Cyber Liability Security for Asset Managers

July 17, 2014
Agenda

- **Welcome and Panelist Introductions** – Richard Magrann-Wells, Senior Vice President, North American Financial Institutionals Group, Willis Group

- **SEC Cyber Liability Preparedness for Asset Managers** – Jay Gould and Brian Finch, Partners, Pillsbury Winthrop Shaw Pittman LLP

- **Technical and Administrative Safeguards** – Vinod Paul, Managing Director, EZ Castle Integration

- **Cyber Insurance** – Tom Srail, Senior Vice President, Willis Group

- **Q&A**
SEC Cyber Liability Preparedness for Asset Managers:
Jay Gould and Brian Finch, Partners

PILLSBURY WINTHROP SHAW Pittman LLP

© Pillsbury Winthrop Shaw Pittman LLP 2014
Identification of Risks and Cybersecurity Governance

Securities and Exchange Commission (“SEC”) will examine 50 registered brokers and investment advisers. The SEC will look at the frequency of actions, policies and procedures, responsible individuals and which portions of the business are included in the following actions:

- Inventories of the hardware and software systems.
- Review of location of customer data and who can access internally and externally.
- Risk assessments to identify physical and cybersecurity threats, vulnerabilities and potential business consequences.

SEC will look for:

- Written information security policy
- Business continuity plan that addresses mitigation of the effects of a cybersecurity incident.
- Any insurance that covers losses and expenses related to cybersecurity incidents.
Protection of Firm Networks and Information

- The SEC will review practices and controls regarding the protection of the firm’s networks and information that are used and the formal policies and procedures for:
  - Written guidance and training to employees
  - How data is handled and disposed of
  - If the firm maintains protection against Distributed Denial of Service (DDoS) attacks
  - Cybersecurity incident response policy

- Backup systems and encryption of data

- Audits of compliance with information security policies
Risks Associated With Remote Customer Access and Funds Transfer Requests

- If the firm offers online account access to customers, the SEC will examine:
  - Details on any third parties that manage account access
  - Information customers may access online and actions that may be taken by customers (transfers, withdrawals, information change, etc.)
  - Authentication process to access account online
  - Systems to detect anomalous transaction requests
  - PIN storage and protection
  - Information customers are given regarding reduction of cybersecurity risks

- If the firm accepts transfer requests by email, the SEC will examine how those requests are verified.

- The firm’s policies for addressing responsibility for losses associated with cybersecurity incidents.
Risks Associated With Vendors and Third Parties

- The SEC will examine the firm’s practices for conducting cybersecurity assessments of vendors and business partners who have access to the firm’s networks or data.

- If the firm includes cybersecurity-related requirements in its contracts with vendors and other third parties, the SEC will examine the details of those requirements.

- SEC will review training materials and policies and procedures related to information security that the firm supplies to vendors and third parties.
Detection of Unauthorized Activity

The SEC will review how and by whom the detection of unauthorized activity on its networks and devices with respect to:

- Assigning specific responsibilities for detection and reporting
- Aggregating and correlating event data
- Establishing written incident alert thresholds
- Monitoring the firm’s network and physical environment to detect potential cybersecurity events
- Detecting malicious code on the network and mobile devices
- Monitoring third party service provider activity on the networks
- Monitoring for unauthorized users, devices, connections and software
- Evaluating remotely-initiated transfer requests
- Using data loss prevention software and vulnerability scans
Other Focus Areas for Examination

- Updated supervisory procedures with Identity Theft Red Flag Rules.
- Records of actual cybersecurity incidents and related theft, losses, unauthorized exposure or unauthorized access to client information.
- Self-identification of cybersecurity losses and three most serious cybersecurity risks.
Pre and Post-9/11 Liability Concerns

Before 9/11, courts typically found that terrorist attacks were unforeseeable, terrorists were responsible for losses incurred, and that defendants did not owe any duty to protect potential defendants.

Post 9/11, courts have held the exact opposite, finding that terrorist attacks were reasonably foreseeable, and a duty was owed to the plaintiffs.

- The danger of a plane crashing as a result of a hijacking was “the very risk that Boeing should reasonably have foreseen.”
- Courts also have found that if a defendant “knew or should have known” of a threat, they have to take “reasonable” mitigation steps.
- Defined as steps could be ones that previously were considered “burdensome,” or even the most stringent of mitigation measures suggested in the course of a vulnerability assessment.
Why Would Plaintiffs Sue Cyber Security Providers and Other Victims?

- No real possibility of recovering from terrorists:
  - The widow of murdered journalist Daniel Pearl filed and quickly withdrew a lawsuit seeking damages against al-Qaida, a dozen reputed terrorists and Pakistan’s largest bank. *No defendants answered the claims.*

- Recover From State Sponsors?
  - Federal judge ordered Iran to pay $2.65 billion to relatives of American military personnel killed in a 1983 Beirut bombing in Lebanon. The judge acknowledged it was *a symbolic decision,* since Iran is estranged from the U.S. *and did not even respond to the lawsuit.*

- That leaves security providers and property owners as the deep pockets.

- Remember – litigation will happen. Families of 9/11 victims pursued claims despite strong.
Cyber Data Breaches – Why Attack?

- Not if, not when, *but how often*.
- Disruption/destruction of operations or data, theft of corporate secrets, trade secrets, other proprietary information.
- Remember, attacks are CHEAP:
  - $2/hour for denial of service attack; $30 to check against standard anti-virus programs;
  - $5,000 for a “zero day” attack program;
  - 70% of newly created viruses only used once or twice.
- So many ways in, impossible to stop them all.
- CONSEQUENCES: Lost IP, lost contracts, acquired vulnerabilities.
Consider The SAFETY Act To Protect Investment Value

“Support Anti-Terrorism by Fostering Effective Technologies Act”.

Eliminates or minimizes liability for sellers of DHS-approved security products/services should suits arise after an attack (physical or cyber), including:

- SAFETY Act protections obtained only submitting an application to DHS.
- Protections apply even if approved technologies are sold to commercial customers, if the cyber attack occurs abroad, and to products/services deployed solely for internal use.

SAFETY Act uses the term “act of terrorism”, but:

- Broadest definition in the U.S. Code of “terrorism”
- Applies essentially to any unlawful act causing harm (including financial) in the U.S.
- NO NEED TO LINK TO A TERRORIST GROUP or show TERRORISTIC INTENT.
SAFETY Act: Designation vs. Certification

- Two levels of protection under the SAFETY Act, Designation and Certification.

- Under “Designation”:
  - Claims may only be filed in Federal court.
  - Damages are capped at a level set by DHS.
  - Bar on punitive damages and prejudgment interest.

- Certification offers all the same defenses PLUS presumption of immediate dismissal.

- In both circumstances claims against CUSTOMERS are to be immediately dismissed.
How Does The SAFETY Act Help?

- Reduces potential exposure of companies to liability post-significant cyber or physical event.
- Provides third party validation of the company’s product/service offerings.
- Increases potential market share (many customers are requiring vendors to hold SAFETY Act protections).
- SAFETY Act awards can serve as evidence of effectiveness and potential revenue growth during the due process phase.
- The cost of obtaining SAFETY Act protections is MINIMAL.
## SAFETY Act vs. Cyber Insurance

<table>
<thead>
<tr>
<th>SAFETY Act</th>
<th>Cyber Insurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Jurisdictional defenses (Federal Ct., no punitive damages, no prejudgment interest).</td>
<td>- Reimbursement for damages, but no cap.</td>
</tr>
<tr>
<td>- Cap on third-party damages.</td>
<td>- No jurisdictional defenses.</td>
</tr>
<tr>
<td>- Possible immunity.</td>
<td>- No government “sanction” of security plans and technologies.</td>
</tr>
<tr>
<td>- Government “endorsement” of security plans and technologies.</td>
<td>- Less certainty as to coverage.</td>
</tr>
<tr>
<td></td>
<td>- Tying SAFETY Act to cyber insurance can result in reduced premiums.</td>
</tr>
</tbody>
</table>
A Look at Technical & Administrative Safeguards
Vinod Paul, Managing Director

EZECASTLE INTEGRATION

© EzeCastleECI 2014
Technology Best Practices

- Principle of Defense in Depth
- Principle of Least Privilege
- Secure User Authentication Protocols
- Audit & Logging
Principle of Defense in Depth

- Multiple layers of security employed simultaneously

Engage real-time Intrusion Detection/Mitigation Solutions

- Track and monitor network activity including intrusions, attacks, and the accessing of sensitive data
Principle of Least Privilege

- **Establish privileged access to core data**
  - Limit access to only those who need it
  - Don’t place highly confidential content on unprotected servers

- **Implement restriction policies**
  - Access control lists on all applications and data
    - Who has access to what? Keep an authentication/access log
  - Inbound/Outbound Internet Access Control lists
  - Use of audited OTPs (one-time-passwords) & minimum-privilege shared accounts
Establish Secure User Authentication Protocols

- Assign unique domain user IDs to each employee
- Enforce strong domain password policies
- Control data security passwords
  - Ensure they are kept in a location and/or format that does not compromise the security of the data they protect
- Restrict access to active users and active user accounts only
Monitor, Audit and Logging Network Activity

- **Central logging system that records:**
  - All login/logout events
  - Inbound/outbound connections through Internet-facing firewalls
  - Email and network traffic

- **Perform a Vulnerability Assessment**
  - Verify firewall configuration and anti-virus patching, network device security and evidence of malicious activity
Beyond Technology

- Developing Written Information Security Plans:

  - Where is data located?
  - Who has access to what information?
  - What incident response procedures are in place?
  - How is data protected?
  - What are employees’ responsibilities?
Security Plan Components

- Developing Written Information Security Plans:

  - Where is data located?
  - Who has access to what information?
  - How is data protected?
  - What are employees’ responsibilities?
  - What incident response procedures are in place?
Security Plan Components

Developing Written Information Security Plans:

- Administrative Safeguards
  - Where is data located?
  - Who has access to what information?
  - What incident response procedures are in place?
  - How is data protected?
  - What are employees’ responsibilities?
Security Plan Components

- Developing Written Information Security Plans:

  - Administrative Safeguards
    - Where is data located?
    - Who has access to what information?
    - What incident response procedures are in place?
    - How is data protected?
    - What are employees’ responsibilities?
Security Plan Components

- Developing Written Information Security Plans:

- Where is data located?
- Who has access to what information?
- What incident response procedures are in place?
- How is data protected?
- What are employees’ responsibilities?
Security Plan Components

- Developing Written Information Security Plans:

  - Where is data located?
  - Who has access to what information?
  - What incident response procedures are in place?
  - How is data protected?
  - What are employees’ responsibilities?
SAFETY Act vs. Cyber Insurance

Technical Safeguards
- Principle of Defense in Depth
- Penetration Testing
- Audit & Logging
- Vulnerability Assessments
- Firewalls
- Strong Passwords, Access Controls and Documentation

Administrative Safeguards
- Policy for data protection, access and location
- Incident Response Plan
- Incident Communications Procedures
- Employee Training and Responsibility Definition
Additional Resources

Critical Cybersecurity Threats & How to Prepare in 2014

Security Incident Response Priorities

Protecting Your Assets: How to Safeguard Your Firm Against Cybersecurity Attacks

Hedge IT Blog
Cyber Liability Insurance for Asset Managers
Thomas Srail, Technology, Media and Telecom Practice Leader
WILLIS NORTH AMERICA
“Cyber” Insurance Timeline

1996
- HIPAA

1998
- GLB

2000
- SB1386

2002
- PCI

2004
- Card Systems

2006
- TJX

2008
- Heartland

2010
- SEC

2012
- Sony

2014
- Target

- Insurance History
- Regulatory/Industry History
- Claims/Losses History
Privacy/Data Risk

What Data do you collect?
- Personally Identifiable Info. (PII)
- Protected Health Info. (PHI)
- Credit/Debit Card Numbers (PCI)

Where is it?
How well is it protected?
How long do you keep it?

What is a Breach?
- Unauthorized disclosure
- Unauthorized acquisition
- Data compromised
What is Different Today?

Familiar mediums

- SQL injections; spear phishing; malware, spyware & ransom-ware (“CryptoLocker”); denial of service attacks; web site defacing

New culprits

- Loosely formed groups of people who are very good at hacking and work together to do so (e.g., Anonymous, Lulzsec)

- State actors (China, Iran, US, Israel, Russia)

New information targeted

- Corporate data and trade secrets; inside information; embarrassing information; corporate weaknesses
What is Different Today?

New targets
- Cars
- Smartphones
- Medical devices

New motives
- Political, ideological, personal, war/terrorism, revenge
- “Hacktivism”
Traditional Insurance Gaps

- Theft or disclosure of third party information (GL)
- Security and privacy – “Intentional Act” exclusions (GL)
- Data is not “tangible property” (GL, Prop, Crime)
- Bodily Injury & Property Damage triggers (GL)
- Value of data if corrupted, destroyed, or disclosed (Prop, GL)
- Contingent risks (from external hosting, etc.)
- Commercial Crime policies require intent, only cover money, securities and tangible property.
- Territorial restrictions
- Sublimit or long waiting period applicable to any virus coverage available (Prop)
# Example of Gaps in Traditional Insurance

## 1st Party Network Risks

<table>
<thead>
<tr>
<th>Physical damage to Data</th>
<th>Virus/Hacker damage to Data</th>
<th>Denial of Service attack</th>
<th>B.I. Loss from IT security breach</th>
<th>IT Extortion or Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>In some policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## 3rd Party Privacy/Network

<table>
<thead>
<tr>
<th>Theft/disclosure of data</th>
<th>Administrative privacy breach</th>
<th>Technology E&amp;O</th>
<th>Media Liability (electronic content)</th>
<th>Privacy breach expense/notification</th>
<th>Damage to 3rd party’s data</th>
<th>Regulatory Privacy Defense/Fines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Coverage Provided

- **Coverage Provided**
- **Limited Coverage**
- **No Coverage**
Cyber Policy Construction

How a Cyber Policy is Constructed

- **Basic forms usually include:**
  - Privacy Expenses (e.g. Notification, Forensics, Credit Monitoring)
  - Privacy/Security Liability
  - Electronic/Internet Media Liability

- **Standard options for:**
  - Extortion
  - First Party Business Income Loss and Data Restoration Costs
  - Full Media

- **Other possible options:**
  - System Failure
  - Technology Liability
Cyber Insurance Markets

A Mature Market

- Over 60 insurers writing coverage
- Substantial claims paid without insurers withdrawing from market
- Recognized underwriting standards
- Estimated $600M+ premium volume stand alone and blended with E&O
- Over 150 Fortune 500 companies of the 300 significantly exposed buy

Sample Markets

<table>
<thead>
<tr>
<th>ACE</th>
<th>Travelers</th>
<th>Navigators</th>
</tr>
</thead>
<tbody>
<tr>
<td>AXIS</td>
<td>Chubb</td>
<td>One Beacon</td>
</tr>
<tr>
<td>Beazley</td>
<td>Catlin</td>
<td>RLI</td>
</tr>
<tr>
<td>AIG</td>
<td>HCC</td>
<td>Swiss Re</td>
</tr>
<tr>
<td>Zurich</td>
<td>Torus</td>
<td>Freedom Speciality</td>
</tr>
<tr>
<td>C.N.A.</td>
<td>Ironshore</td>
<td>XL</td>
</tr>
<tr>
<td>AWAC</td>
<td>Liberty</td>
<td>London Markets</td>
</tr>
</tbody>
</table>
IT Risk Mitigation Steps

- **Risk Assessments (ISO 27005, NIST 80-30, ITGI, etc.)**

- **Internal and Independent Testing**
  - Vulnerability Analysis (network, application, database)
  - Penetration Testing (same, plus client-side)
  - Controls Testing (SAS 70, COBIT)

- **Implement, Test and Continuously Improve**
  - Data Classification and Protection Measures
  - Training and Awareness
  - Logging and Monitoring
  - Patch/Configuration Management
  - Network, Server and Endpoint DLP
  - Antivirus, IDS/IPS, Proxies, DAM
Best Practices

- Maintain a Risk Transfer Instrument
- Have a Proper Background Screening Program for new hires and vendors.
- Pre-arrange a Breach Service Provider, Outside Counsel and Reputational Risk Advisor
  - All specializing in Privacy Law and Breach Crisis Management
- Provide “Certification” through e-Learning to employee base on safeguarding data
  - #1 preventative initiative being adopted by CISOs and CPOs in 2010 (as per Ponemon 2011 Study)
- Develop an Incident Response Plan (required on several federal and state fronts – HTIECH, MA201, et al.)
  - Internal Staff, Outside Counsel, Reputational Risk Advisor, Breach Service Provider
- Conduct annual Risk Assessments and Tabletop Exercises
Best Practices

- Hold an internal “Privacy Summit” to identify vulnerabilities
  - Risk, Compliance and Privacy, HR, Legal, IT, C-level representation (CFO), Physical Security / Facilities – “Technology, Processes and People.”

- Keep General Counsel’s office current to state disclosure laws, federal regulations, foreign requirements and updates
Common Cyber Exclusions

- Known Claims/Prior Acts
- Bodily Injury/Property Damage
- Patent/Trade Secret (Insured’s)
- Intentional Criminal/Dishonest Acts (severability)
- Maintain Reasonable Security (rare)
- Breach of Contract
- Governmental action
- Insured vs. Insured
- War
Coverage Enhancements to Consider

- Choice of Counsel
- Coordinated Retention Endorsement (only one retention will apply to the entire policy)
- Prior Acts coverage (difficult to obtain)
- Wrongful collection coverage
- Privacy regulatory fines/penalties (still not included under all standard forms)
- First-Party contingent/dependent Business Interruption (still not included under all standard forms)
- First-Party coverage for insured’s negligence that cause system interruption resulting in loss of income – sometime termed “system failure”
- Cyber Terrorism Coverage and carve back to war exclusion
- Tight control group (management committee, CFO, GC) around intentional acts exclusion to ensure rogue employees are covered
- Amend “Other Insurance” clause to coordinate with professional liability insurance and any other relevant policies
Coverage Limitations to Avoid

- Narrow definition of personal identifiable information
- Unencrypted laptop or mobile device exclusion
- Limitations on coverage for data not on insured’s system – first and third party – cloud providers or other outsource vendors
- Wild virus exclusion
- Limitations on voluntary privacy breach notification or credit monitoring costs
- Coverage for breach of US privacy statutes or regulations only
- Inadequate sublimits for forensics
- Insurer requirements to use specified vendors unless favorable rates are offered and such vendors are acceptable to the insured
- First-party contingent/dependent Business Interruption sublimit of $100k
# Speaker Contact Information

<table>
<thead>
<tr>
<th>Willis</th>
<th>Pillsbury Winthrop Shaw Pittman LLP</th>
<th>EZ Castle Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Richard Magrann-Wells</strong></td>
<td><strong>Brian Finch</strong></td>
<td><strong>Vinod Paul</strong></td>
</tr>
<tr>
<td>Senior Vice President</td>
<td>Partner</td>
<td>Managing Director</td>
</tr>
<tr>
<td><a href="mailto:richard.magrann-wells@willis.com">richard.magrann-wells@willis.com</a></td>
<td><a href="mailto:brian.finch@pillsburylaw.com">brian.finch@pillsburylaw.com</a></td>
<td><a href="mailto:vpaul@eci.com">vpaul@eci.com</a></td>
</tr>
<tr>
<td>212 915 8357</td>
<td>202-663-8062</td>
<td>212 954-0641</td>
</tr>
<tr>
<td><strong>Jay Gould</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partner</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:jay.gould@pillsburylaw.com">jay.gould@pillsburylaw.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>415-983-1226</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Tom Srail</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Senior Vice President</td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="mailto:tom.srail@willis.com">tom.srail@willis.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>216-357-5997</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Title</td>
<td>Email</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>Nicole Segal</td>
<td>Senior Vice President</td>
<td><a href="mailto:nicole.segal@willis.com">nicole.segal@willis.com</a></td>
</tr>
<tr>
<td>Shahri Griffin</td>
<td>Senior Vice President</td>
<td><a href="mailto:shahri.griffin@willis.com">shahri.griffin@willis.com</a></td>
</tr>
</tbody>
</table>