Cybersecurity Planning

WSU Security Awareness Day

October 23, 2018

Randy Gainer, Partner, CISSP
rgainer@bakerlaw.com
Introduction

- 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 2,500 incidents handled (560+ in 2017 alone)
- Team includes 45+ attorneys specializing in privacy and data security law across the country
Issues to discuss

- Why do we need information security?
- What is information security and privacy risk?
- How do you identify and quantify risk?
- What do risk assessments entail?
- How do we mitigate information security and privacy risk?
- Where do we go from here?
Overview

• In today’s threat environment, completely effective cybersecurity is either impossible or impossibly expensive

• Cybersecurity incidents will happen

• Managers must prepare to respond to and recover from those incidents

• There is no easy way to improve cybersecurity

• A brief look at the threats and effects of cybersecurity incidents
Why do we need information security?
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
  - Malware
  - Phishing and Spear Phishing
  - Ransomware
- Social Engineering
- Thieves
- Vendors
- State sponsored attackers
Why Do Incidents Occur – Most Common Causes

6% System Misconfiguration
11% Stolen/Lost Device or Records
13% Other
17% Inadvertent Disclosure

34% Phishing
- 32% Remote Access
- 24% Other
- 20% W-2 Scam
- 18% Ransomware
- 6% Automated Information Exfiltration

19% Network Intrusion
- 38% Ransomware
- 29% Other
- 17% Automated Information Exfiltration
- 16% Remote Access
Hack or Malware 36%

Unintended Disclosure 28%

Insider 10%

Social Engineering 10%

Portable Device 7%

Physical Loss/Non-Electronic Record 6%

Other 1%

Unknown 1%

2017 INCIDENTS BY CAUSE

Data from Beazley Breach Response Services
2017 INCIDENTS BY INDUSTRY

Data from Beazley Breach Response Services
Cyber Extortion

- Ransomware encrypts data, allowing the attacker to demand money in return for a key that (allegedly) can be used to decrypt the data.

- DDoS attacks can also be used as part of an extortion scheme: an attacker can shut down a website and deny service until a ransom is paid.
Forensic Investigations - Necessary and Expensive

- **87%** Log Review
- **55%** Imaging
- **30%** Malware Analysis
- **13%** Endpoint Scanners

**Use of Outside Forensics**
- 65% of Network Intrusion Incidents
- 41.5% of Data Breach Incidents

**Forensic Investigation Costs**
- $84,417 for All Incidents
- $86,751 for Network Intrusion Incidents
- $436,938 for 20 Largest Investigations

**Completion Time for Forensic Investigation**
- 36 Days

**Evidence of Data Exfiltration in Network Intrusion Incidents**
- 24%
Incident Response Timeline

- **Occurrence to Discovery**: 66 Days
- **Discovery to Containment**: 3 Days
- **Time to Complete Forensic Investigation**: 36 Days
- **Discovery to Notification**: 38 Days
When does notification need to happen?

- Protected Health Information (PHI) or Personal Information (PI) involved
- HIPAA: presumed breach, unless covered entity shows a low probability of compromise
- State law: acquisition or “risk-based" trigger
- Timing (HIPAA - 60 days v. WA state - 45)
- Other state laws vary
What Happens After the Notices are Mailed?

- Reputational harm
- Notification vs. lawsuits
- Litigation and regulatory investigations
- AG inquiries
- Payment card industry inquiries
- Operations and productivity are affected
What is info. security and privacy risk?

• Risk of cybersecurity incidents
  – Costs, reputational damage, regulatory investigations, litigation

• Risk of privacy violations of students, employees, other stakeholders
• How do you identify and quantify risk?
• What do risk assessments entail?
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.
Risk assessments

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Compromise Assessment</th>
<th>Am I compromised?</th>
<th>Identify past or present compromises of your environment, assess future risk of compromise based on your security hygiene and improve your ability to respond.</th>
<th>Know whether or not your organization is currently or was previously compromised.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Am I exposed?</td>
<td>Red Teaming and Penetration Testing</td>
<td></td>
<td>Test your security posture using the same tools, tactics and procedures (TTPs) as the advanced attackers we see every day during our Incident Response engagements.</td>
<td>Identify previously undetected weaknesses before an attacker does.</td>
</tr>
<tr>
<td></td>
<td>Industrial Control Systems Healthcheck</td>
<td></td>
<td>Minimally invasive assessment of an industrial facility’s overall cyber security posture, bridging between IT and OT security.</td>
<td>Understand your ICS’s exposed vulnerabilities and establish a plan to reduce your system’s cyber security risk.</td>
</tr>
<tr>
<td>Am I prepared?</td>
<td>Response Readiness Assessment</td>
<td></td>
<td>An independent maturity assessment of your security monitoring and response capabilities, informed by our experience on the front lines of incident response.</td>
<td>Learn how to improve your organization’s defense posture to find and stop attackers faster.</td>
</tr>
<tr>
<td></td>
<td>Security Program Assessment</td>
<td></td>
<td>An in-depth evaluation of your organization’s information security programs across ten key security domains, each of which is mapped to compliance, security and industry frameworks.</td>
<td>Evaluate the effectiveness of your information security program to improve your security posture and reduce business risk.</td>
</tr>
</tbody>
</table>
Risk assessments (cont’d)

• Program assessments should address:
  – Governance, compliance and organization
  – Data protection (encryption)
  – Security risk management (insurance)
  – Identity & access management
  – Incident response planning
  – Vendor management
  – Host and endpoint protection
  – Application, database and mobile protection
  – Cloud and data center protection
  – Security awareness & training
Conduct risk assessments (cont’d)

• Outside counsel should retain the forensic firm to conduct the assessment to provide technical information to enable counsel to advise the client.
  – Any negative findings can potentially be protected from discovery by attorney-client privilege.
Requirements for privilege

• When:
  – an assessment is led by an attorney;
  – communications about the assessment are kept confidential among managers, employees, and consultants with a need to know the information; and
  – the primary purpose (or in some states, one purpose) of the assessment is to provide legal advice,

• Communications related to the assessment should be protected from discovery by the attorney-client privilege.
Contractual language for privileged assessments

• The objective of this professional services engagement is to assist Counsel to provide legal advice to Client. During the term of this SOW, [technical consultant] will provide professional services as directed by Counsel. For the duration described below, [technical consultant] agrees to provide services ("Services") as set forth below.
Contractual language for privileged assessments

• [Technical consultant] will provide the services at Counsel's direction. All communications, deliverables, or other data gathered by or for [technical consultant] in connection with Mandiant's work under this SOW will be sent directly to Randy Gainer via email at rgainer@bakerlaw.com or care of BakerHostetler, 999 Third Avenue, Suite 3600, Seattle, WA 98104.

• Additionally, all such communications, as well as any internal memoranda, documents, files, emails, and electronic or physical media of any kind that relates in any way to the SOW should be clearly labeled as Attorney-Client Privileged, Prepared at the Direction of Counsel, Prepared in Anticipation of Litigation, or Attorney Work Product.
Report language to support privilege

• The objective of this assessment was to provide technical information to BakerHostetler, LLP (“BakerHostetler”) to enable BakerHostetler to provide legal advice to [client].
How do we mitigate information security and privacy risk?

1. Use appropriate preventative and detective technological tools
   - Deploy multi-factor authentication for remote access and to access sensitive data internally
   - Conduct frequent and regular reviews of logs and system monitoring data

2. Train employees
   - Conduct phishing tests on employees and frequently remind them of cybersecurity risks

3. Conduct periodic security assessments using cybersecurity experts
   - Discover system vulnerabilities and security deficiencies
   - Implement recommended improvements

4. Manage vendors as an attack surface

5. Conduct regular tabletop exercises and revise your incident response plan to implement needed changes

6. Make sure you have appropriate insurance coverage
1. Use appropriate tools

• California Department of Justice (CDOJ) released the California Data Breach Report (Feb. 16, 2016).

• In the report, the CDOJ sets out 20 security controls identified by the Center for Internet Security that “constitutes a minimum level of security – a floor – that any organization that collects or maintains personal information should meet.”
1. Use appropriate tools (cont’d)

<table>
<thead>
<tr>
<th>CSC 1</th>
<th>Inventory of Authorized and Unauthorized Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 2</td>
<td>Inventory of Authorized and Unauthorized Software</td>
</tr>
<tr>
<td>CSC 3</td>
<td>Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
</tr>
<tr>
<td>CSC 4</td>
<td>Continuous Vulnerability Assessment and Remediation</td>
</tr>
<tr>
<td>CSC 5</td>
<td>Controlled Use of Administrative Privileges</td>
</tr>
<tr>
<td>CSC 6</td>
<td>Maintenance, Monitoring, and Analysis of Audit Logs</td>
</tr>
<tr>
<td>CSC 7</td>
<td>Email and Web Browser Protection</td>
</tr>
<tr>
<td>CSC 8</td>
<td>Malware Defenses</td>
</tr>
<tr>
<td>CSC 9</td>
<td>Limitation and Control of Network Ports, Protocols, and Services</td>
</tr>
<tr>
<td>CSC 10</td>
<td>Data Recovery Capability</td>
</tr>
<tr>
<td>CSC 11</td>
<td>Secure Configurations for Network Devices such as Firewalls, Routers, and Switches</td>
</tr>
<tr>
<td>CSC 12</td>
<td>Boundary Defense</td>
</tr>
<tr>
<td>CSC 13</td>
<td>Data Protection</td>
</tr>
<tr>
<td>CSC 14</td>
<td>Controlled Access Based on the Need to Know</td>
</tr>
<tr>
<td>CSC 15</td>
<td>Wireless Access Control</td>
</tr>
<tr>
<td>CSC 16</td>
<td>Account monitoring and Control</td>
</tr>
<tr>
<td>CSC 17</td>
<td>Security Skills Assessment and Appropriate Training to Fill Gaps</td>
</tr>
<tr>
<td>CSC 18</td>
<td>Application Software Security</td>
</tr>
<tr>
<td>CSC 19</td>
<td>Incident Response and Management</td>
</tr>
<tr>
<td>CSC 20</td>
<td>Penetration Tests and Red Team Exercises</td>
</tr>
</tbody>
</table>

https://www.cisecurity.org/critical-controls.cfm
1. Use appropriate tools (cont’d)

Financial institutions have used multi-factor authentication for access to online bank accounts for nearly a decade, sometimes supplementing username and password with biometrics such as “keystroke dynamics” that recognizes a user’s unique typing pattern or with other factors, such as a one-time-password generator.

This form of authentication should be used by all organizations to help protect access to critical systems and sensitive data, such as medical information, financial information, Social Security numbers, as well as company confidential information like intellectual property and trade secrets. Multi-factor authentication is included in the CIS Critical Security Controls for administrative access (CSC 5.6), organizational email accounts (CSC 7), remote login access to company systems (CSC 12.6), and user accounts on the company network (CSC 16.11).

Multi-factor authentication should also be more widely available for consumer-facing online accounts that contain sensitive personal information. Such accounts include online shopping accounts, health care web sites and patient portals, and web-based email accounts.

1. Use appropriate tools (cont’d)

• Security Information and Event Monitoring (SIEM) System;
• A security operation center (SOC) staffed by trained security engineers or provided by a vendor to monitor SIEM output;
• Log retention capabilities on systems that store or process PI for at least one year.
2. Train employees

- Successful phishing attacks were the single largest cause of cybersecurity incidents we handled in 2017.
  - Employees click on links in phishing emails disguised as invoices, links requesting that users update their email account credentials, and DocuSign attachments.
  - Attackers gain access to emails and attachments in the user’s account and to documents in public folders accessible with the user’s credentials.
  - Logs may or may not be available to determine what emails and other documents the attackers accessed.
  - Data mining may be needed to determine what documents the attackers may have accessed.
  - Numerous individuals and regulators may need to be notified.
2. Train employees (cont’d)

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

- Scammers phish online payroll management account credentials used by corporate HR professionals.
2. Train employees (cont’d)
2. Train employees (cont’d)

- PhishMe and similar training tools can decrease the number of employees who are deceived by phishing emails.
- Periodic reminders about phishing risks can also help.
4. Manage vendors

- Business-critical vendors are often the riskiest:

Source: Cyence Big Data Analytics Platform
ongoing forensic investigation has indicated that the intruder stole a vendor's credentials which were used to access our system.”

- Molly Snyder, Target spokeswoman

4. Manage vendors (cont’d)

• Four Key Considerations:
  – Conduct privacy and security due diligence when selecting a vendor
  – Ensure the vendor agreement contains appropriate safeguards for personal data
  – Monitor vendors to verify that they comply with their privacy and security obligations throughout the life of the relationship
  – Require cyber insurance where appropriate
5. Conduct tabletop exercises & revise your IRP
Conduct tabletop exercises & revise your IRP (cont’d)

• IRT leader/coordinator
• Privacy officer
• Legal
• Risk management
• Others as appropriate
  – Information security
  – HR, employee relations, patient relations
  – Public relations
  – Fulfillment Vendor
  – Broker
  – Outside legal counsel
  – Crisis Management Firm
Conduct tabletop exercises & revise your IRP (cont’d)

- Some of the questions for the IRT:
  - Was computerized PI involved?
  - Do you notify your cyber insurer?
  - Do you notify management?
  - Do you involve law enforcement?
  - Do you hire a forensics company?
  - Do you retain counsel?
  - Do you involve regulatory agencies?
  - Is a crisis management vendor necessary?
  - Do you offer credit monitoring?
Conduct tabletop exercises & revise your IRP (cont’d)

Appendix E - Notification Checklist

☐ Consider whether an external forensic firm should be engaged. If so, engage firm through external counsel.

☐ Determine the potentially affected individuals and the data elements for those individuals.

☐ Analyze the data elements to determine if notification is required under federal and state laws.

☐ Determine if law enforcement should be notified.

☐ Determine which regulators, if any, need to be notified.

☐ Determine whether a crisis management firm needs to be engaged (consider sensitivity of data, number of people involved, etc.). If so, engage firm through external counsel.

☐ Prepare and continue to update a media hold statement in conjunction with communications team, legal counsel and the crisis management firm, if one was retained.

☐ Determine if notification vendor (for mailing and operating a call center) is to be used.

☐ Assess if credit monitoring should be offered and to whom (minors and adults).
Obtain the right cybersecurity insurance coverage

- Incident costs can range from a few thousand dollars to several hundred million, depending on the number of PI records exposed.
- Coverage should address internal costs, third-party claims and regulatory claims.
- Business interruption costs and socially engineered fraudulent fund transfers should be considered.
Where do we go from here?

• If you haven’t done some of these things, now’s the time.
  – Use appropriate preventative and detective technological tools
  – Train employees
  – Conduct periodic security assessments using cybersecurity experts
  – Manage vendors as an attack surface
  – Conduct regular tabletop exercises and revise your incident response plan to implement needed changes
  – Make sure you have appropriate insurance coverage
Questions
These materials have been prepared by Baker & Hostetler LLP for informational purposes only and are not legal advice. The information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional counsel. You should consult a lawyer for individual advice regarding your own situation.