MARSH

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

Really…Cyber Insurance Covers That?

2017 Atlantic Universities Risk Management Seminar

Jeremiah Tonn
VP, National Cyber Practice

MARSH & McLENNAN COMPANIES

@WillFerrell
Will Ferrell

I changed all my passwords to ' incorrect'. So my computer just tells me when I forget.

http://funpicc.blogspot.ca/2011/04/your-password-is-incorrect-will-ferrell.html

Agenda

- Introduction
- Cyber Insurance Considerations
- Risk Transfer Process
- Key Takeaways

Introduction - Setting the Stage

Setting the Stage – Current Threat Environment

Rapid growth of attack vectors has led to the following:

- Difficult to predict next target – targets may be collateral based on a zero-day vulnerability, not because of value in ransoms
- Defenses that take months to develop/market/deploy are defeated in days by anti-forensic hacker teams
- 2016 – move from theft of data to ransomware
- 2017 – Monetizing of lulz – move from encryption ransomware to DOS/destruction

Source: September 2017 Kivu Consulting Presentation – Ransomware & Current Trends Update

Common Cyber Risks for Universities

Privacy Exposures:

- Loss of sensitive personal information of current and former students and current and former employees
- Loss of sensitive contractual information of non-public corporate/commercial information of third parties
- Research of Faculty and Students:
  - Sensitive third party trade secrets or other information of corporations that may partner with the university
  - Sensitive personal information of individuals included in research

Network Security Exposures:

- Cyber extortion (e.g. WannaCry/NotPetya)
- Corruption of data (e.g. types of data: students, employees, software relied on for administrative purposes)
- Transmission of malware to third party vendors and partners
- Website defacement
- Business Interruption:
  - Loss of revenue from retail locations (e.g. bookstores, food and beverage, entertainment, other retail, etc.)
  - While less likely, loss of revenue from the loss of students. Note that computer network outage would likely lead to a delay in revenue instead of a loss of revenue with regards to tuition.

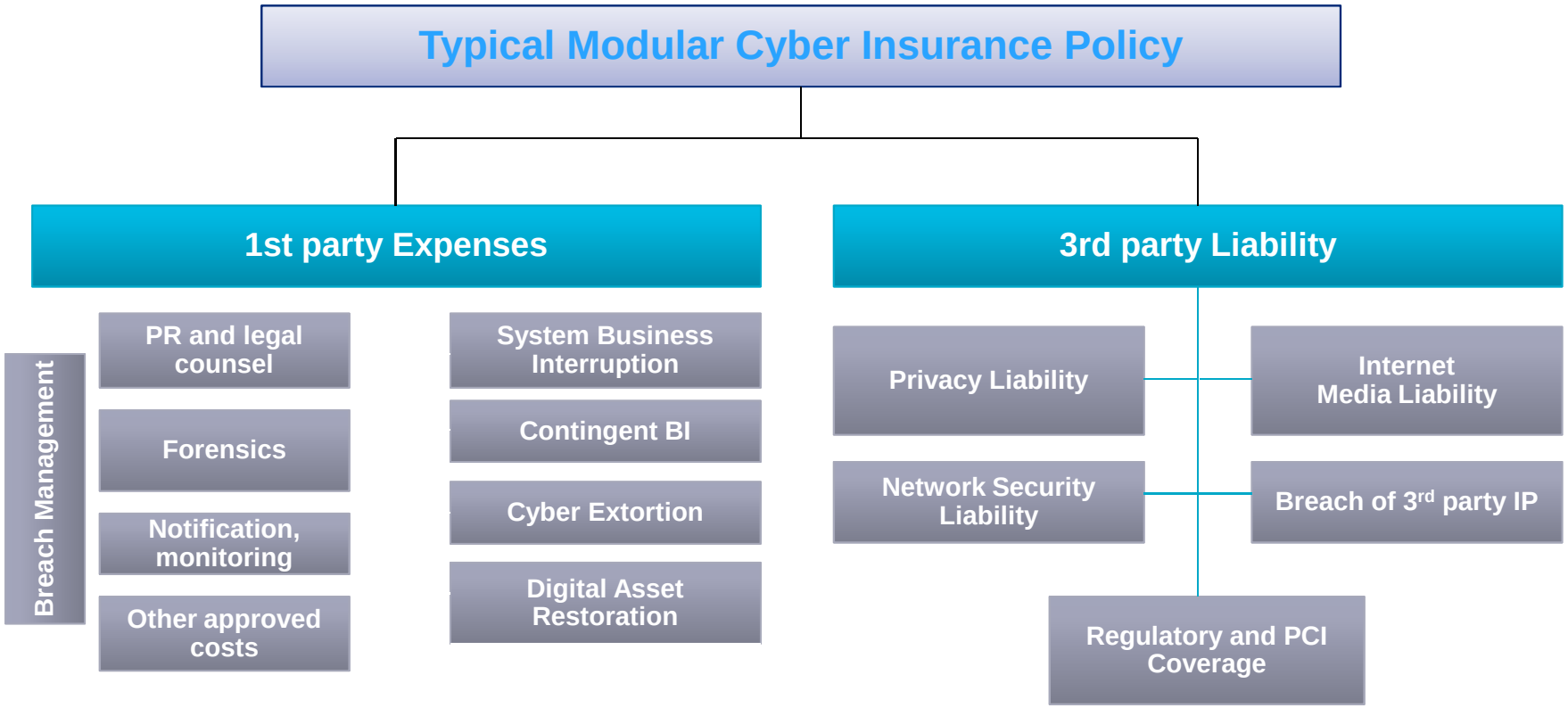
Cyber Insurance Considerations

Where are the Gaps?

While most institutions purchase a variety of traditional insurance programs, many of these programs are not designed to deal with the emerging class of cyber risks. Even though coverage may be available in some areas, many clients find that significant gaps in coverage exist for cyber-attacks.

Cyber Threat	Traditional Insurance Policies				Potential Cyber Insurance Solutions
	Property	General Liability	Crime Policy	D&O	
Corporate IP					
Confidentiality of Corporate IP					Specialty IP Infringement Policies
Integrity & Availability of Corporate IP					Data Restoration Coverage
Third-Party Data					
Confidentiality, Integrity, and Availability of Third-Party Data					Comprehensive Cyber Policy
Technology Infrastructure					
Availability of Operational Technology, Core and General Information Systems					Network Business Interruption / Extra Expense Coverage
Availability of Outsourced Information Systems					Dependent Business Interruption Coverage
Relationship Capital					
Integrity (Value) of Relationship Capital (B2B & B2C)					Specialty Reputational Risk Policies
Financial Assets					
Availability (Theft) of Financial Assets					Cyber Crime Policies and Endorsements
Cyber-exposed Physical Assets					
Integrity (Physical Damage) of Cyber-exposed Physical Assets					Specialty Cyber Property Damage Policies

Cyber Risk: Common Coverage Elements



It is important to note that 1st party expense coverage is generally written on a Discovery Basis, while 3rd party liability coverage is written on a Claims Made basis

Cyber Insurance Coverage Descriptions

	Coverage	Description	Covered Costs
First Party Cover 1st Party Insurance coverage: direct loss and out of pocket expense incurred by insured	**Business Income/ Extra Expense**	Interruption or suspension of computer systems due to a network security breach. Coverage may be added to include system failure.	• Loss of Income • Costs in excess of normal operating expenses required to restore systems • Dependent business interruption • Forensic expenses
	Data Asset Protection	Costs to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed.	• Restoration of corrupted data • Vendor costs to recreate lost data
	Event Management	Costs resulting from a network security or privacy breach:	• Forensics • Notification • Credit Monitoring • Call Center • Public Relations • Sales Discounts
	Cyber Extortion	Network or data compromised if ransom not paid	• Forensics • Investigation • Negotiations and payments of ransoms demanded
Third Party Cover 3rd Party insurance coverage: defense and liability incurred due to caused to others by the insured.	**Privacy Liability**	Failure to prevent unauthorized access, disclosure or collection, or failure of others to whom you have entrusted such information, for not properly notifying of a privacy breach.	• Liability and defense • Third party trade secrets • Notification to individuals • Investigation costs • Costs related to public relations efforts • Sales Discounts
	Network Security Liability	Failure of system security to prevent or mitigate a computer attack. Failure of system security includes failure of written policies and procedures addressing technology use.	• Liability and defense • Bank lawsuits • Consumer Lawsuits • Sales Discounts
	Privacy Regulatory Defense Costs	Privacy breach and related fines or penalties assessed by Regulators.	• Investigation by a Regulator • Liability and Defense costs • PCI / PHI fines and penalties • Prep costs to testify before regulators • Consumer / Bank lawsuits

Common Cyber Insurance Limitations and Exclusions

	Exposure	Losses Not Covered	Considerations
Some Risks Not Covered By A Cyber Policy	Reputational Damage	• Reduced value of your brand.	• Global Brand Recognition
	Remediation Costs	• Costs to remediate systems, i.e. hardware or improve the network or controls beyond that which existed prior to a cyber-attack or data breach. • Costs to coordinate with law enforcement efforts.	• No coverage for costs related to post-event system improvements
	Theft of Intellectual Property	• Theft of any intellectual property. • Lost or diminished value.	• Publication of IP to public internet
	Cyber Crime a/k/a Social Engineering	• Theft of funds from you.	• Coverage can be addressed via the corporate crime program
	Some Common Exclusions	• Prior knowledge of circumstances or situations which may give rise to a claim • Fraudulent/criminal behavior of the C-Suite • Bodily Injury/Property Damage claims • War (there is an endorsement to address Cyber Terrorism) • Insured vs. Insured claims (certain exceptions) • Contractual Liability Claims (certain exceptions) • Power outages (unless in your direct operational control)	• Prior knowledge of potential claims (not vulnerabilities) must be disclosed up front as these are good faith contracts • Cannot insure criminal activity/behavior • Address via the CGL and Property policy • Uninsurable risk • Cannot sue each other and profit from insurance • Carveback for employee claims and PCI

Claims Concerns

There are many headlines about “Cyber Insurance Claim Denied”, Almost all of these articles then go on to note how it is the General Liability or Property insurance that is denying the claim

- Late notice can be a big issue: certain coverages are written on a claims made and reported vs. discovery basis. *Be aware and understand the retroactive and continuity dates*
- Many denials or conflicts surround coverages that are either optional which the insured did not purchase or not covered in general. For example:

  — **Wrongful Collection of Information** – Many insureds face allegations that information was unlawfully or wrongfully collected or wrongfully sold.

  — **Business Interruption Cause of Loss** – We have seen claims denied because the insured could not determine the cause of the loss.

  — **Choice of Vendors** – We have seen costs denied because the insured did not use insurer panel or did not obtain consent before incurring event management costs.

  — **Theft of Funds** – The loss of data/privacy liability related to phishing attacks/social engineering is included under cyber policies; however, cyber insurers are **denying the actual theft of funds** as this is a crime coverage issue

  — **Condition of System** – Systems required to be maintained at a certain level or to a certain standard; *Not something we would accept when placing coverage.*

We have generally seen that cyber insurers are not denying legitimate claims - insurers are looking to grow this market and prove the product works

Simplified Data Breach Event Timeline

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 party 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

Risk Transfer Process

Risk Assessment and Application Process

General Process Steps:

- Initial meeting to understand exposures and concerns
- Quantification
- Completion of Cyber Application
- Request terms from underwriters and summarize
- Two or more meetings to discuss options and next steps

Timeline:

- Typically 1 to 1.5 months after completion of application
- From start of initial discussions to placement of coverage typically 2-4 months

Underwriting Considerations

Insurers are generally interested in understanding the following:

- Overall business operations
- Structure of team(s) responsible for information technology and privacy
- Overall risk management approach (e.g. centralized vs. decentralized, policies and procedures, etc.)
- Types and amount of sensitive information you are responsible for
- Structure of computer network (e.g. use of segregation, interconnectivity internally, interconnectivity with outside vendors, etc.)
- Ability to identify where sensitive information is located
- Vendor Management
- Network security controls:
  - Protection of sensitive information within the network
  - Network monitoring and detection capabilities
- Breach Response Capabilities:
  - Incident Response Planning
  - Business Continuity Planning

Key Takeaways

Key Takeaways

- Your security and privacy risk management policies and procedures are the most important and first line of defense
- Analyze and quantify the security and privacy exposures that are most relevant to your organization
- Determine which security and privacy exposures/risks your organization is comfortable accepting and which exposures/risks your organization may consider transferring through insurance
- Analyze your organization’s current portfolio of insurance products to see if you already have some from of security and privacy coverage
- If, after considering the items above, your organization feels that cyber insurance would be helpful as a second line of defense reach out to your broker to discuss further

For further information, please contact your local Marsh office or visit our web site at: marsh.com

Jeremiah Tonn
Vice President, National Cyber Practice
Marsh Canada
120 Bremner Boulevard, Suite 800
Toronto, Ontario M5J 0A8
jeremiah.tonn@marsh.com

Appendix – Insurable Claim Scenarios

Insurable Claims Scenarios

Coverage Parts:	Description & Claim Scenario
Network Security and Privacy Breach Liability Coverage	Covers 3rd party liability and claims expenses related to a network security breach or privacy liability breach. **Likely 3rd Party Claimants:** Customers, Employees, Industry Counterparties.
Claim Scenarios: 1. Lawsuit brought by customers who's private information was compromised. 2. Lawsuit brought by a trading partner who suffered economic damage because you failed to protect your computer network from a cyber intrusion. 3. Lawsuit brought by a trading partner alleging that malware entered their system from a connection with your computer networks.	
Regulatory Action	Covers costs to respond to regulatory investigations or other actions by regulators including (but not limited to): OPC.
Claim Scenario: 1. Regulatory investigation by the provincial or federal OPC following a cyber breach on your systems.	
Event Management | Breach Remediation Services	Covers first party breach costs including forensics investigation, notifications, attorney costs, call centre, credit monitoring, and identity theft insurance/remediation services. **Notable Exceptions**: 1st party card reissuance costs (may be negotiated), general operating expenses. Costs to remediate your systems, IT incremental costs, extended marketing campaign
Claim Scenarios: 1. Costs for breach investigation services such as to hire forensic firms to investigate a privacy or network security breach. This also includes your costs to identify restoration services for data that has been damaged/corrupted during the attack. 2. Costs for breach notice response and legal services. In the event of a privacy data breach, this would include your costs to hire law firms that advise you on an appropriate legal strategy, notification requirements, costs to do notifications, costs for credit monitoring, identity theft insurance for affected individuals, and for call centres, if needed.	
Media Liability (Optional)	Defense and liability for defamation, libel, slander, product disparagement or trade libel; plagiarism, piracy or misappropriation of ideas; infringement of copyright or trademark. **Likely 3rd Party Claimants:** Authors, producers, publishers, competitors.
Claim Scenarios: 1. Media liability claims are lawsuits and demands alleging defamation, libel or slander resulting from your *website or other online activities.*	

Insurable Claims Scenarios

Coverage Parts:	Description & Claim Scenario
Business Income/ Extra Expense **(Subject to 24 hour waiting period - can likely amend to 12 hrs.)**	Loss of income, extra expenses, and normal operating expenses that continue and result directly from a system interruption. Coverage triggers can include: 1.Cyber Security Breach or Ddos 2.System Failure, i.e. an unplanned outage 3.Outsource Provider breach or cyber attack (contingent coverage)
Claim Scenarios: 1. Malware impairs your operational environment for an extended period while regulators investigate the cause of the malware and appropriate remediation steps. Your plant remains shut down for 3 weeks and suffers significant income loss. 2. Malware finds it way into your network causing it to be inoperable . You incur significant expenses to operate a work around.	
Data Restoration	Costs to recreate, recollect or restore electronic data or software loss arising out of: 1.Cyber Security Failure/Breach 2.Privacy Event/Breach
Claim Scenarios: 1. Wiper Malware erases data on all of your computer work stations You incur significant cost to restore data.	
Cyber Extortion	Costs of consultants and extortion monies (including payment in cryptocurrencies) for threats related to interrupting systems or releasing confidential/private information.
Claim Scenarios: 1. You are a victim to ransomware that encrypts critical data. You are forced to pay an extortion demand to unlock the encryption and incur material expenses via the forensic exercise/investigation.	
PCI Coverage	Extends to PCI Assessments, Fines & Penalties.
Claim Scenarios: 1. Legal expenses to respond to a lawsuit by credit card issuers for fraudulent charges on credit card numbers that were somehow accessed through a breach on your systems. 2. PCI assessment fines are levied against you because credit card numbers were somehow accessed through a breach on your systems.	