– Failure to deploy data loss prevention software;
– Failure to manage vendor security;
– Failure to conduct periodic risk assessments or to correct vulnerabilities discovered in assessments;
– Failure to prevent SQL injection attacks;
– Failure to change default configurations or passwords;
– Absence of appropriate policies;
– Insufficient employee training or awareness; and
– Insufficient dedicated security roles.
Practice incident response plans

Response Program Supervisory Guidance
(12 C.F.R. 748, App’x B):

• An incident response program should provide that the credit union will:
  – Assess the nature and scope of the incident and what member information is involved;
  – Notify the NCUA Regional Director and applicable state supervisory authority as soon as possible after discovery of unauthorized access to or use of sensitive member information;
  – Notify law enforcement and file a SAR if warranted;
  – Contain the incident; and
  – Notify members when warranted.
Practice incident response plans

Review your incident response plan and conduct tabletop exercises with the team that will respond to an incident, including your

- Forensic investigator;
- Counsel; and
- Crisis management firm.
Evaluate your cyber liability coverage

Does it cover

– Incident response costs (incurred with consent of the insurer in response to an incident that triggers notification obligations, e.g., legal, call center, mail center costs);
– Computer forensic costs (associated with confirming the breach and identifying affected data subjects);
– Credit or Identity Protection Costs
– Crisis Management
Evaluate your cyber liability coverage

- Hacker Damage (costs to repair or replace your data, computer systems, or programs);
- Business Interruption (e.g., costs caused by an attacker that DDOS’s your website);
- Cyber Extortion (e.g., money paid and expenses incurred as a result of your receipt, of an illegal threat to destroy or encrypt your data);
- Defense costs/settlement expenses; and
- Regulatory fines.
Evaluate your cyber liability coverage

Direct costs:
- forensics,
- legal,
- notification,
- credit monitoring;

Indirect costs:
- employee time,
- decreased brand value,
- reputation harm,
- lost customers.

Source: Ponemon Institute, 2015 Cost of Data Breach Study: United States
Evaluate your cyber liability coverage

Figure 4. Per capita cost by industry classification of benchmarked companies

| Industry       | Per capita cost
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td>$398</td>
</tr>
<tr>
<td>Pharmaceutical</td>
<td>$298</td>
</tr>
<tr>
<td>Financial</td>
<td>$259</td>
</tr>
<tr>
<td>Energy</td>
<td>$256</td>
</tr>
<tr>
<td>Transportation</td>
<td>$252</td>
</tr>
<tr>
<td>Communications</td>
<td>$237</td>
</tr>
<tr>
<td>Education</td>
<td>$225</td>
</tr>
<tr>
<td>Services</td>
<td>$219</td>
</tr>
<tr>
<td>Consumer</td>
<td>$218</td>
</tr>
<tr>
<td>Industrial</td>
<td>$190</td>
</tr>
<tr>
<td>Retail</td>
<td>$189</td>
</tr>
<tr>
<td>Media</td>
<td>$185</td>
</tr>
<tr>
<td>Technology</td>
<td>$178</td>
</tr>
<tr>
<td>Research</td>
<td>$166</td>
</tr>
<tr>
<td>Hospitality</td>
<td>$135</td>
</tr>
<tr>
<td>Public</td>
<td>$73</td>
</tr>
</tbody>
</table>

Source: Ponemon Institute, 2015 Cost of Data Breach Study: United States
Evaluate your cyber liability coverage

Other issues:

- Scope of duty to defend and choice of counsel
- Allocation of defense costs
- Sublimits for covered costs
What you will have to do to respond

Discovery of a Security Incident

- Theft, loss, or Unauthorized Disclosure of Personally Identifiable Non-Public Information or Third Party Corporate Information that is in the care, custody or control of the Insured Organization, or a third party for whom the Insured Organization is legally liable

Evaluation of the Security Incident

- Forensic Investigation and Legal Review

Managing the Short-Term Crisis

- Notification and Credit Monitoring
- Public Relations

Handling the Long-Term Consequences

- Class-Action Lawsuits
- Regulatory Fines, Penalties, and Consumer Redress
- Reputational Damage
- Income Loss

Public Relations

Reputational Damage

Income Loss
What you will have to do to respond

• Notification issues:
  – Is it a “breach”?
  – Should you notify your broker or insurer?
  – Should you retain counsel?
  – Should you hire a forensics company?
  – Should you notify regulatory agencies?
  – Should you hire a crisis management firm?
  – Should you offer credit monitoring?
What you will have to do to respond

• More issues:
  – Can you meet 30-day and 45-day state deadlines?
  – Should you notify affected individuals or the data owner?
  – Should you notify state consumer agencies or Attorneys General?
  – Should you notify credit reporting agencies?
  – Should you notify local police departments, the Secret Service, or the FBI?
What you will have to do to respond

Federal law: Interagency Guidelines, authorized under Gramm-Leach-Bliley Act (GLBA) 501(b), impose certain breach notification requirements on financial institutions:

• Investigate
  – Must promptly investigate when alerted to unauthorized access to member information

• Notify Members
  – Notification to members required when determined that misuse of members’ information has occurred or is reasonably possible
  – Notification must occur “as soon as possible”
  – If unable to determine which specific member possibly affected, must notify relevant group(s) of members
What you will have to do to respond

NCUA position on member notification:

– “If the credit union determines that misuse of its information about a member has occurred or is reasonably possible, it should notify the affected member as soon as possible.

– “For purposes of this Guidance, sensitive member information means a member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account.”

What you will have to do to respond

GLBA and Breach Notification Regulations:

• Required Content of Member Notification:
  – Recommend that member review account statements and immediately report any suspicious activity to the credit union;
  – Provide information on placing a fraud alert in the member’s consumer report;
  – Recommend obtaining and reviewing credit reports from credit reporting agencies;
  – Explain how to obtain a credit report free of charge; and
  – Refer to the FTC’s identity-theft guidance.
What you will have to do to respond

- **State law requirements:**
  - 47 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?
What you will have to do to respond

- How are state data breach notification laws triggered?
  - Access to or acquisition of specific types of information by an unauthorized person of
  - Name plus
    - Social Security number
    - Driver's license number
    - Credit card number
    - Bank account Information
    - Online account and password (some states)
  - Risk of Harm
  - Computerized records vs. information on paper
What you will have to do to respond

Guiding principles for responding to an incident:

- Let the forensics drive the decision-making;
- Be guarded, consistent, and honest in communications;
- Mitigate harm
  - E.g., use a claims program; and
- Don’t try to win members back in breach notification communications.
What you will have to do to respond

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 a WISP and incident response plan?
9. How did you detect the intrusion?
10. What have you done so far?
What you will have to do to respond

More questions regulators may ask:

11. Why did it take so long to notify members?
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. Why did you have former members’ information?
18. If a vendor caused the breach:
   – What does the vendor agreement require?
   – Has the vendor experienced other breaches?
   – Do you audit the vendor?
What you may have to do to respond

Defend against class action claims:

- Negligence
- Implied-in-fact contract
- Unjust enrichment
- Breach of fiduciary duty
- Invasion of privacy
- State consumer fraud statutes
- State notification statutes
- Federal statutory claims (statutory damages)
What you may have to do to respond

Litigate a motion to dismiss class action claims. There is a split regarding how courts apply the holding of *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138 (2013):

- Courts accepting defendants’ standing arguments and dismissing lawsuits:
  - *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588 (N.D. Ill. 2013)

- Courts rejecting defendants’ standing arguments and letting lawsuits proceed:
  - *Remijas v. Neiman Marcus Group, Inc.*, 794 F.3d 688 (7th Cir. 2015)
What you may have to do to respond

• Defeat claims against officers and board members:
  – In *Davis v. Steinhafel*, Target shareholders allege Target’s officers and directors are personally liable for
  • Failing to implement internal controls to protect customers’ personal and financial information; and
  – Breaching their duties of loyalty and good faith by failing to institute adequate internal controls, imprudently managing the company, failing to supervise employees, and wasting assets.
Questions?

BakerHostetler

Randy Gainer, Partner CISSP
Seattle
rgainer@bakerlaw.com
206.332.1381