Psst... Your P.I.I. Is Showing

Media & the Law Seminar
April 25, 2014
Kansas City, Mo.
Introductions

Panelists

• Michael Born, Lockton Companies
• Christopher Cwalina, Holland & Knight
• Rebecca Stroder, Mandiant

Moderator: Blaine Kimrey, Lathrop & Gage LLP
Meet Wayne Bruce

▪ General Counsel of the Gotham Business Review, a highly respected daily business newspaper with a strong web presence.

▪ This morning, Wayne’s CIO told him that they discovered a data breach: an attacker was able to access the Review’s files holding subscriber user names, passwords, and credit card information.
In 2013 Mandiant noted an increase in threat actor activity in two key industries:

- **Financial Services**: up to 15% from 11%
- **Media & Entertainment**: up to 13% from 7%

The chart shows the following industries and their respective percentages:

- **Other**: 23%
- **Education**: 3%
- **Legal Services**: 3%
- **Transportation**: 3%
- **Pharmaceuticals & Biotechnology**: 4%
- **Telecommunications**: 4%
- **Chemical Manufacturing**: 4%
- **Construction**: 4%
- **Retail**: 4%
- **Aerospace & Defense**: 6%
- **Business Services**: 4%
- **Manufacturing**: 10%
How Compromises Are Being Detected

37% of victims discovered the breach internally

63% of victims were notified by an external entity

- 2% by a customer
- 4% by a business partner
- 15% by an outsourced service provider
- 42% by law enforcement

33% of victims discovered the breach internally

Down from 37% in 2012

67% of victims were notified by an external entity
229
median number of days that threat groups were present on a victim’s network before detection

14 days less than 2012

Longest Presence: 2,287 days
Trouble in Gotham (and beyond): What Next?
Part 1: Early Assessment

Technical issues

a. Initial Assessment of Scope
b. Identification of Entry Points
c. Investigation/Remediation
Part 1: Early Assessment

[Diagram showing timeline and events related to the Target data breach, including dates and actions taken such as announcing breaches, appointing investigators, and offering credit monitoring.]
Part 1: Early Assessment

Phishing Email Trends

44% of observed phishing emails were IT related, often attempting to impersonate the targeted company's IT department.

93% of phishing emails were sent on weekdays.
Part 1: Early Assessment

Dear [News Agency Name] journalists,

Please take attention of UNHCR report about Syria:

http://malicious-url.com

Thanks & Regards
[name of actual report’s author]

Hello,

Please read the following article, its very important:

http://malicious-url.com

Thanks & Regards
[signature line of News Agency employee]

Hello,

Please read the following article, its very important:

http://malicious-url.com

Many Respect

Hello [Name],

Please check this link:

http://malicious-url.com

All Respect
[Name]
### Part 1: Early Assessment

<table>
<thead>
<tr>
<th>ITEM STOLEN</th>
<th>HOW THE ATTACKERS USE INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Infrastructure Documentation Including Schematics and Configuration Files</td>
<td>Understand firewall and other IDS configurations and where vulnerabilities that can be exploited exist.</td>
</tr>
<tr>
<td>Organization Chart</td>
<td>Establish individuals to target in spear-phishing campaigns or to target for email and data theft.</td>
</tr>
<tr>
<td>Systems Documentation</td>
<td>Identify where targeted systems existing within a victim network.</td>
</tr>
<tr>
<td>VPN Configuration Files</td>
<td>Identify what VPN users have access to within a victim’s network and target VPN credential data to steal.</td>
</tr>
</tbody>
</table>
Part 1: Early Assessment

Technical issues

a. Initial Assessment of Scope
b. Identification of Entry Points
c. Investigation/Remediation
Part 1: Early Assessment

Insurance issues
  a. Assess potentially applicable policies
# Part 1: Early Assessment

<table>
<thead>
<tr>
<th>Event</th>
<th>General or Professional Liability</th>
<th>Property</th>
<th>D&amp;O</th>
<th>Crime</th>
<th>Cyber Liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security Breach</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Privacy Breach</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Media Liability</td>
<td>POSSIBLE</td>
<td>NONE</td>
<td>POSSIBLE</td>
<td>NONE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Virus Transmission</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Damage to Data</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Breach Notification</td>
<td>NONE</td>
<td>NONE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Regulatory Investigation</td>
<td>POSSIBLE</td>
<td>NONE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Extortion</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>NONE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Virus/Hacker Attack</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Denial of Service Attack</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>COVERED</td>
</tr>
<tr>
<td>Network Business Interruption</td>
<td>NONE</td>
<td>POSSIBLE</td>
<td>POSSIBLE</td>
<td>NONE</td>
<td>COVERED</td>
</tr>
</tbody>
</table>
Traditional Polices: Limited Coverage at Best

General Liability Policies:

- A N.Y. trial court recently ruled that a commercial general liability (CGL) policy does not provide coverage for litigation stemming from April 2011 hacking of Sony Corp.’s PlayStation online services. *Zurich American Insurance Co. v. Sony Corp. of America et al.* Sony has appealed.

- Recent revision by Insurance Services Office, Inc. (ISO) to standard CGL policy forms to be effective on or after **May 1, 2014** in all but four U.S. states/territories.
  - Exclusion of coverage for claims arising from the access or disclosure of confidential information.
  - In addition to third-party damage claims, eliminates coverage for costs of:
    - Notifications
    - Credit monitoring
    - Forensic investigations
    - Public-relations campaigns
    - Other expenses typically related to data breach
Traditional Polices: Limited Coverage at Best

Crime Polices:
• Some coverage under computer-fraud provisions, but typically only applies to loss of property or funds.
• No coverage for direct costs of responding to the breach or for privacy related liability damages and defense costs.

D&O and E&O (Professional Liability Policies)
• May be some coverage for liability claims, but only those arising from the provision of professional services and usually a negligence trigger.
• Still no coverage for the direct costs of responding to the data security breach.
Part 1: Early Assessment

Insurance issues
a. Assess potentially applicable policies
b. Timely notification
  - Some windows as short as 3 days
c. Obtain prior written approval as required
  - “Voluntary payments” provision
Part 1: Early Assessment

3. Legal issues
   a. Litigation hold?
   b. Contracts & indemnities
      • Vendors
      • Payment processors, etc.
   c. Nature of breach/data compromised
Common Early Mistakes

Technical:

• “Fixing” the problem by deleting files, re-imaging, etc.
• Using only internal personnel to address the breach
• Assuming the SI or other IT service provider can handle the investigation/remediation work (some can, many can’t)
Common Early Mistakes

Insurance:
• Lack of policy awareness
• Not having response team (external and internal) identified in advance
• Failure to notify/seek approval
Common Early Mistakes

Legal:
- Failure to instigate litigation hold
- Making public statements without advice of counsel
- Missing notification deadlines
- Overall failure to understand gravity of the situation
Part 2: Notifications

- Law enforcement
- Insurers
- Regulators
- Customers/data subjects
- Third-party service providers
- Media
Part 3: When it Gets More Complicated
While investigating the original breach, Mr. Wayne has learned that the attackers also targeted sensitive information in Gotham Business Review reporters’ email accounts.
Part 3: When it Gets More Complicated

**Repetitive Attacks by Industry, 2012**

- 31% Aerospace & Defense
- 17% Energy, Oil & Gas
- 15% Pharmaceuticals
- 11% Finance
- 4% Media & Entertainment
- 3% Computer Hardware & Software
- 2% Telecommunications
- 2% Legal & Consulting Services
- 13% Other
Part 3: When it Gets More Complicated

Response to 2nd breach:
Part 3: When it Gets More Complicated

Insurance issues as breach evolves:

• Notify carrier in advance of any big decisions and give them time to respond.
  • Better yet, obtain prior written approval.

• Track your spending. Ask the carrier to pay directly once retention/deductible has been exhausted.
Part 4: Litigation/Resolution
Part 4: Litigation/Resolution

Major Trends/Decisions:
Part 4: Litigation/Resolution

Insurance Issues:

- Both you and insurance carrier must agree to settlement

- Be aware of your “hammer clause” provisions in the event that you do not want to follow the settlement recommendations of your carrier.
Final Thoughts?

• Know your coverage
• Know the limits of your own organization’s expertise
• Act quickly
• Embrace complexity
• Don’t wait until a breach happens to start planning