Presentation for the
Connecticut Chapter of the
Turnaround Management Association

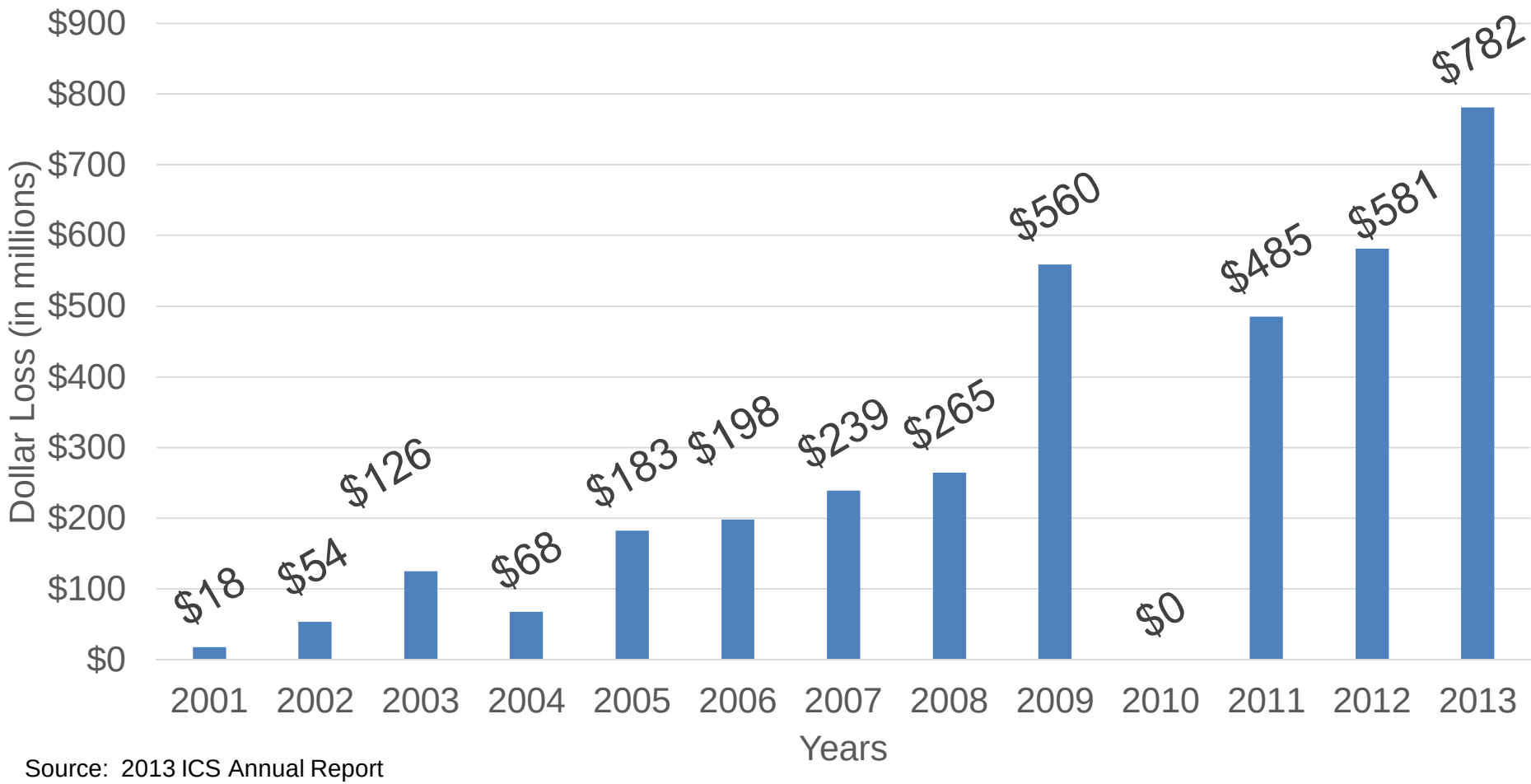
Cyber Security: What Every Turnaround Manager Should Know

DAY PITNEY LLP

Tales from a hacker:

Michelle D. Syc
Senior Analyst, Advisory & Assurance Services
ADNET Technologies, LLC
(860) 409-1738
MSyc@thinkADNET.com

Cybercrime Loss Snapshot



Source: 2013 ICS Annual Report

The Underground Economy: What is your data worth?

Product	Price (US Dollars)
Business Application Credentials	$155 - $193
Credit Card Credentials	$35-$135
Online Service Account Credentials	$20
List of mobile phone numbers	$290 - $1,236
List of landline phone numbers	$317-$1931

Source: Trend Micro Global Black Market Prices as of February 2015 / Note: based on Brazilian Underground Economy

Managing Cyber Risks:
A Legal Perspective

Richard D. (“Rick”) Harris, Esq.
Partner
Day Pitney LLP
One Audubon Street, New Haven, CT
(203) 752-5094
rdharris@daypitney.com

DAY PITNEY LLP

Overview

- What business assets are most at risk from cyber threats?
- The increasing significance of intangible assets for business valuation.
- Common sources of cyber threats.
- Guidance for corporate management.

What business assets are most at risk from cyber threats?

- **"Intellectual Property"** means "creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce." Types of intellectual property include copyrights, patents, trademarks, industrial designs, and trade secrets. –World Intellectual Property Organization ("WIPO")

- **"Trade Secret"** is broadly defined in the U.S. Economic Espionage Act as: *"All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, analyses, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public."* (i.e., anything from customer lists to manufacturing processes)

- **"Good Will"** is the established reputation of a business regarded as a quantifiable asset, e.g., as represented by the excess of the price paid at a takeover for a company over its fair market value.

Requirements for preservation of trade secrets

- Followed by 47 states and several U.S. Territories, the Uniform Trade Secrets Act protects from misappropriation "information, including a formula, pattern, compilation, program, device, method, technique, or process, that (1) derives independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

- Under the Restatement of Torts, whether certain information constitutes a trade secret depends on six factors:
  1. The extent to which the information is known outside the business
  2. The extent to which it is known by employees and others involved in the business
  3. The extent of measures taken by the claimant to guard the secrecy of the information
  4. The value of the information to the business and its competitors
  5. The amount of effort or money expended by the business in developing the information
  6. The ease or difficulty with which the information could be properly acquired or duplicated by others.

- Bottom Line: Trade secrets must be kept **"secret."**

Increasing significance of intangible assets for business valuation

- Intangible assets are more valuable today than ever before as industries increasingly rely on intangible assets both as a important business tools and, in some cases, as the exclusive value of the industry (*ex.*, software, pharmaceutical, and Internet-based industries).

- "As the United States continues its shift to a knowledge- and service-based economy, the strength and competitiveness of domestic firms increasingly depends upon their know-how and intangible assets."

–The Congressional Research Service

Notable Statistics

- A study by the Federal Reserve System found that in the 1990s, U.S. business spending on knowledge capital, including computerized information, scientific and creative property, and economic competencies, grew faster than any other form of business or personal spending.

- In 2007, estimates put the value of U.S. intellectual property at between $5 trillion and $5.5 trillion. This is equal to approximately 45 percent of U.S. GDP and exceeds the GDP of any other nation worldwide.

- It is estimated that U.S. businesses invest about $1 trillion a year on idea-related intangibles (this is approximately equivalent to spending on traditional tangible capital).

- Among the S&P 500, intangible assets comprised just 17% of the total value of the company in 1975. By 2009, this figure had increased to 81%.

Common Sources of Cyber Threats

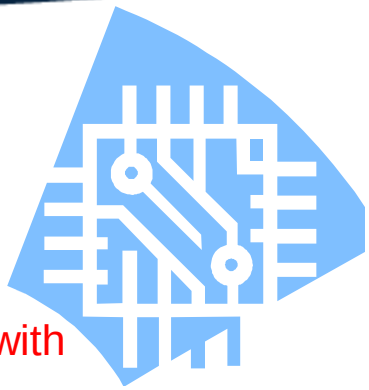
- Widespread data storage via computer networks and clouds makes it more difficult than ever for companies to guard their intellectual property, and experts have identified the theft of trade secrets as "one of the major cybersecurity risks of our time." –Scholl and Bahou, ISSA

- In 2013, theft of intellectual property was estimated to cost U.S. organizations nearly $300 billion per year.

- In 2009, McAfee estimated that over $1 trillion was spent on data leaks among companies worldwide.

- Theft of IP may not be immediately discovered. "Outside attackers burrow into company networks and remain undiscovered for months or even years. It is much like having termites in your house—often, by the time you discover them, the damage is done." - Robert S. Mueller, III, FBI Director

Common Sources of Cyber Threats



- Insider Threats:
  - Current and former employees are the group most often associated with misappropriation of trade secrets.
  - **Example**: In 2007, former research scientist Gary Min was sentenced to 18 months in prison for theft of IP. As a disgruntled employee of E.I. du Pont de Nemours and Company, Min downloaded $400 million worth of information describing product lines (like Kevlar and Teflon) from company servers before leaving the company. He had downloaded the material to a laptop issued by his new employer and intended to take the information overseas.

- Threats from Third Parties:
  - "Cyber Espionage" for the benefit of foreign governments and competitors.
  - In 2013, an Annual Report by Verizon found that out of 621 data breach cases reviewed, 19% of all attacks studied were conducted by "state-affiliated actors."

Common Sources of Cyber Threats (cont.)

- One study found that in cyber breach cases where the intrusions were traced to Chinese hackers, ninety-four percent of the targeted companies did not know of the breach until a third party informed them. The median time between intrusion and detection was over a year.

- **Example:** In 2011, Xiang Dong "Mike" Yu, a former project engineer for the Ford Motor Company, was sentenced to nearly six years in prison for downloading information worth between $50 million and $100 million onto an external hard drive and taking it to a Chinese competitor.

- Threats *through* Third Parties
  - Although the infamous Target Breach did not involve the theft of intellectual property, it is still instructive with regard to potential threats to IP and trade secrets.
  - 11 GB of data stolen from Target in December 2013.
  - The attackers hacked into a third party vendor to obtain credentials to access Target's corporate network.

Guidance based on Securities Laws

- In October 2011, the SEC released guidance stating that, although no existing federal disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, a number of disclosure requirements may impose an obligation on issuers to disclose such risks and incidents.

- For example, the SEC stated that issuers should disclose the risk of cyber incidents to investors if these issues make an investment in the company speculative or risky.

Guidance based on Securities Laws (cont.)

- Depending on the issuer's particular facts and circumstances, and to the extent material, appropriate disclosures may include:
  - Discussion of aspects of the issuer's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
  - To the extent the issuer outsources functions that have material cybersecurity risks, description of those functions and how the issuer addresses those risks;
  - Description of cyber incidents experienced by the issuer that are individually, or in the aggregate, material, including a description of the costs and other consequences;
  - Risks related to cyber incidents that may remain undetected for an extended period; and
  - Description of relevant insurance coverage.

Guidance based on Securities Laws (cont.)

"Board oversight of cyber-risk management is critical to ensuring that companies are taking adequate steps to prevent, and prepare for, the harms that can result from such attacks. There is no substitution for proper preparation, deliberation, and engagement on cybersecurity issues. Given the heightened awareness of these rapidly evolving risks, directors should take seriously their obligation to make sure that companies are appropriately addressing those risks." **–Commissioner Aguilar, SEC**

- Place information about cyber security on the board's agenda.
- Assign information security to a key committee, and ensure adequate support for that committee.
- Identify information security leaders, hold them accountable, and ensure support for them.
- Ensure the effectiveness of the corporation's policy through review and approval.
- Clearly communicate the board's commitment to information security.
- Ask management to give specific reports on information security risks, incidents, and activities.
- Devote more audit committee time to addressing information security risks.

Guidance based on state laws

Create a Written Information Security Program (“WISP”)

1. Designate an employee with privacy and security management oversight responsibilities.
2. Identify all reasonably foreseeable risks to security, confidentiality, and integrity of personal information and related systems.
3. Design and implement safeguards to control the identified risks.
4. Train staff to implement the program.
5. Arrange for an independent party to test and monitor the safeguards' controls, systems, policies, and procedures.
6. Oversee third-party service providers with access to customer information.
7. Regularly evaluate and adjust the program.
8. Design and implement policies and procedures for responding to an incident.
9. Provide the board of directors with an annual assessment of the program.
10. Plan for compliance with applicable state “breach notification” statutes

Guidance based on state laws (cont.)

- Comply with breach notification statutes
  - E.g. Conn. Gen. Stat. 36a-701b
- Comply with pre-existing privacy policies
  - Website privacy policies
  - Policies required by state laws regarding safeguarding of sensitive personal information (e.g., Conn. Gen. Stat. 42-471)
- Comply with Payment Card Industry (PCI) Data Security Standard
- Comply with other contractual obligations
- Comply with industry specific requirements (Finance, Healthcare, etc.)

Other Recommendations for Managers

1. **Employment policies,** including background checks and carefully considered termination policies. Other examples: Training new hires to promote company policies; revoking departing employees' access to information; conducting exit interviews requiring statement that departing employee has not taken any confidential or proprietary information.
2. **System Access Agreements and NDAs** for both employees and third party vendors.
3. **Oversight** of service providers, including (i) Taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect proprietary information; and (ii) Requiring such third-party service providers by contract to implement and maintain such appropriate security measures.
4. **Computer security** should at a minimum include passwords and firewalls. Electronically stored information should be classified and compartmentalized, with access granted on a need-to-know basis. Physical access to any network or data centers should also be restricted.

Consider Cyber-Insurance

Managing Cyber Risk: Cyber Liability Insurance Policies

Michael Vitulli
Senior Vice President
Risk Strategies Company
160 Federal Street
Boston, MA 02110
(617) 330-5726
Mvitulli@risk-strategies.com

Cyber Liability Policies

Those policies typically offer a menu of coverages. Insurance buyers can find coverage for their costs to:

- Forensic Investigation – Indemnify costs to determine scope and cause of breach.
- Crisis Management Expenses – Indemnify costs associated with hiring a PR firm to mitigate negative publicity after a breach., including costs for consumer education and assistance Many policies now cover the cost of retaining outside counsel to evaluate the firm's potential obligations for a breach.
- Privacy Breach Notification Costs – Indemnify legal fees and costs (including mailing expenses) to notify customers of a privacy breach.
- Credit Monitoring Costs – Indemnify costs to monitor affected individuals for identity theft.
- Cyber Extortion – Indemnify costs to manage the threat to commit an attack against an insured's computer system or to disclose personally identifiable information obtained through a security breach.
- Business Interruption – Costs associated with interruption of the insured's normal business activities due to a network security breach.
- Data Restoration – Funds to recover or restore data that is damaged, altered, destroyed, stolen, or misused by a covered cause of loss.
- Defense of Claims – Indemnify costs to defend against subsequent regulatory actions and consumer, corporate and investor lawsuits.
- System Remediation – Indemnify costs to harden the breached data security system against future attacks.

Policies Where Some Coverage MAY Exist

- Directors & Officers
  - Coverage for shareholder suits in the event of a data breach (Target)
- Property
  - Positive coverage grants for data destruction
- General Liability
  - ISO, the organization that issues standard policy forms for insurers, recently issued a standard endorsement to exclude cyber from the CGL policy, and carriers are starting to use this more and more
- Package
  - Some small sublimits can be provided
- Errors & Omissions
  - Professional liability policies often provide some element of Cyber coverage as a “Module”

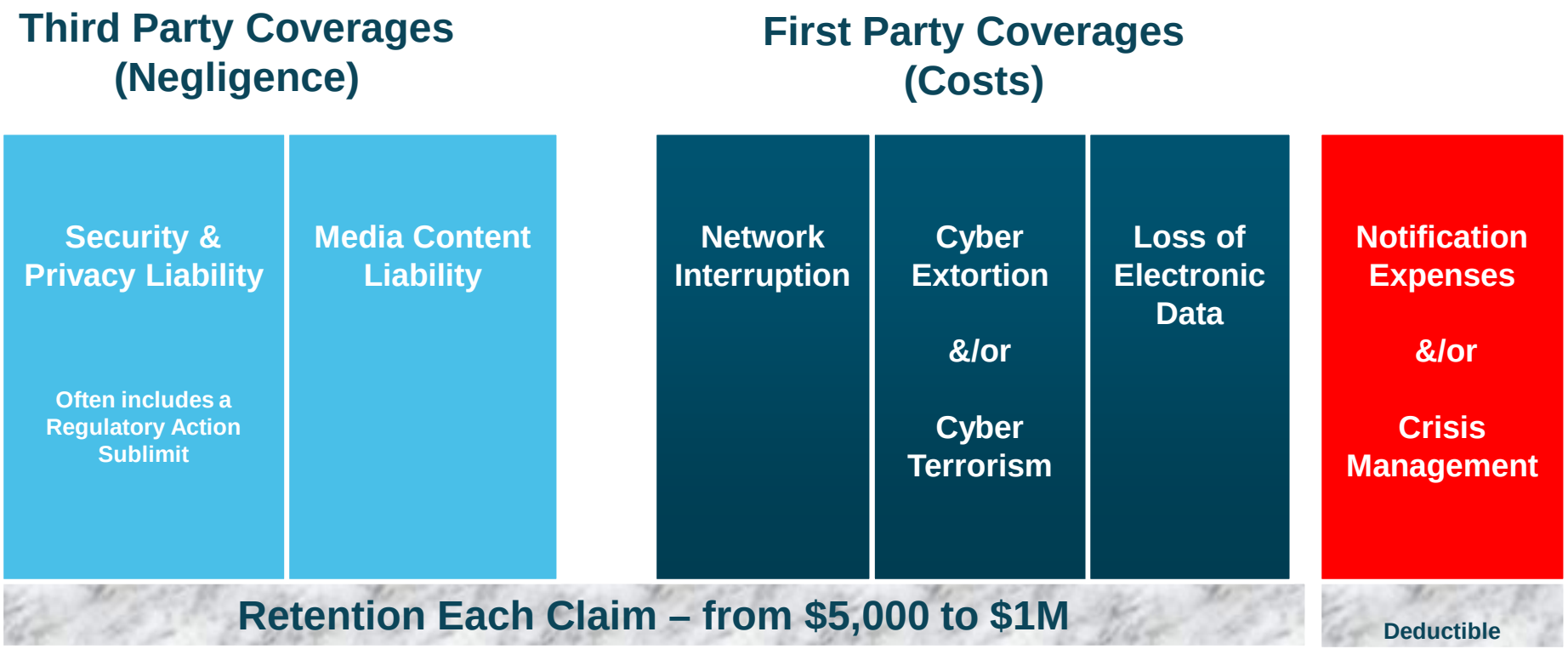
Directors Should be Concerned

Source: Mintz Levin Report

Why Directors Should Be Concerned

- A data breach is not a unitary or self-contained event. The fallout from a breach could impact the directors as well.
- A security breach may lead to an investigation or an enforcement action by the Securities and Exchange Commission (SEC). The SEC may direct its investigation at the directors and subpoena the directors' documents and records.
- Compliance with subpoenas may be extremely expensive and, depending upon how the D&O policy defines "claim", there may not be coverage.
- Moreover, even if the SEC declines to investigate a data breach, the directors nevertheless face exposure to shareholder litigation and, in some cases, investigation by state authorities.
- Shareholder litigation in the cybersecurity context will typically allege a failure by the board to oversee and prevent the loss. This failure potentially gives rise to oversight liability under Delaware law, where many public companies are incorporated.
- At least two separate shareholder derivative lawsuits have been filed against Target's directors and officers, alleging breach of fiduciary duty, waste of corporate assets, gross mismanagement and abuse of control. A similar lawsuit was filed in 2010 against the officers and directors of TJX Companies' by its shareholders following a credit card data breach.

Types of Coverages to be Included



Can also include Professional Liability, if applicable to your company.

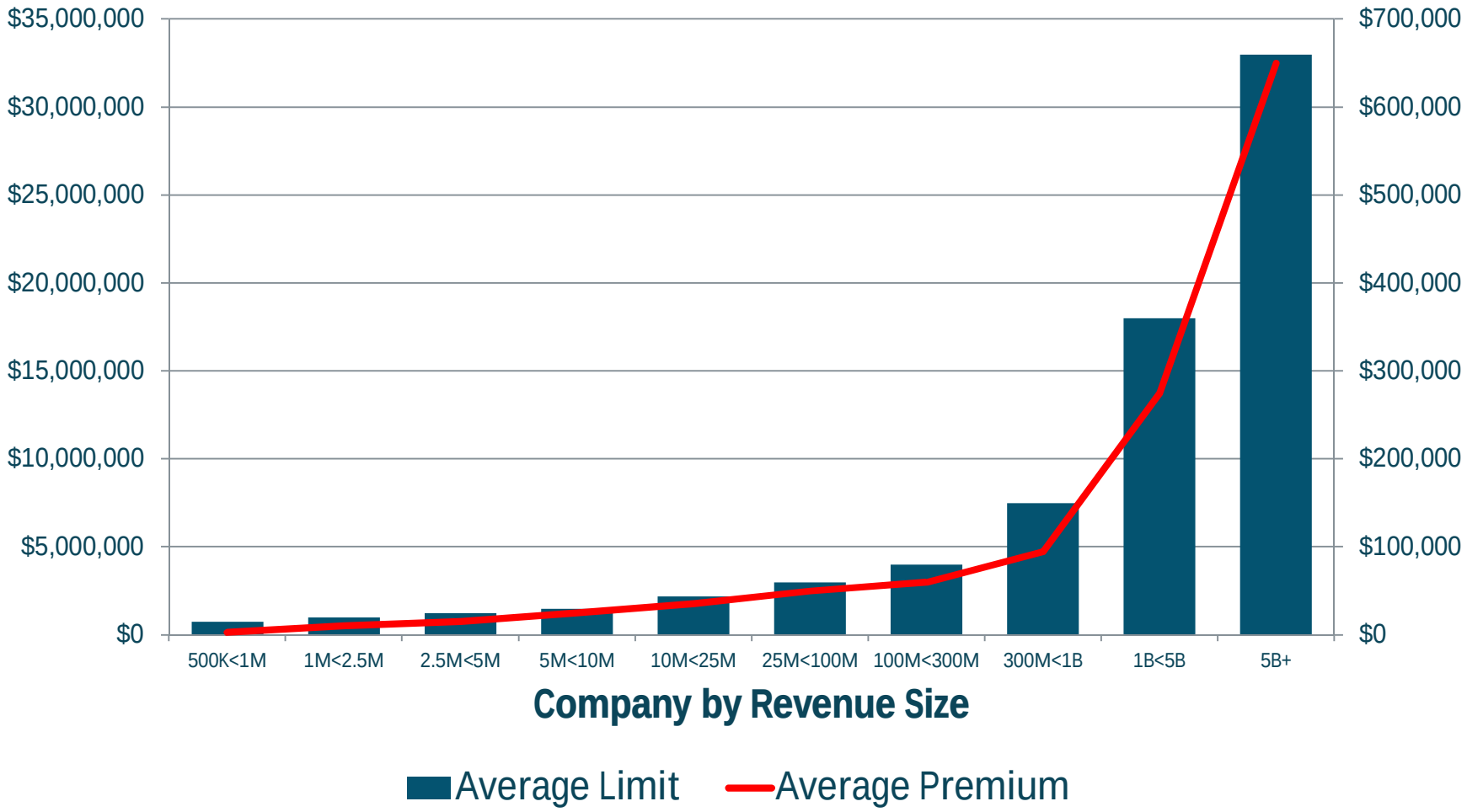
Insurers Providing Cyber Liability Coverage

sample list, not complete

ACE	Hartford
AIG	London / Lloyd's
Axis	IronShore
Beazley	Philadelphia
C N A	RSUI
CFC	XL
Chubb	Zurich
Endurance	There are 50-60 Insurers who will provide cover

Average Premium & Limit by Company Size

Source: Advisen Survey



Companies Purchasing Cyber Liability Insurance

Source: Advisen Survey

Revenue Range ($)	% Purchasing Cyber
<2.5M	3.8%
2.5 to 5M	4.8%
5M to 10M	6.6%
10M to 25M	7.2%
25M to 100M	10.0%
100M to 300M	17.6%
300M to 1B	20.5%
1B to 5B	21.8%
Over 5 B	25.9%

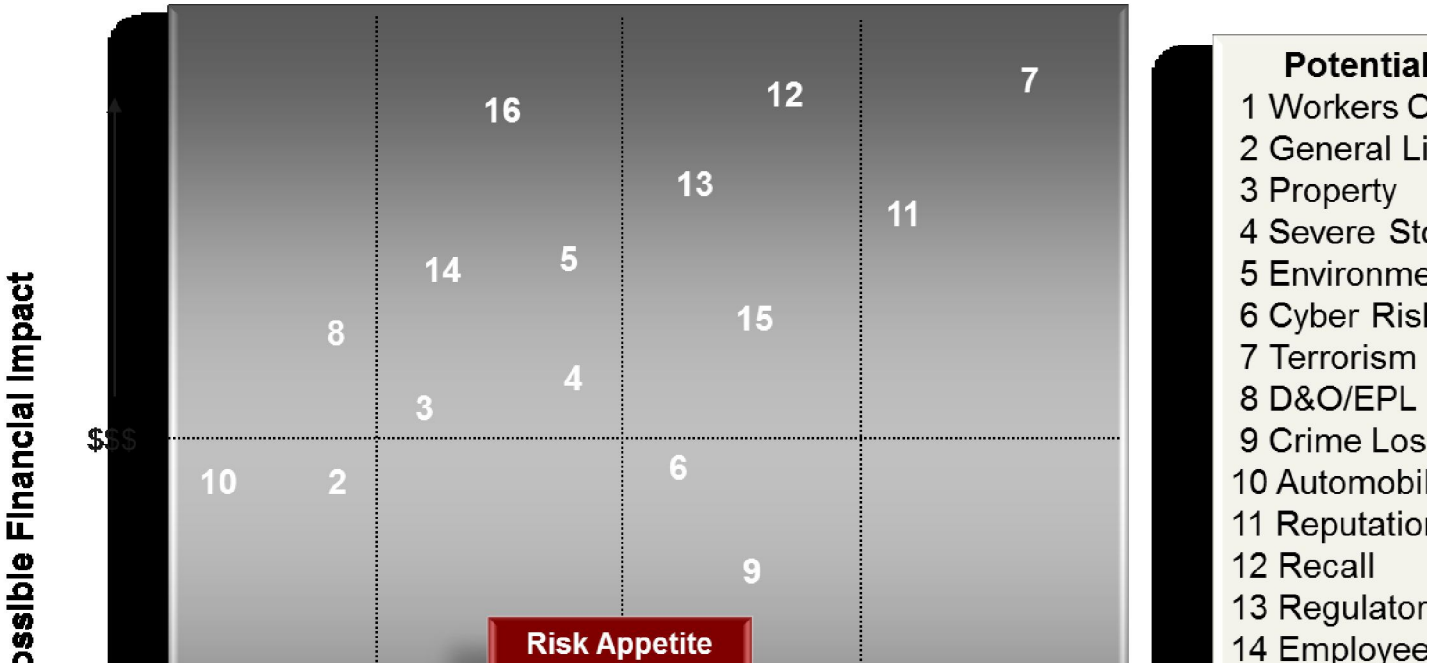
Underwriting Concerns

- The volume and type of data
  - Merger and acquisition activity and financial results in a given industry may correlate with the pressures a chief information security officer might face and the budgetary commitment an insurance buyer can make to data security.
- How that data is protected from both unauthorized access and negligent disclosure
  - Laptops, phones
  - Company server, cloud, encryption
  - Former employee data
  - PCI Compliance
  - System-Penetration Detection
- Vender Management Controls
  - Who is used
  - What systems access do they have?
- Contracts

Specific Concerns for the CTTMA

- Regulatory
  - Conn. Gen Stat. § 36a-701b
- Prior Acts
  - Important to note that policies are “Claims Made” and will only cover incidents that have occurred and have been reported within the policy period (plus “retro” date)
- Industry Specific
  - Health Care
  - Tech
  - Finance
  - Construction / Real Estate
  - Manufacturing

CTTMA Concerns – Mapping the Risks



Where Do Threats Come From?

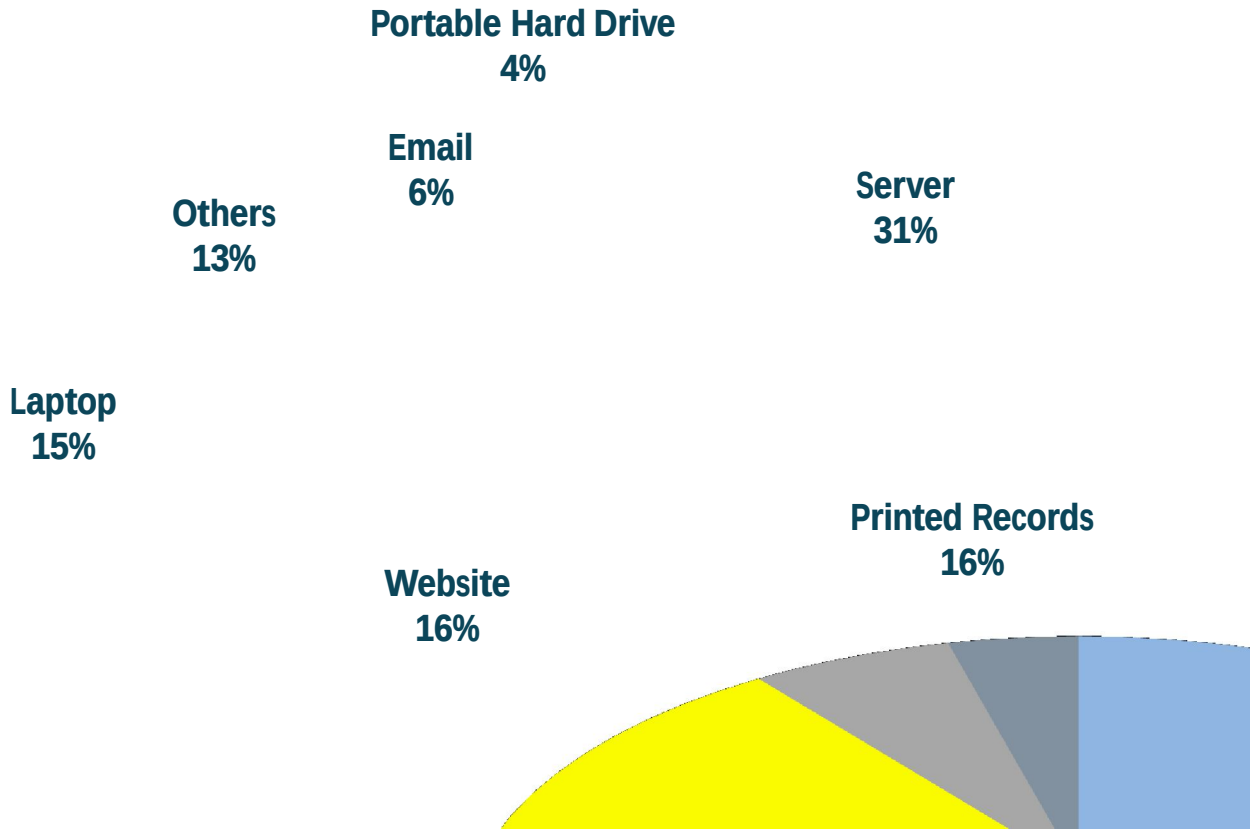
- Disgruntled Employees and Former Employees
- Vendors
- State Sponsored attack
- Extremists (Terrorism or “Hacktivists”)
- Criminal gangs
- Cyber Espionage attack

Types of Incidents

- Unauthorized Intrusion (Hacking) Leading to:
  - System/ Data Damage via Virus
  - Virus infusion transmit to 3rd parties
  - Release of Confidential Information
  - Threat of the above
- Stolen or Lost Smart Phones, Laptops, or memory devices (incl. tapes, CDs, USB drives, Hard Drives etc.)
- Poor destruction/disposal of confidential information such as throwing papers into a dumpster without shredding properly.
- Improper use of another's intellectual property
- Improper performance of a Professional Service or an Internet Professional Service such as IT Consulting, ISP, Network Security or Internet Media Services.

Sources of Data

Source: Advisen Survey



Type of Data Lost

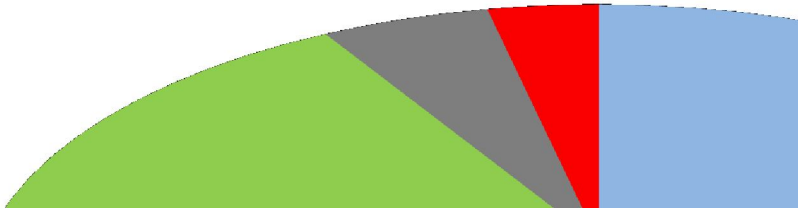
Source: Advisen Survey

Corporate Loss of Business Income 5%

Corporate Loss of Digital Assets 3%

Personal Privacy 35%

Personal Financial Identity 57%



Loss Cases by Industry – Global

Source: Advisen Survey