CYBER RISK AND CORPORATE GOVERNANCE
WEF GLOBAL RISKS: CYBER

Risk Interconnections Map

- Data fraud/theft
- Organized crime and illicit trade
- Global governance failure
- Cyber attacks
- Terrorist attack
- Critical information Infrastructure breakdown

Introduction

Discovery

- Actual or alleged theft, loss, or unauthorized collection/disclosure of confidential information that is in the care, custody, or control of the Insured, or a 3rd for whom the Insured is legally liable.

**Discovery can come about in several ways:**
- Self discovery — usually the best case.
- Customer inquiry or vendor discovery.
- Call from regulator or law enforcement.

First Response

- **Forensic Investigation and Legal Review**
  - Forensic tells you what happened.
  - Legal sets out options/obligations.

External Issues

- Public Relations
- Notification
- Remedial Service Offering

Long-Term Consequences

- Income Loss
- Damage to Brand or Reputation
- Regulatory Fines, Penalties, and Consumer Redress
- Civil Litigation

CYBER RISK AND CORPORATE GOVERNANCE

SIMPLIFIED DATA BREACH TIMELINE
A SNAPSHOT OF DATA BREACHES IN 2012

- 621 confirmed data breaches
- 47,000+ reported security incidents
- 44 million or more compromised records

- 78% took weeks or longer to discover
- 75% driven by financial motives
- 78% of initial intrusions rated as “low difficulty”
- 92% from external hackers

Source: Verizon 2013 Data Breach Investigations
ECONOMIC COST OF CYBER CRIME

Source: McAfee and the Center for Strategic and International Studies

Between $24 billion and $120 billion.

Between $300 billion and $1 trillion.

• Costs include:
  - Loss of intellectual property.
  - Loss of sensitive business information (such as negotiating strategies).
  - Additional costs of securing exposed networks.
  - Reputational damage.

Source: McAfee and the Center for Strategic and International Studies
### Top Consumer Complaints in 2011

<table>
<thead>
<tr>
<th>Rank</th>
<th>Category</th>
<th>No. of complaints</th>
<th>Percentage of complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Identity theft</td>
<td>279,156</td>
<td>15%</td>
</tr>
</tbody>
</table>

Identity theft has been the No. 1 complaint to the FTC since 2000.

Source: Federal Trade Commission
“The FTC recognizes that even a strong information security policy will sometimes fail; for that reason, the FTC will close investigations without violations when it finds that the policies in place were reasonable, even when a breach has occurred.”

— Jon Leibowitz, former FTC Chairman; Partner at Davis Polk Wardwell
WHO IS INVOLVED IN IDENTIFYING, PRIORITIZING AND ASSESSING RISKS?

• **Federal Trade Commission (FTC):** Mandates cyber practices on specific companies through enforcement actions which set standards within industries.

• **Securities and Exchange Commission (SEC):** CF Disclosure Guidance S-K (Oct 2011) clarifies that enforcement actions can compel the adoption of cyber practices.

• **State Attorneys General:** 47 States have data breach laws.

• **National Institute of Standards and Technology/ Department of Homeland Security (NIST/DHS):** Executive Order 13636 (Feb 2013) mandates a cyber standards “baseline” for critical infrastructure.

• **Federal Energy Regulatory Commission (FERC):** Has proposed regulations for cyber security of the bulk electric system.

• **Government Services Administration (GSA):** Requires cyber security standards for federal government contracts.


• **Department of Health and Human Services (HHS):** Assesses fines under the Health Insurance Portability and Accountability Act of 1996 and HIPAA HITECH.
• Disclosure triggers.
  – A key concern is the adequacy of a company’s disclosures to shareholders related to cyber
    security risks and cyber incidents.
• Likelihood of cyber incidents.
  – Prior cyber incidents and their severity and frequency are relevant.
• The financial impact of potential cyber incidents on an organization could include:
  – Remediation costs.
  – Additional security implementation costs.
  – Lost revenue.
  – Reputational damage / loss of customers.
  – Litigation / regulatory actions.
• Adequacy of preventative measures to reduce cyber security risks
• Materiality threshold — cyber risks that could materially impact financial performance.
CYBER RISK AND CORPORATE GOVERNANCE
SEC NOTICE

• SEC notice goes beyond personal information security breaches to consider:
  – Business interruption caused by a cyber incident.
  – Theft of intellectual property due to poor security and impact on organization.
• Purpose of disclosure is financial decision making.
• Some breaches are not material.
• Past breaches may not be indicative of future risk.
• Reporting and analysis is just as concerned with prevention/containment as with threats and incidents.
• Disclose the nature of the cyber security risk and how it impacts organization.
• Business and operations causing material cyber risk and potential costs and consequences, including consideration of outsourced functionalities.
• Prior cyber incident history, including costs and consequences.
• Description of relevant insurance coverage for cyber.
• No need to make disclosures that would compromise the organization’s security.
• Disconnect between security risk assessment and financial impact assessment.
• Security risk is complex, widespread, technical, and ever-changing. As a result, it is difficult to quantify probability.
  – There is little data.
  – Industry standards and security assessments should be considered.
  – Risk assessment needs to be almost “real time.”
  – Hard to know impact of preventative measures in reducing risk.
• Chief Financial Officer and Chief Security Officer collaboration required.
• Information flow up to the board is required.
• Nexus between risk of security incidents and financial impact needs to be clearly articulated to the board.
  – Worst case scenarios should be considered.
  – Policies and procedures should allow for communications to be understood by the board.
  – This is not an IT issue for the board.
## CYBER RISK AND CORPORATE GOVERNANCE
### INSURANCE COVERAGE

<table>
<thead>
<tr>
<th>RISKS</th>
<th>COVERAGE</th>
<th>TRADITIONAL POLICIES</th>
<th>CYBER &amp; PRIVACY POLICY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal liability to others for privacy breaches</td>
<td>Privacy Liability: Harm suffered by others due to the disclosure of confidential information</td>
<td>Typically covered</td>
<td>Not typically covered</td>
</tr>
<tr>
<td>Legal liability to others for computer security breaches</td>
<td>Network Security Liability: Harm suffered by others from a failure of your network security</td>
<td>Typically covered</td>
<td>Not typically covered</td>
</tr>
<tr>
<td>Loss or damage to data/information</td>
<td>Property Loss: The value of data stolen, destroyed, or corrupted by a computer attack</td>
<td>Typically covered</td>
<td>Not typically covered</td>
</tr>
<tr>
<td>Loss of revenue due to a computer attack</td>
<td>Loss of Revenue: Business income that is interrupted by a computer attack</td>
<td>Typically covered</td>
<td>Not typically covered</td>
</tr>
<tr>
<td>Extra expense to recover/respond to a computer attack</td>
<td>Cyber Extortion: The cost of investigation and the extortion demand</td>
<td>Typically covered</td>
<td>Not typically covered</td>
</tr>
<tr>
<td>Loss or damage to reputation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identity theft</td>
<td>Expenses resulting from identity theft</td>
<td>Typically covered</td>
<td>Not typically covered</td>
</tr>
<tr>
<td>Privacy notification requirements</td>
<td>Cost to comply with privacy breach notification statutes</td>
<td>Typically covered</td>
<td>Not typically covered</td>
</tr>
<tr>
<td>Regulatory actions</td>
<td>Legal defense for regulatory actions</td>
<td>Typically covered</td>
<td>Not typically covered</td>
</tr>
</tbody>
</table>
CYBER RISK AND CORPORATE GOVERNANCE
CYBER LIABILITY PURCHASING BY SIZE AND INDUSTRY

PERCENT INCREASE IN 2013 OF CLIENTS PURCHASING CYBER LIABILITY INSURANCE

- Significant difference between how a small or midsize enterprise approaches insurance and how a large organization does.
  - For example:
    - Control.
    - Mechanics.

- Cyber policies now have provisions covering nearly every aspect of an organization’s response to an actual or perceived breach.
- Markets have moved beyond simple risk transfer, providing loss prevention and risk mitigation tools.

Source: Marsh Global Analytics
Recent shareholder actions have followed closely upon the heels of a disclosed data breach. SEC disclosure did not create new rules; it did create an ersatz standard for what a company needs to do to “properly” notify the financial community of a material cyber event. In the context of a company failing to manage a business risk and then failing to properly disclose it: D&O 101. The D&O policy will respond just as it would had the event not been shrouded by cyber jargon.
CYBER RISK AND CORPORATE GOVERNANCE

ANALYTICS

• Amassing data that now can be used as predictive and loss modeling.
• Not just about privacy — data looks at the probability and severity of technology risk as it relates to supply chain disruption.
• Loss modeling and risk mapping allows a company to get a clear sense of the scope and breadth of the risk as opposed to just a sense of what a policy will cost.
• Understanding the risk is now more of an analytical exercise than when cyber insurance first debuted nearly two decades ago.
• Risk managers need to be able to demonstrate to the board that they have taken a reasoned approached to evaluating and understanding the risks.
• Analytics can help the board:
  – Understand the company relative to a common information security standard.
  – Map out the key risks.
  – Model the financial impact of loss scenarios.
  – Place those scenarios and risks in the context of the company’s risk transfer portfolio.
• Continue to see insurers grow their loss prevention and loss mitigation services for midsize companies.
• Insurers have to come to terms with social media/networking.
• Common analogy: Cyber insurance is traveling a path not dissimilar from EPLI market.
• Cyber risk is not going away.
• For every market that has hesitated to move forward, another has stepped in.
CYBER RISK AND CORPORATE GOVERNANCE
THE BOARD’S ROLE IS CRITICAL

“Until such time as cyber security becomes a regular board of director's agenda item...the potential for disruption is real and serious and we all pay the price.”

— Howard A. Schmidt, former Cyber Security Coordinator for President Obama