RIMS CANADA Conference

Proudly presents…

Cyber Risk – State of the Art

Matthew Davies, Chubb Insurance
Catherine Dowdall, Canada Post
Mike Petersen, Marsh

Agenda

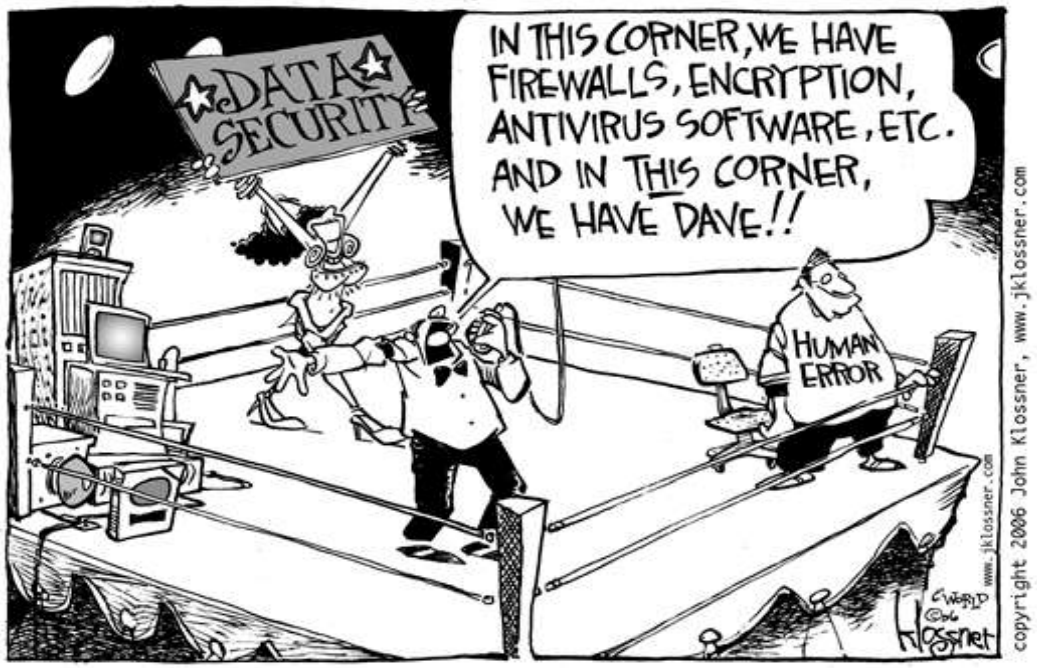
1. Who is At Risk?
2. New/Emerging Risk and Trends
3. Canada Post Perspective
4. Why Should My Company Consider Cyber Risk Coverage?
   - What Is It?
   - Coverage Gaps
   - Limits
5. Market Overview
6. Claims
7. Contract Language

Our Goal is to help you:

1. Understand the basics about cyber risks insurance coverage and why you need to consider this coverage for your company; and

2. Be able to communicate this risk to your senior management and your Board of Directors

Reality


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
copyright 2006 John Klossner, www.jklossner.com

“There are only two types of companies: those that have been hacked and those that will be”

FBI Director Robert Mueller March 1, 2012

The Canadian Perspective – Is There a Risk to Canadian Companies?

- “Class Action launched against Elections Ontario over missing voter information” – Globe and Mail, July 20, 2012
- “Durham Regional Health class action lawsuit puts price on personal information” – thestar.com May 28, 2012
- “5 employees fired after Eastern Health privacy breaches” – CBC News, July 25, 2012
- Correctional Service Canada “to pay victims of breach of privacy” – thewhig.com August 26, 2010

Who Is At Risk?

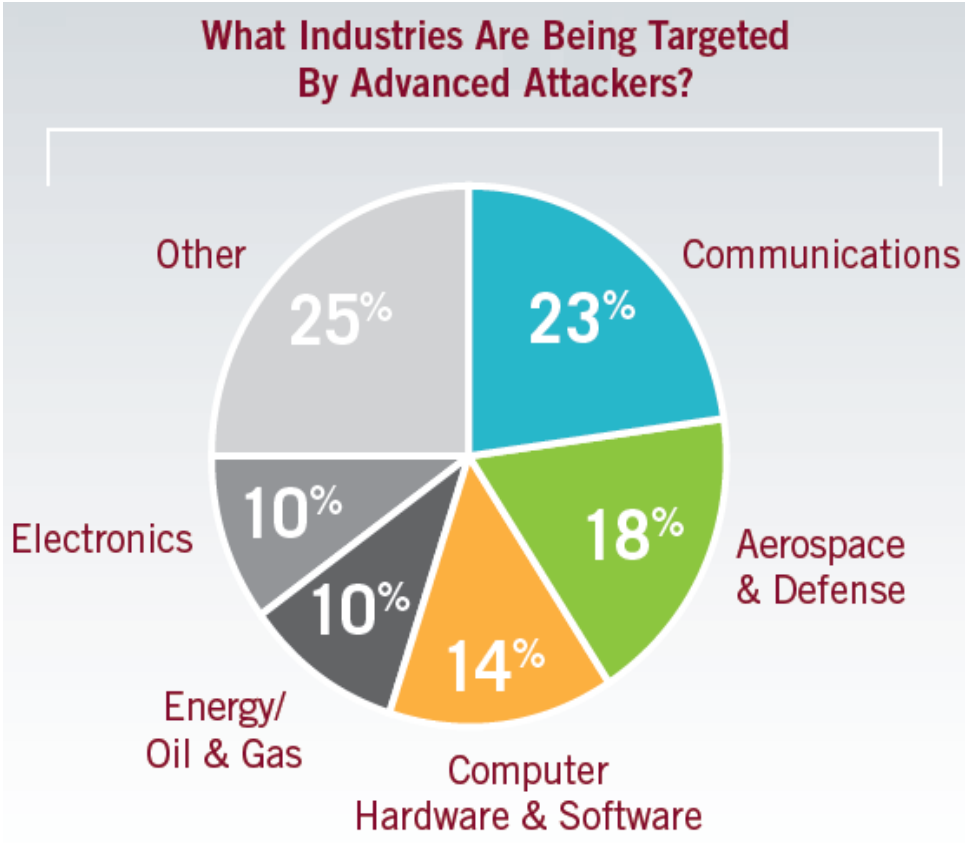
Verizon Security Consultants 2011 Data Breach Investigations Report

- A sample of 900 breaches. Some key findings:
  - 92% stemmed from external agents (up 22% over 2010)
  - 17% implicated insiders (down 31% over 2010)
  - 50% utilized some form of hacking/malware
  - 86% of data breach discovered by third parties, NOT by the company itself
  - 92% of attacks were not highly difficult (up 7% over 2010)
  - 96% of incidents were avoidable with simple controls
  - Main attack pathway – web applications (54%)

Who Is At Risk?

- **NetDiligence Cyber Liability & Data Breach Insurance Claims June 2011**
- Cyber underwriters provided information on 117 events 2005-2010. Victimized organizations had some form of cyber coverage. A claim was filed. Some key findings:
  - Average cost of a data breach: $2.4 Million
  - Average cost per record: $1.36
  - Average cost for legal defense: $500,000
  - Average legal settlement: $1 Million
  - 50% of events involved Personally Identifiable Information (PII). 75% of records exposed contained credit card information
  - Personal Health Information (PHI) compromised 21% of breaches
  - Hackers caused 32% of breaches
  - 60% of breaches occurred in financial services, healthcare & retail

Who Is At Risk?



416

median number of days that the attackers were present on a victim network before detection

Courtesy of Mandiant: M-Trends an evolving threat

What Are The New And Emerging Risks?

- Your company is already infected – learn to live with it
- Mobile devices – security threats increasing; mobile banking, geolocation
- Cloud Computing – as services grow related breach incidents will to; US Patriot Act
- Small businesses are not secure and not prepared
- Global Systemic risk – increasing interdependence; ripple effect
- Insider threats are real
- Increased regulatory scrutiny in Canada
- (Social) media attention leads to rapid escalation
- C-suite discussions – reputational risk, crisis management

Trends Influencing Cyber Insurance Buying Decisions

1) Regulatory Requirements evolve:

- Alberta Personal Information Protection Act

http://www.oipc.ab.ca/pages/OIP/BreachNotificationDecisions.aspx

- Amendments to SEC guidance
- Getting Accountability Right with a Privacy Management Program
- US revenue or customers = complex regulatory environment

2) Increased Security Threats Due to Technology (mobile devices, etc.)

3) Reputational Risk

4) Corporate Sustainability

Cyber Risks: A Canada Post Perspective

Canada Post: A Company in Transition

PC vs. PAPER vs. INTERNET

Why is the tablet a Game Changer?

Canada Post Mail Volumes

epost.ca: your free digital mailbox from Canada Post

One place. One login. One password.

Enjoy all-in-one-place convenience for bills and statements like cable, phone, utilities, credit cards, property taxes and more with a single Log in. Store your bills and statements electronically for up to seven years. View them any time, from anywhere, online. Learn more.

The peace of mind of complete security

As the trusted provider of Canadians' mail, we are committed to ensuring the security and privacy of your digital mail. That's why we use advanced encryption technology. Learn more.

Over 7 million Canadians agree

Launched in 2000, epost was the first and is the largest bill consolidator in Canada. Today, it is a personal, digital mailbox for over 7.5 million subscribers, offering 250 bills and statements from over a 100 mailers in a safe and secure way. And best of all, it's completely free!

What is epost?

- epost is a **secure** B2C and G2C electronic communications channel
  - Bills & invoices
  - Statements
  - Notices and updates
- Protected by *Canada Post Act*
  - epost communication = “mail” as defined by Act
  - Tampering is a federal offense
- *Electronic Postmark* certifies message/document have not been altered, modified or tampered with during delivery

Why epost?

- For businesses…
  - Bank-grade security with all data stored in Canada
  - Allows regulated industries to meet mail-related compliance obligations
  - Offers customers more multichannel options
  - Cost effective
- For consumers…
  - Manage bills in one place, with one username and password
  - Secure, convenient 24/7 access
  - Behind firewall of all major Canadian financial institutions
  - Free, with 7-year storage

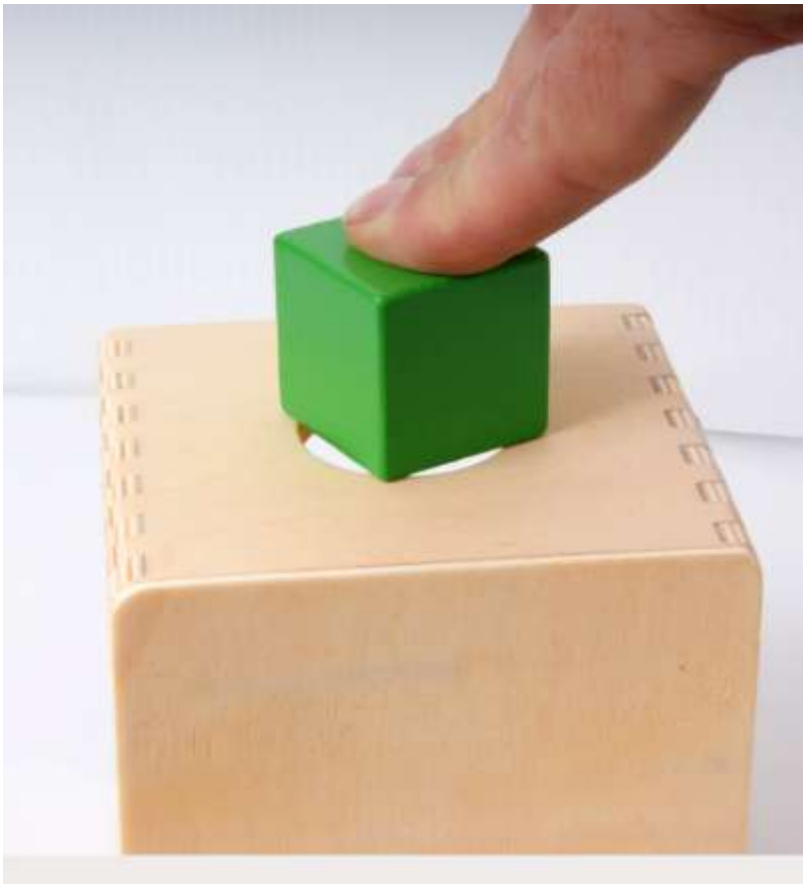
What are the Cyber Risks: A Canada Post Perspective

- Some contracts require cyber coverage
- ‘Cloud Vendor” contract language often not satisfactory
- Not all suppliers have E&O and cyber coverage requirements in contracts (legacy issue)
- Suppliers trying to limit liability to the value of the contract

Why Consider Cyber Coverage?

What Are the Gaps In Traditional Policies?

Traditional insurance was written for a world that no longer exists. Attempting to fit all of the risks a business faces today into a traditional policy is like putting a square peg into a round hole.



What Are the Gaps In Traditional Policies?

- **Errors and Omissions (E&O)**: even a broadly worded E&O policy is still tied to “professional services” and often further tied to a requirement that there be an act of negligence
- **Property**: courts have consistently held that data isn’t “property”— “direct physical loss” requirement not satisfied
- **Crime**: requires intent and only covers money, securities, and tangible property
- **Kidnap and Ransom (K&R)**: no coverage without amendment for “cyber-extortion”
- **General Liability**: often does not provide coverage for damage to electronic data, criminal or intentional acts of insureds or employees, or pre-claim expenses; is there Bodily Injury or Property damage?
- **Directors & Officers Liability** – insured vs insured exclusion; entity coverage?; who is named in the lawsuit?
- **Employment Practices Liability** – protection for own employees only

What Is Network Security / Privacy Insurance?

- **Privacy Liability**
  Harm suffered by others due to the disclosure of confidential information
- **Network Security Liability**
  Harm suffered by others from a failure of your network security
- **Cyber/Extortion**
  The cost of investigation and the extortion demand (limited cover for ransom and crisis consultant expenses)
- **Regulatory Defence**
  Legal defence for regulatory actions including coverage for fines and penalties when insurable
- **Crisis Management Costs**
  The costs of complying with the various breach notification laws and regulations
- **Property Loss**
  The value of data stolen, destroyed, or corrupted by a computer attack
- **Loss of Revenue**
  Business income that is interrupted by a computer attack

Coverage for privacy liability requires no negligence on the part of the insured and provides coverage for the intentional acts of insured's employees

Security and Privacy Insurance Policy Coverage Overview

Privacy and Cyber Perils	Property	General Liability	Traditional Fidelity Bond	Computer Crime	E&O	Special Risk	Broad Privacy and Cyber Policy
Indemnification of notification costs, including credit monitoring services							Privacy Liability (sublimited)
Defense of regulatory action due to a breach of privacy regulation							Privacy Liability (sublimited)
Coverage for fines and penalties due to a breach of privacy regulation							Privacy Liability
Threats or extortion relating to release of confidential information or breach of computer security							Cyber Extortion
Liability resulting from disclosure of electronic information and electronic information assets							Network Operations Security
Liability from disclosure confidential commercial and/or personal information (i.e. breach of privacy)							Privacy Liability
Destruction, corruption, or theft of electronic information assets/data due to failure of computer or network							Information asset protection
Theft of computer systems resources							Information asset protection
Business Interruption due to a material interruption in an element of a computer system due to failure of computer or network security (including extra expense and forensic expenses)							Network Business Interruption
Business interruption due to a service provider suffering an outage as a result of a failure of its computer or network security							Network Business Interruption (sublimitted or expanded based upon risk profile)
Liability for economic harm suffered by others from a failure of a computer or network security (including written policies and procedures designed to prevent such occurrences)							Network Operations Security

Typically not covered

Typically covered

See notes — Typically dependant upon specifics of claims, may not be covered

Cyber Property Network Business Interruption and Data Asset Protection

- **Failure of Network Security:**
  Failure of insured's computer systems' security to prevent or mitigate a computer attack that:
  - Destroys, corrupts, or deletes data, applications, software
  - Steals resources of computer system (e.g., bandwidth)
  - Interrupts the operations of computer system
  - Creates operational extra expense
- **Dependent Business Interruption:**
  - Coverage for business interruption suffered by an insured as a result of a business it depends on for some element of its computer network being hacked.
  - Usually sublimited to $100,000 unless scheduled to the policy
- **Covered Loss:**
  - Cost to recreate, restore, replace the lost data, software, applications
  - Cost to determine that such assets cannot be restored, recreated, or replaced
  - Lost revenue during the period of interruption
  - Extra expense incurred during the period of interruption
  - Value of data or stolen computer systems' resources (requires a special endorsement) (Can sit excess/DIC of Crime-Fidelity)
  - Forensic costs (sub-limited)

  Some carriers have adopted a broader trigger of "system outage" or "failure of technology."

Potential value of a privacy event based upon number of records compromised

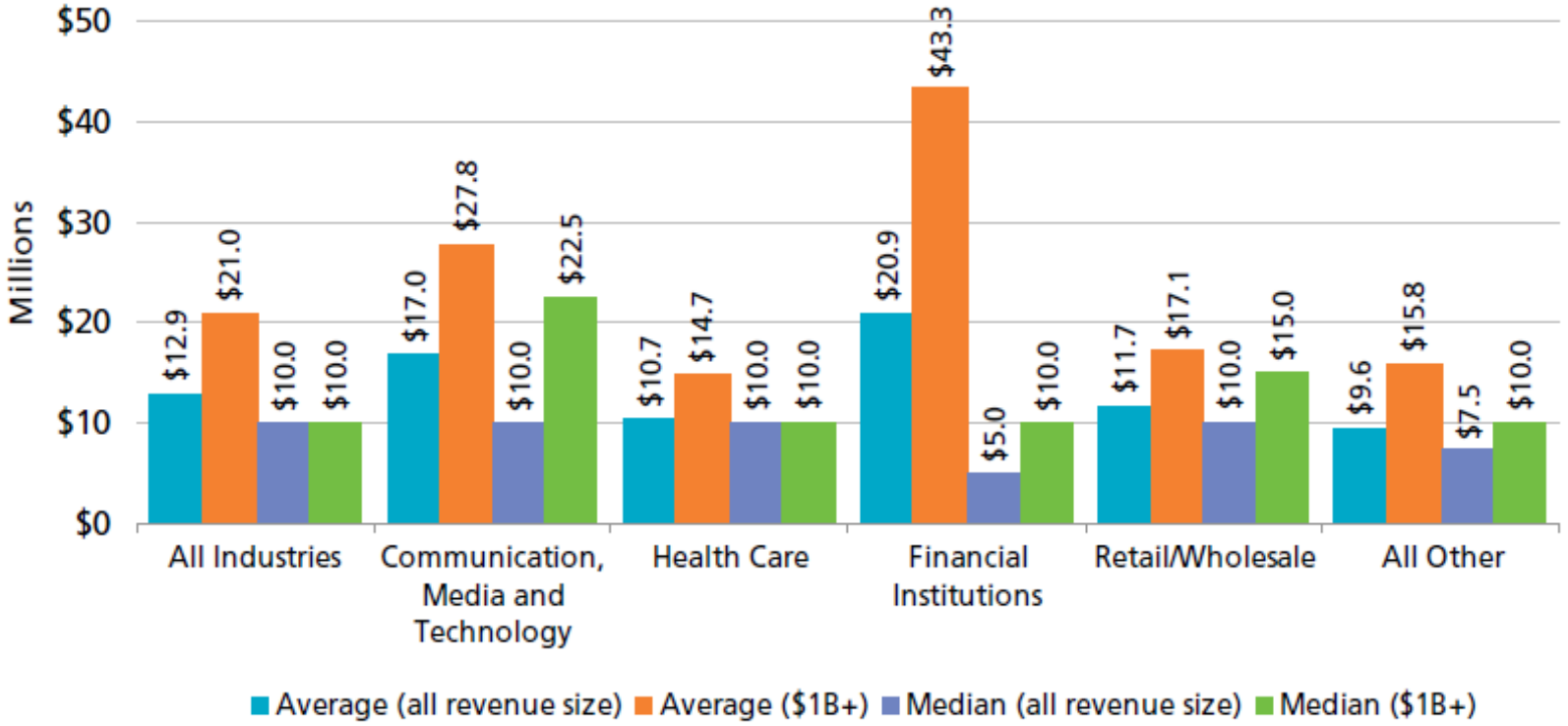
Number of records compromised	100,000	250,000	500,000	1,000,000
Privacy notification costs	$200,000	$500,000	$1,000,000	$2,000,000
Call center costs	$100,000	$250,000	$500,000	$1,000,000
Credit monitoring cost	$540,000	$1,350,000	$2,700,000	$5,400,000
Identity theft repair	$350,000	$875,000	$1,750,000	$3,500,000
Total estimated expenses**	**$1,190,000**	**$2,975,000**	**$5,950,000**	**$11,900,000**

Assumptions:
Notification costs – $2 per record
Call center costs - $5 per call (20% expected participation)
Credit monitoring - $27 per record (20% expected participation)
Identity theft repair - $350 per record (5% of those monitored experience theft)

****Regulatory actions, forensic, and legal expense:** Since a regulatory action usually precedes the civil action, substantial legal and forensic expense can be incurred even for events where no one is actually harmed or even at risk of harm

What limits are purchased

Distribution of Total Cyber Risk Limits Purchased



Marsh Benchmarking July 2011

- Average limits purchased: $12.9M
- Financial Institutions purchased highest limits

Q: Should the Cyber Policy Overlap with Professional Liability Policy?

- Privacy liability policies should typically be with the same carrier if the professional liability policy provides services or products in order to eliminate any possible conflict between carriers
  - Example: Tech firm X has an E&O policy and a privacy policy with separate insurers. Tech Firm X software fails and causes a release of private information of its customers. Is this an E&O or a privacy breach?
- This can be done on a standalone basis or a bolt on module

Underwriting Process

- Ballpark quotes can be obtained with entity name and revenue
- Application: required for 1st time buyers; will include a warranty statement. Most coverage is “claims made & reported” so try to limit the scope of the warranty statement to specific individuals; amend the prior knowledge exclusion to be the same as the warranty statement. For renewal applications: some have warranty language.
- Two principle structures
  - Dollar sublimit permitting the insured to select their own vendors
  - Per person sublimit providing access to the underwriters vendors
- 25+ Underwriters offer coverage in Canada. Principal markets:
  - ACE
  - Chartis
  - Chubb
- Canadian Market capacity: more than $250 million

Market Approach

- Currently there are two approaches in the market for crisis management coverage:
  - Providing a dollar sublimit
    - Pros:
      - Insured maintains control of the process
      - Insured knows exactly how much money they have available for an "event"
    - Cons:
      - Insurer may not agree to all costs incurred
      - Insurer may not approve insured's selected vendors
      - Dollar sublimit may not be sufficient to respond to all costs associated with an "event"
  - Providing a per person sublimit.
    - Pros:
      - Insured selects response firm from a panel counsel list
      - the response is handled by the insurer
    - Cons:
      - The Insured hands over the response to the insurer
      - Building beyond standard 2 million individuals affected is difficult
- For larger, more sophisticated insurance buyers, the per person sublimit removes control, which they expect to maintain
- For smaller, less sophisticated buyers, the per person option provides a turn key product necessary to satisfy statutory regulations

Evolving Contract Language

Contract language becoming more specific

- Clearly requesting Network/Cyber-Liability/E-Commerce coverage
- Advising the supplier to comply with all consumer protection laws and that the supplier will not be in violation of these laws
- Setting out limit requirements, most frequently in the $2 Million to $5 Million range
- Suppliers are asked to be added as an additional insured
- Addressing extended reporting periods or “tails” after contract work is complete – 2, 3 years

Placement Tips

Placement Tips

- All wordings are not the same. These are relatively new product offerings and a great deal of creativity is taking place at this time. Analyze and understand the differences
- Understand how the limits & retentions work
  - Is it a total all inclusive aggregate/retention, or
  - Does each component have it's own sublimit/retention or
  - Are some areas of coverage sublimited ie such as regulatory defense
- Some insurers will offer Crisis Management coverage with a standalone limit
- Pay attention to regulatory proceedings; they may form part of the privacy coverage

Placement Tips

Remember:

- Placement of coverage is the last step in the process
- Insurance is never a valid alternative to good risk management
- Relying on technology as a “silver bullet” that will defend against “all risks” is to turn a blind eye to major risks
- Address cyber risk holistically
- Include representatives from legal, communications, corporate social responsibility, issues management, strategic planning, HR
- Assess your existing capabilities – consider broad impacts, consequences, reputational risk
- Assess and refine your current crisis management processes

What Makes You A Good Cyber Risk From An Underwriter's Point Of View?

- In the absence of insurance coverage, if you had a privacy or cyber breach, would you be just a bit shaken, somewhat maimed or outright killed in action?
  - Incident response plan
  - Business continuity plan
  - Media response plan
  - Intrusion testing
  - Payment card industry (PCI) compliance
- Controls in place that set expectations you have of your employees to take ownership and be aware of their responsibilities to protect sensitive information:
  - Social media policy
  - Appropriate use of e-mail and Internet at work policy

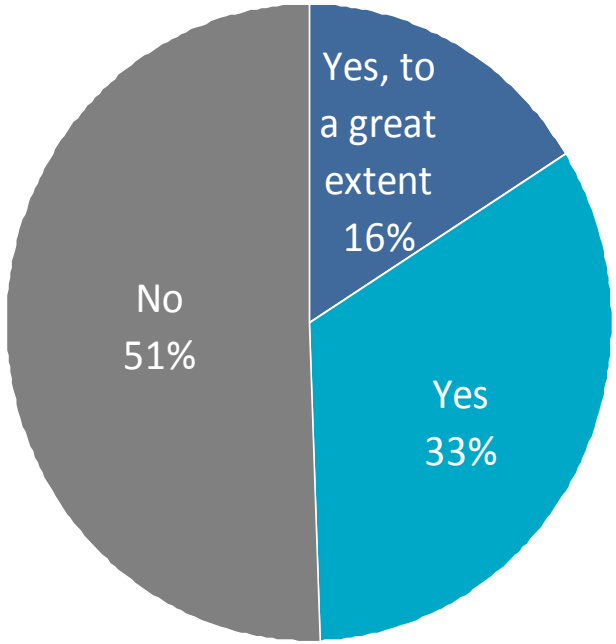
What Makes You A Good Cyber Risk From An Underwriter's Point Of View?

- Insurers like insureds who rely on insurance as a contingency, not as a substitute for doing the right thing to be as flame-proof as possible.
- Governance – how engaged is your board of directors in security concerns?
- Is your industry or your brand a lightening rod?
- Where are your customers and employees domiciled?
- What do you require of your vendors and sub-contractors with whom you share your data?
- What kind of data do you have:
  - Personally identifiable information?
  - Confidential third party corporate client information?
- How critical to your operations is your e-commerce platform?

Is Senior Management Prepared?

- Essential steps for your senior management team:
  1. Ensure that cyber risk is appropriately included in the enterprise risk management, reporting process and corporate preparedness program.
  2. Ensure that a solid overall crisis management process and capability are in place.
- Senior management must also participate in and practice simulation exercises.
- Board members need to be informed of the risks and understand the magnitude and procedures in place.

Are boards of directors provided with adequate information to provide IT risk oversight?



Source: Oliver Wyman / National Association of Corporate
Directors, IT Risk Governance Survey

Claims

Health Care Organization Loss Scenarios from Chubb

Lost iPad

COVERAGE	CyberSecurity by Chubb
Cause of action	Unfair Trade Practices, Violations of HIPAA, Negligence, Invasion of Privacy
Type of organization	Hospital
Number of employees	2800
Annual revenue	$420 million

DESCRIPTION OF EVENT

A nurse lost an iPad containing names and protected health information for 25,000 patients vaccinated against the flu. A class action was filed against the nurse's employer, a hospital, alleging negligence and invasion of privacy. In addition, consistent with HITECH, an attorney general action was filed against the hospital for alleged violations of HIPAA, including failure to properly encrypt portable data and failure to provide timely notice to impacted individuals. Finally, the attorney general alleged violations of the state's unfair trade practice law.

RESOLUTION

The hospital incurred more than $750,000 in expenses associated with notifying patients regarding the lost iPad, hiring a public relations firm, establishing a call center, providing monitoring and restoration services, and retaining independent counsel to assess notice and compliance obligations. In addition, following class certification and defense costs in the amount of $500,000, the hospital resolved the litigation for approximately $1 million. The hospital also paid $500,000 in monetary fines and penalties as a result of the HIPAA and unfair trade practice violations and was required to implement new encryption and training protocols.

Media Loss Scenario from Chubb

Hack of Third-Party Network Gets Media Company into Hot Water

COVERAGE	CyberSecurity by Chubb
Cause of action	Unfair Trade Practices, Negligence, Invasion of Privacy
Type of organization	Media and Entertainment Company
Number of employees	1000
Annual revenue	$30 million

DESCRIPTION OF EVENT

A media and entertainment company outsourced the storage and protection of its employment information to a third-party service provider. Subsequently, the service provider's network was breached, and outsiders were able to obtain unauthorized access to names, social security numbers and financial account details for 1,000 employees. A class action was ultimately filed against the employer, alleging failure to protect the personally identifiable information (PII), to adhere to the company's network security and privacy policy, to timely notify the employees about the breach, and to properly retain and oversee a viable third-party service provider.

RESOLUTION

The company incurred $200,000 in expenses associated with notifying employees about the theft of PII, changing account numbers, establishing a call center, and retaining independent counsel to assess notice and compliance obligations. In addition, the company afforded employees with monitoring and restoration services for two years following the breach at a total cost of $50,000. Further, after incurring approximately $100,000 in legal defense costs, the class-action lawsuit was resolved for $950,000. Lastly, while the company attempted to subrogate against the third-party service provider, the provider lacked sufficient assets and insurance to fully indemnify itself.

Professional Services Loss Scenarios from Chubb

PII Theft Results in Extortion, Business Interruption, Extra Expense

COVERAGE	CyberSecurity by Chubb
Cause of action	Breach of Contract, Negligence
Type of organization	Law Firm
Number of employees	55
Annual revenue	$20 million

DESCRIPTION OF EVENT

An unknown organization hacked a law firm's network, and the intruder may have gained access to sensitive client information, including a public company's acquisition target, another public company's prospective patent technology, the draft prospectus of a venture capital client, and a significant number of class-action lists containing plaintiffs' personally identifiable information (PII). A forensic technician hired by the law firm determined that a bug had been planted in its network. Soon after, the firm received a call from the intruder seeking $10 million to not place the stolen information on-line.

RESOLUTION

The law firm incurred $2 million in expenses associated with a forensic investigation, extortion-related negotiations, a ransom payment, notification, credit and identity monitoring, restoration services and independent counsel fees. It also sustained more than $600,000 in lost business income and extra expenses associated with the system shutdown.

Professional Services Loss Scenarios from Chubb

PII Theft Leads to Lawsuits, Business Interruption, Extra Expenses

COVERAGE	CyberSecurity by Chubb
Cause of action	Hacker, Breach of Contract, Negligence
Type of organization	Administrator
Number of employees	500
Annual revenue	$65 million

DESCRIPTION OF EVENT

An unknown organization hacked an administrator's network prior to a major holiday weekend and stole personally identifiable information (PII). In addition to obtaining names and credit card information of 25,000 customers, the organization stole employment data from 250 employees of the firm. Furthermore, the unknown organization disseminated a virus through the administrator's system and subsequently shut down the network altogether, rendering the firm unable to conduct business for 72 hours. The administrator's clients, who were unable to access the network for business purposes and sustained virus-related impacts to their own systems, sued the administrator for impaired access and conduit-related injuries.

RESOLUTION

The administrator incurred $250,000 in expenses associated with a forensic investigation, notification, monitoring and restoration, and independent counsel fees. It also sustained more than $2 million in lost business income and extra expenses associated with the system shutdown. Finally, it assumed an additional $300,000 in third-party defense costs and paid $5 million in damages to customers who were unable to obtain access to the network during a business critical timeframe.

Professional Services Loss Scenarios from Chubb

Rogue Employee Sells Electronic PII

COVERAGE	CyberSecurity by Chubb
Cause of action	Violation of State Notification Regulations, Breach of Contract, Negligence
Type of organization	Hotel
Number of employees	2500
Annual revenue	App. $250 million

DESCRIPTION OF EVENT

A former hotel executive gained unauthorized access to the hotel's confidential internal database that included names and credit/debit card information of 75,000 patrons. The database also included names and social security numbers for more than 2,500 hotel employees. The former executive ultimately sold the personally identifiable information (PII) to an organization allegedly affiliated with organized crime. After the unauthorized access was detected by the hotel's IT department and outside forensic investigators, the hotel notified the impacted patrons and employees about the breach. A regulatory action was subsequently initiated on behalf of impacted patrons and employees to establish a consumer redress fund.

RESOLUTION

The hotel incurred more than $2.5 million in expenses associated with forensic investigation, privacy notification, credit/identity monitoring and restoration, public relations, and regulatory defense fees. It also paid $2.5 million in fines and penalties as a result of the unauthorized access to its database and its failure to timely notify patrons and employees of the breach.

Contract Language

Evolving Contract Language

Contract Language is evolving and becoming more sophisticated:

11.2. Privacy Compliance
Supplier will comply with all data security, marketing and consumer protection laws that apply to the collection, access disclosure, and use of Privacy Restricted Data and will not cause to be in violation *of* any such applicable law s. Additionally. Supplier will comply with (i) applicable industry standards and best practices and (ii) any privacy-related policies *or* guidelines within 30 days of receipt of such policies or guidelines from.

If Supplier conducts any direct marketing. it may not rely on any exception to any law governing direct marketing (e.g. the established-business-relationship rule) without first getting the written approval of……

F. Network/Cyber-Liability/E-Commerce insurance covering acts, errors, or omissions arising out of Services performed under this Agreement in an amount not less than $5,000,000 per occurrence and $5,000,000 annual aggregate. A “Claims Made” policy not renewed or replaced will have an extended reporting period or “tail” of not less than 2 years.

Evolving Contract Language

Technology Products & Services E&O - Information Security & Privacy Liability Service Provided to Others.

Such insurance shall cover any and all errors, omissions and/or negligent acts in the delivery of Products, Services and Software under this Contract. Such errors and omissions insurance shall include coverage for claims and losses with respect to network risks (such as data breaches, unauthorized access/use. ID theft, invasion of privacy, damage/loss/theft of data, degradation. downtime. etc.) and infringement of intellectual property, such as copyrights, trademarks, service marks and trade dress.

Such insurance shall include limits of coverage of the local currency equivalent of not less than $5,000,000 and shall remain in effect for not less than three (3) years following the date of termination or expiration of this Contract. Evidence of coverage must be sent to us for three years following termination or expiration of this Contract.

Evolving Contract Language

Contract language becoming more specific

- Professional Liability Insurance covering actual or alleged acts, errors or omissions committed by the Consultant, its agents or employees, arising out of the performance of this Agreement. The policy coverage shall also extend to include personal injury. bodily injury and property damage arising from the performance of professional service and/or arising out of the Work.
- The **Client** shall be named as an additional insured under the aforementioned policies. Said policies to contain no provision that would prevent, preclude or exclude a claim brought by the Client
- Computer Security and Privacy Liability covering actual or alleged acts, errors or omissions committed by the Consultant, its agents or employees. The policy shall also extend to include the intentional, fraudulent or criminal acts of the Consultant, its agents or employees. The policy shall expressly provide, but not be limited to, coverage for the following perils:
  - unauthorized use/access of a computer system
  - defense of any regulatory action involving a breach of privacy
  - failure to protect
  - confidential intimation (personal and commercial information) from disclosure
  - notification costs, whether or not required by statute.
- The policy(s) shall have limits of liability of at least $ per occurrence and $ in the aggregate. If any deductible is applicable, such deductible shall not exceed $, unless such increased deductible or retention is approved by the Client

Enjoy the rest of the
2012 RIMS Canada Conference!