CYBER LIABILITY SYMPOSIUM
Panel

• Jason Glasgow – Travelers Insurance Company
• Sean Hoar, Esq., Davis Wright Tremaine
• Timothy Wallach, Supervisory Special Agent, Cyber Task Force, FBI Seattle Division
• Andreas Kaltsounis- Stroz Friedberg

Moderator

• Peter Marchel, Esq., Marchel & Associates Risk Consulting
CYBER EVENT

- Top 3 technical or organizational challenges for incident response:
  - Ability to detect and respond to attacks
  - Weakest area of preparedness / response
  - Testing – no such thing as one-n-done
CYBER EVENT

• Weakest area of preparedness / response:
  – In-house skills
  – Incident detection
  – Technology to detect and respond
  – Rapid Response
Across the Cyber Threat Landscape
Cyber threat actors are exploiting networks for an ever-widening array of economic and political objectives.

<table>
<thead>
<tr>
<th>Objective</th>
<th>NUISANCE</th>
<th>DATA THEFT</th>
<th>CYBER CRIME</th>
<th>HACKTIVISM</th>
<th>DESTRUCTIVE ATTACK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Advantage</td>
<td></td>
<td>&amp; Policy</td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>Botnets &amp; Spam</td>
<td>Advanced Persistent</td>
<td>Credit Card Theft</td>
<td>Website Defacements</td>
<td>Delete Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Threat Groups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td>Often Automated</td>
<td>Persistent</td>
<td>Frequently Opportunistic</td>
<td>Conspicuous</td>
<td>Conflict Driven</td>
</tr>
</tbody>
</table>

Mandiant’s Mtrends 2015: A View From the Front Lines
## Average breach claim costs

<table>
<thead>
<tr>
<th>Category</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost business</td>
<td>$3.72M</td>
</tr>
<tr>
<td>Notification</td>
<td>$560k</td>
</tr>
<tr>
<td>Post breach</td>
<td>$1.64M</td>
</tr>
<tr>
<td>Detection</td>
<td>$610k</td>
</tr>
<tr>
<td>Legal defense</td>
<td>$698k</td>
</tr>
<tr>
<td>Legal settlement</td>
<td>$558k</td>
</tr>
</tbody>
</table>

Sources: NetDiligence® Cyber Claims Study 2014 and Ponemon 2015 Cost of a Data Breach Study
Why so expensive?

Security breach action steps

► Determining cause of security breach and persons whose identity information was accessed or acquired without their authorization

► Legal fees to determine applicable laws, develop materials and proactively defend firm from future liabilities

► Notify victims of breach, may include
  • Physical mailings
  • Emails
  • Call centers (incoming and outgoing)

► Potentially offering credit monitoring services
Prices hackers receive on the black market

<table>
<thead>
<tr>
<th>Item</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security number</td>
<td>$30</td>
</tr>
<tr>
<td>Date of birth</td>
<td>$11</td>
</tr>
<tr>
<td>Credentials</td>
<td></td>
</tr>
<tr>
<td>Health insurance</td>
<td>$20</td>
</tr>
<tr>
<td>Visa or Mastercard</td>
<td>$4</td>
</tr>
<tr>
<td>American Express</td>
<td>$7</td>
</tr>
<tr>
<td>Discover Card</td>
<td>$8</td>
</tr>
<tr>
<td>Credit card with mag strip or chip</td>
<td>$12</td>
</tr>
<tr>
<td>Bank account # (with $70 - $150k)</td>
<td>$300 or less</td>
</tr>
<tr>
<td>Full identity kit</td>
<td>$1,200 - $1,300</td>
</tr>
</tbody>
</table>

Source: Dell SecureWorks Reports (2013/2014)
Potential impact of a cyber event

- Costs of legal compliance
- Forensics, legal consultants
- Network damages and costs to repair or upgrade
- Business interruption
- Indemnify victims
And more potential impact of a cyber event

- Indemnify financial institutions
- Defense costs
- Injunctive relief
- Damage to shareholders
- Ticking time-bomb theory
Factors that decrease the cost of a data breach

- Strong security posture
- Incident response planning
- Business continuity management
- CISO appointment

Factors that increase the cost of a data breach

- Lost or stolen devices
- Third party involvement
- Notification before investigation completed

Source: 2014 Cost of Data Breach Study: Global Analysis
Sponsored by IBM, Conducted by Ponemon Institute LLC
Data Breach Life Cycle

Access the Problem
- Discover breach
- Contain losses, secure area
- Alert preparedness team
- Notify law enforcement
- Notify regulators

Engage External Resources
- Alert vendor
- Call forensics team
- Alert public relations (internal or external)

Comply with Notification
- Draft and send notification
- Active call center
- Public disclosure (if appropriate)

Manage Ongoing Business
- Continue assuring customers
- Continue data systems monitoring
- Resume business as usual
Information Security Incident Cycle

Preparation → Detection & Analysis → Containment Eradication & Recovery → Post-Incident Activity

How Do You Increase Security?

Conduct inventory of data

- What type of information do you process, transmit or store?
  - Personally identifiable information (PII)
  - Protected health information (PHI)
  - Payment Card Industry (PCI) information
  - Corporate confidential information
  - Employee information

- Where is the information stored?
  - Servers/devices onsite?
  - Services in the cloud?

- How is the information protected?
  - Is data encrypted?
  - Who has access?

- How long do you retain the information?
  - Do you have a data retention policy?
How Do You Increase Security?

Implement best practices

- Conduct inventory of all hardware and software
- Use current version of operating systems
- Automate security patching
- Enable intrusion detection and prevention systems
- Segment network
- Control access based on need to know
- Use multi-factor authentication

- Eliminate unnecessary data and processes
- Protect data
- Monitor endpoints
- Conduct due diligence on all third party service providers
- Conduct risk assessments
- Conduct vulnerability testing
- Develop incident response plan
- Test incident response plan with “tabletop” exercises
### Develop Incident Response Plan

#### Purpose
- Improve information security
- Prepare efficient, effective response to information security incident
  - Systematic
  - Minimal loss or theft
  - Minimal disruption
  - Legally compliant
  - Preserve reputation
- Collect evidence of attack
- Coordinate remediation
- Recover and restore information system

#### Key Team Members
- CISO/IT Lead
- Legal/Outside counsel
- Financial management
- Risk management
- Human resources
- Breach response vendors
  - Outside counsel
  - Forensics
  - Notification
  - Call center
  - Credit monitoring
  - Identity restoration
  - Public relations/crisis communications
**Establish Incident Response Team**

### Outside Counsel
- Project management skill
- Crisis management skill
- Breach response experience
  - Knowledge of breach notification requirements
  - Knowledge of privacy and security law
- Existing relationship
  - Engagement in place
  - Trusted partner
  - Knowledge of business
- Attorney/client privilege

### Breach Response Vendors
- MSAs in place
- Fewer decisions during digital crisis
- Reduced costs
- Instant response
- Existing relationship
  - Knowledge of network
  - Knowledge of vulnerability test data
  - Table top exercise partner
Preparation for a Breach: Cyber Insurance

- Your CGL policy does not cover data loss or “cyber” events ...
- What does your policy cover?
  - First party losses and costs?
  - Third party costs?
  - Remediation costs?
  - Fines and penalties?
  - Risk management services?
  - Selection of outside counsel?
  - Selection of breach responders?
  - Employee owned devices?
  - What is the retroactive date?
- Do the limits of liability match your realistic exposure?
The Initial Response to a Breach

- Conduct an assessment with CISO/IT Lead
  - If possible breach - implement incident response plan
- Notify insurer
  - Confirm approval of all breach response vendors
- Engage outside counsel
- Engage digital forensics team through outside counsel
- Implement litigation hold
- Begin to assess whether additional breach response vendors may be necessary
  - Public relations/crisis communications
  - Notification
  - Call center
  - Remediation services
Deploy forensics firm to assess, contain, eradicate, analyze and remediate
- Identify target of breach, i.e. PII, PHI, IP, PCI data, financial account information, etc.
- Determine whether data loss occurred; if so, whether it has stopped
- Eliminate threat
- Determine extent of loss

Preserve and secure evidence, including all log files

Recovery – return affected systems to normal operations
Post-incident Activity

- Determine whether to notify law enforcement
- Determine whether breach notification is required
  - If law enforcement is notified, and if breach notification is required, determine whether notification should be delayed pending law enforcement investigation
- If breach notification is required
  - Determine whether remediation services will be provided
  - Draft notification letters and frequently asked questions
  - Send notification letters to affected consumers and regulatory officials
- Prepare for post-incident regulatory response
- Conduct post-incident debrief
Key Takeaways

• Know your insurance program.
• Know your limits.
• Review policy and limits annually.
• Know how to report a claim.
• Know how to interact with the insurance company.
Key Takeaways (cont.)

• Every system is vulnerable.
• Bad guys are:
  – Persistent
  – Well-resourced
  – Increasingly sophisticated
• Increase your security system.
• Prepare for the inevitable incident.
Key Takeaways (cont.)

• Understand your exposure
  – Number and type of records

• Understand where data resides
  – Who has access

• Understand liability falls with the owner of the data

• Establish relationships externally or internally to prepare for pre and post breach
Question & Answer

Panel
Jason Glasgow, Travelers Insurance Company
T:(860) 277-4231 E:jglasgow@Travelers.com

Sean Hoar, Esq., Davis Wright Tremaine
T:(206) 622-3150 E:seanhoar@dwt.com

Andreas Kaltsounis- Stroz Friedberg
T:(206) 204-3616 E:akaltsounis@strozfriedberg.com

Timothy Wallach, Supervisory Special Agent, Cyber Task Force, FBI Seattle Division
1110 3rd Avenue, Seattle, WA 98101
T:(206) 287-3601 E:Timothy.Wallach@ic.fbi.gov

Moderator
Peter Marchel, Esq., Marchel & Associates Risk Consulting
T:(425) 788-4349 E:peterm@marchelassociates.com