MARSH

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

Untangling the Web of Cyber Risk: An Insurance Perspective

BCAW: May 16th, 2017

Gregory Eskins
National Cyber Practice Leader
gregory.eskins@marsh.com

MARSH & McLENNAN COMPANIES

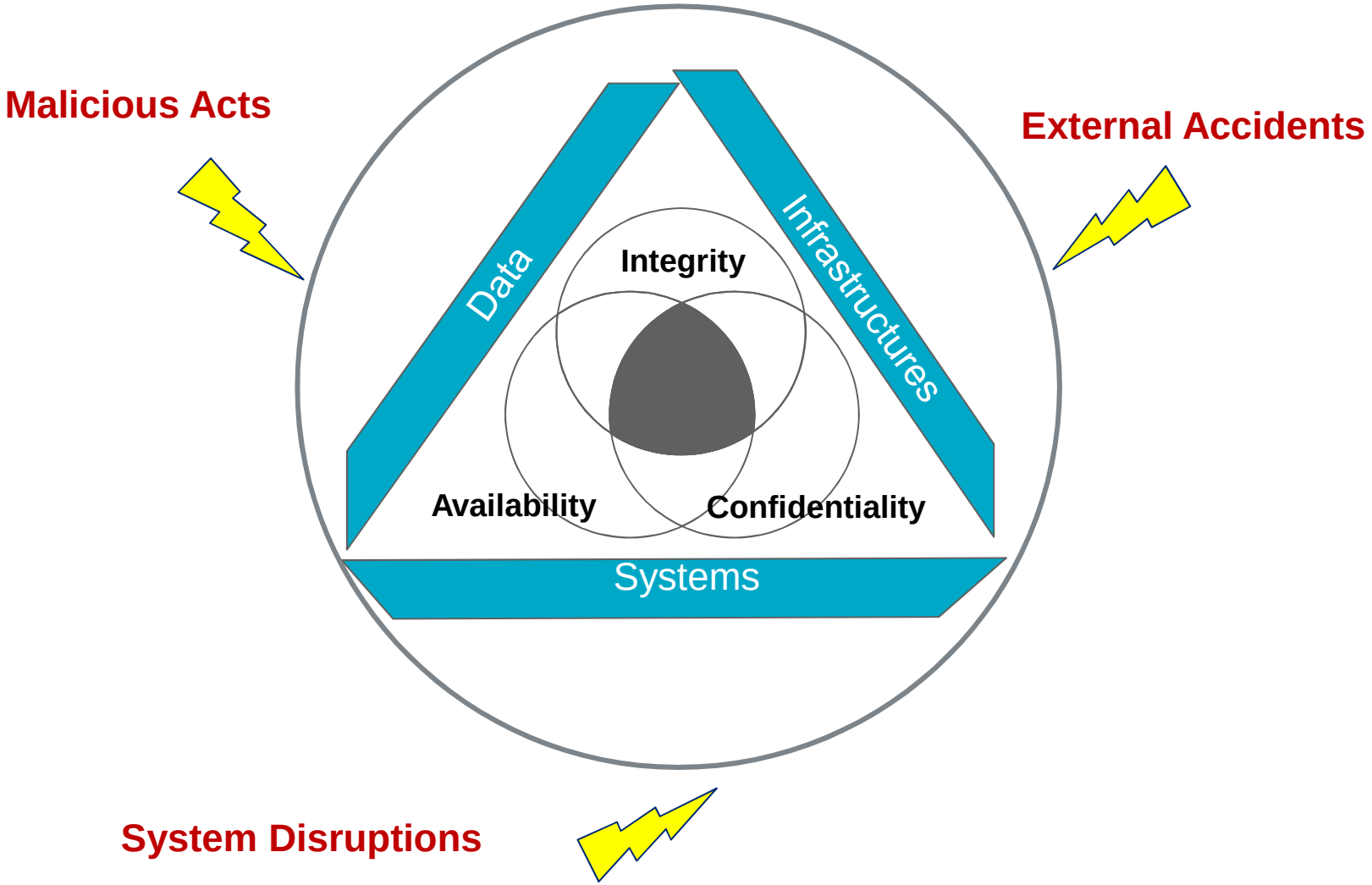
@WillFerrell
Will Ferrell

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

Setting the Stage – Common Cyber Scenarios

Identification of Cyber Risk Scenarios



Most Common Cyber Risk Scenarios

- Cyber Extortion
- Theft of Marketable Data: Retail / Market / IP
- Embezzlement
- Infrastructure or Technology Disruption / Destruction
- Confidential Information Leak, Website Defacement
- Cyber War, Espionage, Influence on Politics, Dissuasion…

Without malicious intent:

- Loss of Portable Device, Data Storage
- Accidental Data Corruption, Software Bug
- Loss of Telecommunication, Power Outage

Quantification: What Impacts?

Investigation and Remediation	• Forensic investigation • Remediation to repair or replace systems
Business Interruption	• Costs associated with business downtime
Crisis Services & Data Privacy Impacts	• Identity theft repair and protection, credit monitoring • Public relations, notification, and call center services
Claim Settlement & Legal Defence	• Payouts for class action / claim settlements with customers, employees, third parties, financial institutions, etc. • Associated legal fees
Regulatory Fines or Penalties	• Fines for government and payment card regulators/associations law violations

Data Breach Scenario Sample

ILLUSTRATION

Credit Card Data Breach Scenario	Consequences	Total Impact ($M)	FI	HI	RI	Fq.
The network is breached by a cyber crime attacker, 400,000 credit card numbers are stolen and sold on the black market. The incident is published in the press thus negatively impacting the organization's reputation –victims, including card owners, Payment Card Companies, etc. engage a successful class action	• Disclosure of credit card information : 400 000 records • Forensic investigation and remediation costs: **$2M** • Notification costs: **$250K** • Legal Defense costs : **$10M** • ID Theft, Identity Monitoring, Credit Monitoring: **$600K** • Third Party Call Center for Crisis Services: **$200K** • Class action settlement for payment card companies and financial institutions: **$6.5M** • Class action settlement for victims: **$1.25M** • Regulatory penalties and fines: **$479K** • Public relations: **$200K**	$21.48 M	4	1	4	2

Legend
FI = Financial Impact
HI = Human Impact
RI = Reputational Impact
Fq.= Frequency

Scale
1 = Low
2 = Moderate
3 = High
4 = Severe

Critical Infrastructure Damage Scenario Sample

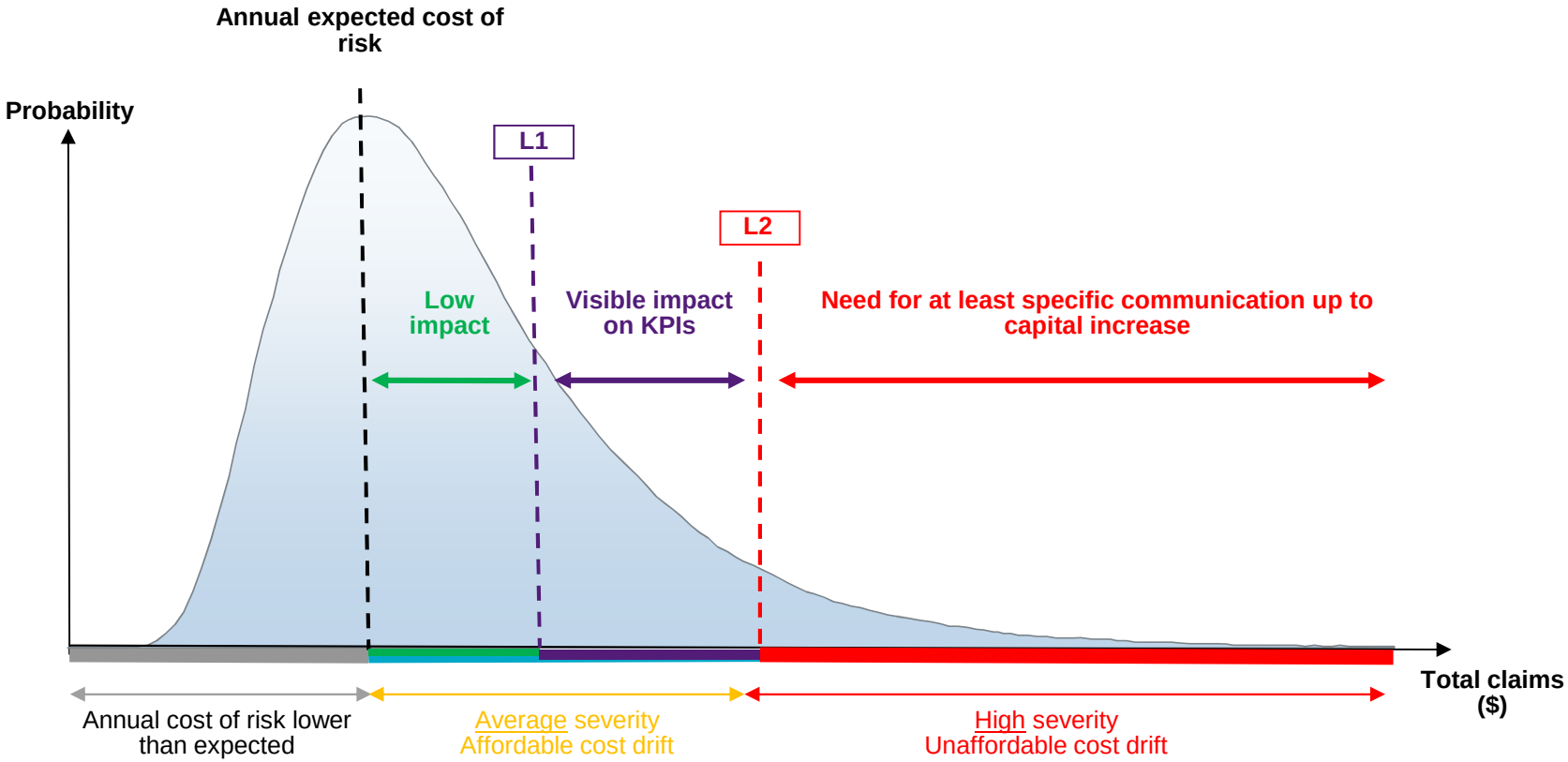
ILLUSTRATION

Critical Infrastructure Damage and Disruption Scenario	Consequences	Total Impact ($M)	FI	HI	RI	Fq.
A hacker gains access to operational controls through an internet portal intending to damage the infrastructure. This is accomplished using the industrial control system. Assets are damaged and operations are interrupted leading to 6 months downtime until systems are controlled and repairs are completed. Gross negligence in cybersecurity allows a client and employee lawsuits to be successful.	• Investigation and Remediation: **$14M** • Asset repair costs: **$105M** • Business Interruption costs: **$21M** • Class action settlement and legal costs: **$19M**	$159M	4	1	3	1

Legend
FI = Financial Impact
HI = Human Impact
RI = Reputational Impact
Fq.= Frequency

Scale
1 = Low
2 = Moderate
3 = High
4 = Severe

Risk Tolerance Estimation



L1 – How much you can afford to lose before a visible impact on forecasted earnings?

L2 – How much you can afford to lose before altering the corporate strategy?

Cyber Risk Quantification Results

ILLUSTRATION

Risk Name	Financial Impact ($M)
Critical infrastructure damage	159.
Credit card data breach	21.4
Privacy breach of customer PII data	4.00
Third party data center fire	3.50
Advanced persistent threat results in tracking & theft of sensitive data	3.00
Hacktivist targeting, website defacement & media exposure	1.50
Malware used in targeted attacks causes destruction of assets	0.75
Corporate office fire	0.50
Data corruption due to inadequate patch	0.20
Interruption of the third party data center / DOS attack	0.20

L2

L1

L2 Risk Tolerance Level /Threshold 2: A loss exceeding this amount would require revision of the Strategic Plan

L1 Risk Tolerance Level /Threshold 1: A loss beyond this amount would be visible on performance indicators

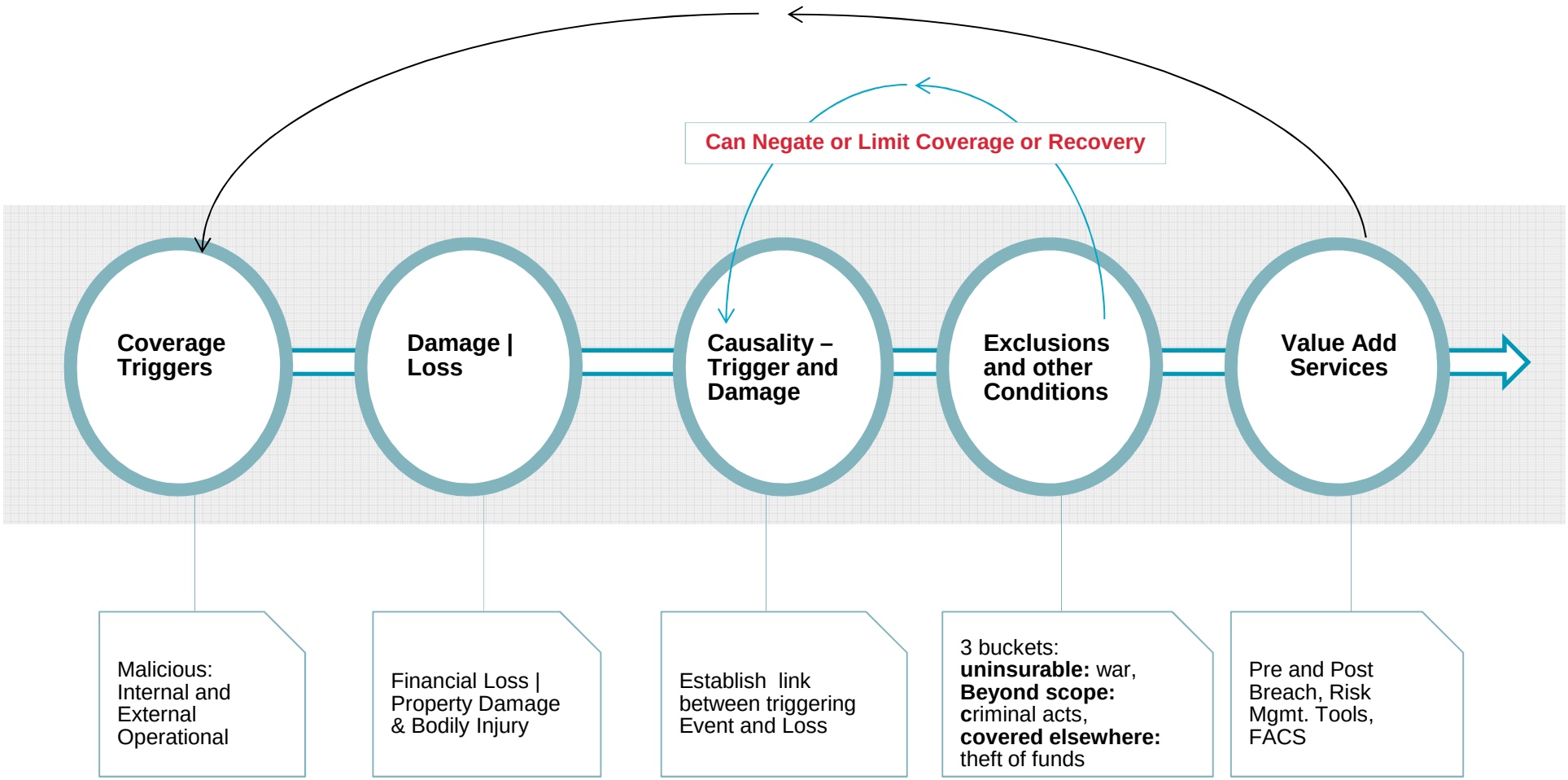
Cyber Insurance Considerations

Where are the Gaps?

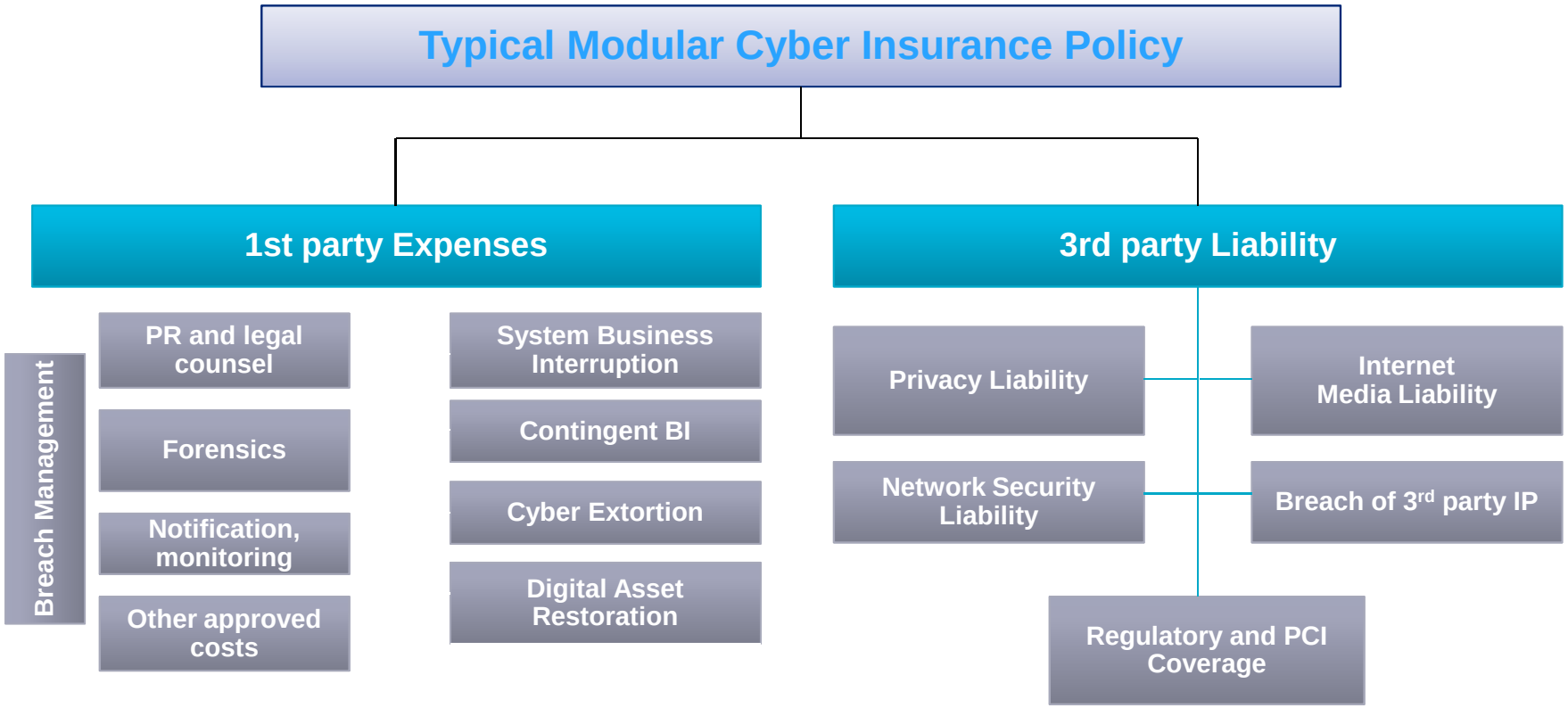
While most institutions purchase a variety of traditional insurance programs, many of these programs are not designed to deal with the emerging class of cyber risks. Even though coverage may be available in some areas, many clients find that significant gaps in coverage exist for cyber-attacks.

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

When Considering Cyber Coverage



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

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.	

Interaction of Financial Lines Insurance Policies

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

Third-Party/Vendor Cybersecurity Risk Management Program Building Blocks

Third Parties/Vendors Permeate Operations

- Organizations inherit risks from third parties/vendors on two fronts – *growth in the volume of relationships* and *increasingly complex integration* into the business and back-office operations. Each third party/vendor granted access to enterprise networks expands the *"attack surface"* and *points of vulnerability* available to cyber threat actors.

Legacy Relationships	Present-day and Future Relationships
• Payroll. • HR benefits management. • Pension Plans and other retirement services.	• IT and HR Help Desk. • Back-office finance and administration. • Cloud computing. • Office 365 and corporate information systems. • Shadow IT and specialized solutions providers (e.g., marketing and business process outsourcing). • Cloud computing.

Third Party/Vendor Security Challenges

Access	Who has access?
Attack Surface	Larger and more complex.
Inventory of Vendors	Often incomplete.
Vendor Security Posture	Limited insight.
Aggregation Risk	Common dependencies among vendors.
Security Policy	Vendor non-compliance.
Ongoing Monitoring	Warrants a cost-effective solution.

Three Essential Building Blocks

- **Program Design**
  - Solid program leaders with strong support from the CIO/CISO, C-suite executives, sourcing/procurement, and business unit leaders.
  - Partnering with legal and procurement departments to implement effective contract language/service level agreements, and embedding risk-based assessments into third party/vendor onboarding processes.
  - Aligning internal policies and business processes with regulatory requirements and best practices; establishing metrics to track and report on program effectiveness.
- **Third-Party Inventory and Baseline Assessment**
  - Developing an initial inventory, building trust, and canvasing to identify third parties/vendors at large and decentralized organizations.
  - Defining the program foundation including: efficient risk-based assessment and independent audit requirements and termination processes to secure data when relationships with third parties/vendors end.
  - Implementing periodic reassessment of existing vendors and developing automated capabilities to monitor vendor cyber risk and threat profiles.
- **Ongoing Monitoring**
  - Providing monthly (or quarterly) reports and analysis of risks.
  - Establishing feedback mechanisms for internal/external stakeholders and mechanisms for program improvement, such as an annual program review.

Third-Party/Vendor Threats and Concerns

Contractual	Who is responsible for what?
Incident Reporting	Contractually required to report?
Indemnification	Is cyber covered?
Data Protection/ Network Security	Are THEY prepared?
Integration	Connected to OUR network?
Regulatory Risk	Subject to same requirements?
Subcontractors	Who's watching THEM?

Key Recommendations

- **Establish a well-defined process.**
  - ‘Tier’ third parties/vendors with varying levels of access to sensitive data and trusted integration to the corporate network.
  - Leverage information classification/information protection program as another factor for prioritizing third party/vendor assessments.

- **Implement a cost-effective means of continuous monitoring.**
  - The cybersecurity profile of third-parties/vendors with access to corporate networks, systems, and data can change frequently.
  - Allows corrective and proactive action to be taken as risks/threats present themselves.

- **Align Third/Party Vendor Risk Management program with Security Operations and Incident Response capabilities.**
  - Create communication paths and integrate and align the program with related cybersecurity operations such as the security operations center (SOC) or managed security services provider (MSSP) and incident/breach response program.

Key Takeaways

Key Takeaways - Preparation

- Incident response plans
- Network and endpoint visibility
- Retainers: IR, legal, marketing and communications expertise
- Law enforcement contacts
- Cyber Insurance, understand what is covered, engage as early as possible
- Asset management
- Remediation plans

Key Takeaways - Response

- Engage senior management
- Validate claims
- Preserve evidence
- Engage external counsel and form the investigation and remediation teams
- Protect incident findings with attorney-client privilege
- Common communication channel
- Minimize information sharing on a need to know basis
- Know your notification requirements
- Plan for disclosure early-on
- Communicate effectively and in a timely manner

Key Takeaways - Remediation

- Delay disclosure and remediation until scoping is complete
- Be able to isolate critical systems and data
- Disaster recovery plan for critical systems
- Have offline back-ups
- Plan to scale IT services

Key Takeaways - Disclosure

- DON’T release the breach disclosure and details on separate dates
- Release the information to employees at the same time as your external communications (if disclosure is required)
- Prepare a special landing page to provide information to stakeholders
- Communicate to all audiences as often as you can – and do it simultaneously
- If the media breaks the story before disclosure, address inquiries as soon as possible – with the same statement, at the same time
- Don’t give any media preferential treatment, release the information to all the media almost simultaneously
- Understand media will continue to dig. It’s better to have 10 articles with the same information than 3 articles with different information

Market Trends

Capacity

- $1B in theoretical capacity spread between North America, London and Bermuda
- Common Primary Markets vary by market segmentation and industry class
- New capacity and products appear on what seems like a quarterly basis

Coverage

- While carriers are comfortable offering full limits across coverage grants for Liability insuring agreements, varying appetites exist for first party insuring agreements
- Broad Business Interruption coverage Triggers and Dependent/Contingent Business Interruption are generally only granted by a select few carriers via a thorough underwriting process (in some cases, critical BPO or Cloud providers must be scheduled)

Appetite

- Continues to evolve; a comprehensive underwriting process, i.e. application + underwriting calls, are increasingly required for certain industry classes. More specifically, underwriters are placing increased scrutiny on Healthcare, Retail, Education, Energy, & Financial Institutions.
- Technology E&O remains a favourable class of business for most markets.

Retentions

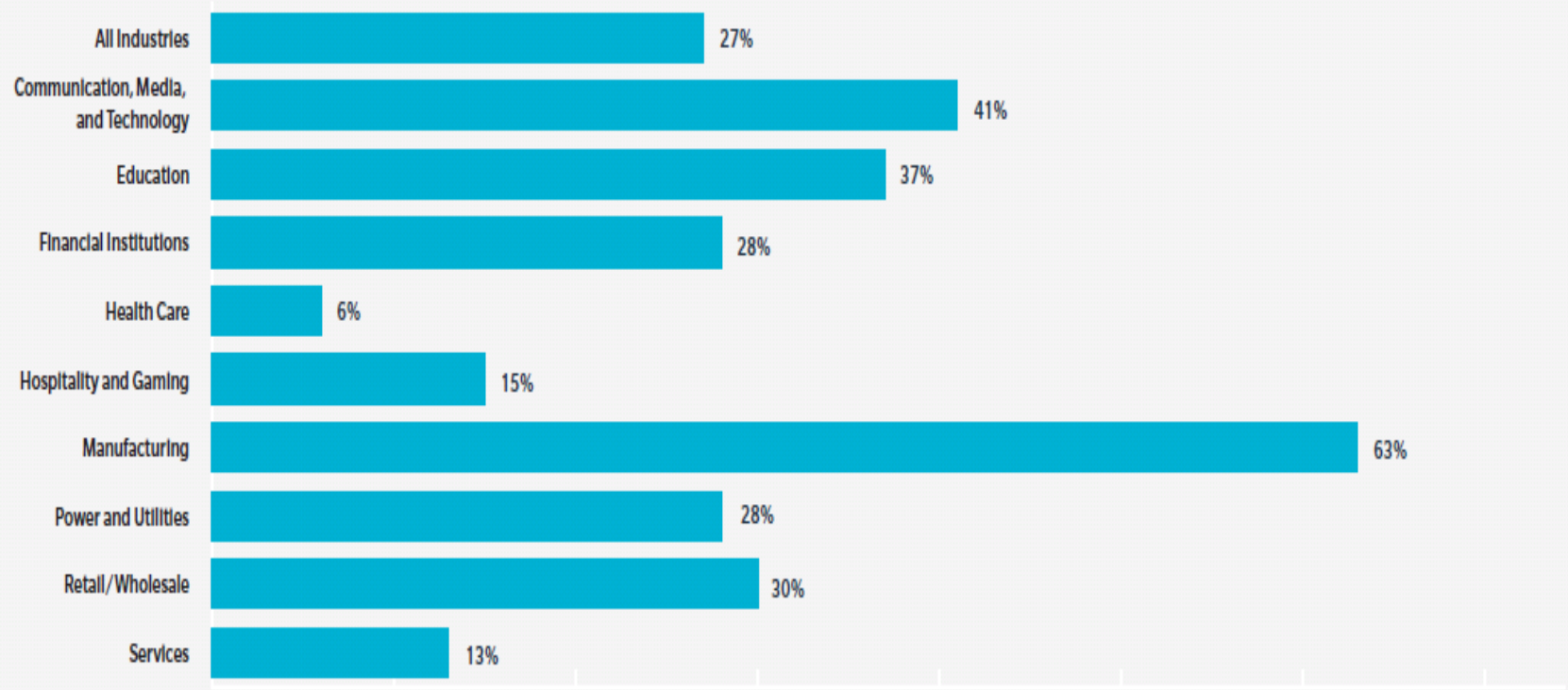
- Desired retentions are heavily dependent on internal risk philosophy and industry class
- For organizations with >$1B in revenue - retentions ≥$1M may be required (depending on industry class) and will usually lead to full limits across all insuring agreements
- Increasing retentions lead to nominal premium savings (hence, the cost/benefit is not usually justified)

Pricing

- Premiums are generally derived via a combination of overall exposure, the control environment (maturity of InfoSec program), industry class, retention level and scope of coverage desired
- Rate increases of 0-10% for average to good risk profiles is not uncommon; higher increases are being sought for Retail and Healthcare risks

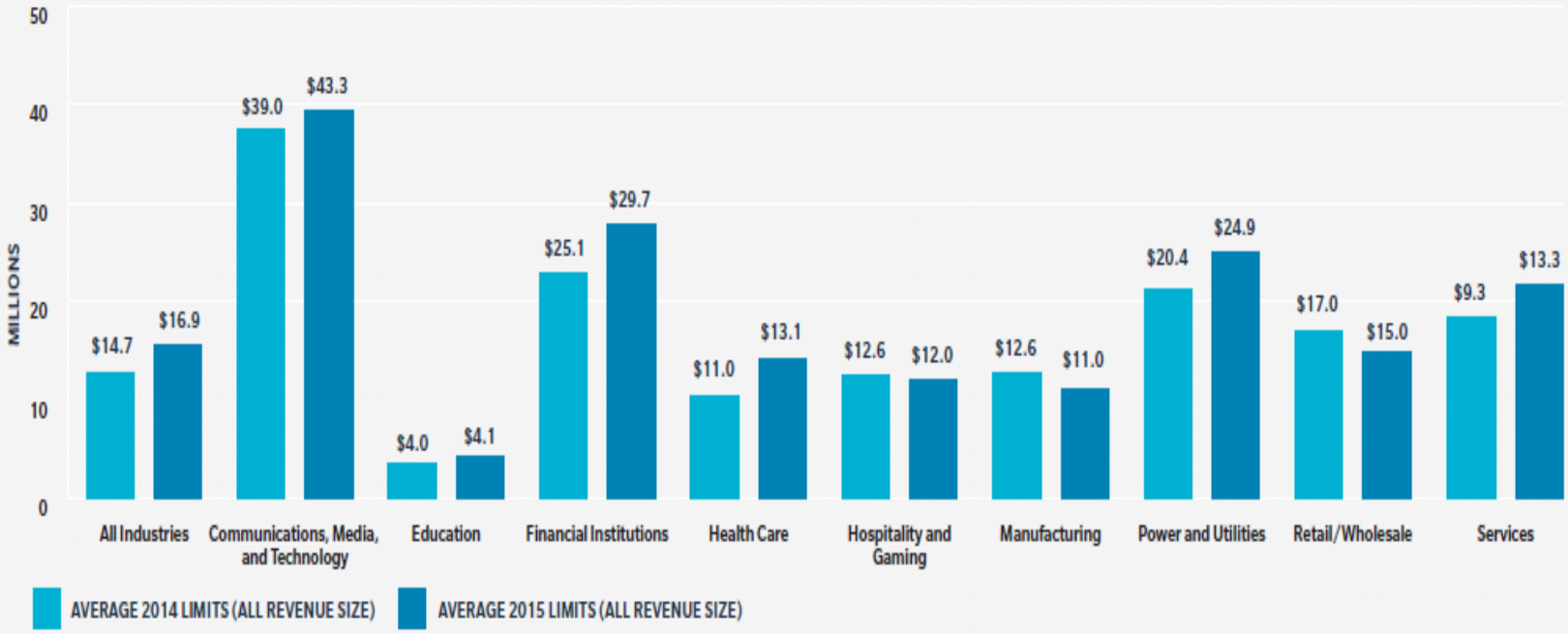
Buying Patterns

FIGURE 1: 2015 Cyber Insurance Growth Rates by Industry (Marsh Clients)
Source: Marsh Global Analytics



Buying Patterns

FIGURE 4: Cyber Liability Total Limits Purchased (All Size Revenues/Marsh Clients)
Source: Marsh Global Analytics



Underwriting Considerations

Cyber & Network Security Underwriting Topics

Security Organization

- Who is responsible for oversight of the information security of the organization?
- How often is the Board of Directors given presentations or updates on information and privacy security risks facing the organization?
- Is there a committee on the Board, or lead director, responsible for information and privacy security oversight?
- Please provide an overview of the information security / privacy training conducted for employees?

Security Policy & Standards:

- Please provide an overview of the Information Security Policy, Privacy Policy and Acceptable Use Policy.
  - What are the key elements of the policy?
  - Who is responsible for oversight of the policy?
  - How is the policy implemented and monitored?
  - How often is the policy reviewed and updated?

Physical & Environmental Security:

- What kind of employee fraud monitoring and employee activity monitoring is done?
- Does the organization have a periodic confirmation of user access process? If so how often is this done?
- How many unique identities does the organization have on its networks?

Cyber & Network Security Underwriting Topics

Computer & Network Management:

- When was the most recent vulnerability assessment conducted?
- Please describe programs in place to detect Phishing.
- What network tools does the organization collect incidents from? (Firewall, DLP etc.)
- What tools are used for wireless intrusion detection?
- Please discuss the PCI data flow. (The assessment indicates no encryption of data at rest. It appears that the organization does not encrypt laptops either. Please outline what protections are in place in lieu of encryption.)
- Please provide an overview of the encryption program for the organization.
- Has the organization completed encryption of all mobile devices?
- Please describe the process for response when your file integrity monitoring technology flags an event that requires a response. How is threat intelligence/monitoring incorporated into the organization's security efforts? What are the primary sources of threat intelligence? Please describe a recent instance in which a change in the threat environment triggered a response at the organization. Do you have a team tasked with monitoring these logs in near real time, and responding to detected incidents?
- Does the organization have Data Loss Prevention (DLP) software installed?
- Please discuss the results of the latest scans and annual penetration test.
- Does the organization have a process and tools in place to identify unauthorized equipment on the network, and to maintain a complete and accurate inventory of all authorized systems connected to the corporate network?
- Does the organization employ 2-factor authentication for sensitive functions and/or actions?
- Does the organization have tools in place that keep unauthorized software from executing (e.g. application whitelisting)?

Cyber & Network Security Underwriting Topics

Access Control:

- Please provide an overview of the IT network, including control centers, data centers, and significant connections with third parties (where sensitive data or operationally-critical data is exchanged or stored).
  - Please discuss the key technologies that are deployed to protect data and operations.
  - Where is sensitive information encrypted?
  - Is there network segmentation? Given the different lines of businesses, please elaborate on what type of segmentation is in place, if any. Is all information aggregated, or is it segmented with no way to get from one database (holding sensitive information) to the other database holding sensitive information?
- Please provide an overview of remote access technologies/ controls.
- Does the organization have a process in place to control and limit the assignment and use of administrative privileges on all equipment and software?

Compliance:

- Please discuss the annual compliance assessment process.
- Please provide an overview of the log monitoring process.
  - Is this process outsourced or is it conducted in house with 24x7 monitoring?
- Please provide more details on threat awareness controls and how the organization monitors network security for malicious activity (i.e. activity analysis/SIEM (Fireye, Splunk, etc).
- Please provide more details on threat management and awareness of cyber threat intelligence from third parties.

Cyber & Network Security Underwriting Topics

Vendor Management:

- Please provide an overview of controls in place for third party vendor access (what type of review happens before allowing access, does the organization require 2-factor authentication for any third party to access their network, etc.).
- Please provide overview of the vendor management program. How are vendors vetted and what are the requirements that each vendor must meet to become an approved vendor? Who oversees the vendor management process?

Business Continuity and Incidence Response:

- Please provide an overview of the Company's Incident Response Plan as respects to network security and privacy breach scenarios?
  - How would a cyber-attack that materially impacted the operation of a critical asset or system be addressed to minimize operational disruption?
  - What was the actual Return to Operation from the last Business Continuity exercise?
  - Please discuss the organization's Back-up procedures.

Cyber Insurance Terminology

- **Cyber Liability:**
  - liability to a third party as a result of ABC Corp's failure to properly handle, manage, store or otherwise control personally identifiable information in its care, custody or control, or such failure by an independent contractor that is holding, processing or transferring such information on behalf of ABC Corp. This coverage also includes an alleged violation of privacy laws including failure to timely disclose a security breach.
  - liability to a third party as a result of a failure of ABC Corp's network security to protect against destruction, deletion or corruption of a third party's electronic data, denial of service attacks against Internet sites or computers; or transmission of viruses to third party computers and systems.
- **Regulatory Defense & Penalties:** defense expenses and civil fines or penalties paid to a governmental entity in connection with an investigative demand or civil proceeding regarding actual or alleged violation of privacy laws.
- **Privacy Notification Expense:**; costs to provide notification in compliance with a breach notification laws; and costs for providing credit monitoring or other similar services to impacted individuals.
- **Breach Management Expenses:** reasonable and necessary costs to hire a computer security expert to determine the existence of and cause of a data breach; fees charged by an attorney to determine the applicability of and actions necessary to comply with breach notification laws; costs to hire a public relations firm for the purpose of averting or mitigating material damage to the ABC Corp's reputation as it relates to the coverages afforded by a Cyber policy.
- **Data Asset Protection:** recovery of the ABC Corp's costs and expenses incurred to restore, recreate or regain access to electronic data from back-ups or from originals or to gather, assemble and recreate such electronic data from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction, deletion or damage.
- **Cyber Business Interruption:** reimbursement of ABC Corp's loss of income or extra expense resulting from an interruption or suspension of its systems due to a failure of network security to prevent a security breach.
- **Cyber Extortion:** ransom or investigative expenses associated with a threat directed at ABC Corp to release, divulge, disseminate, destroy, steal, or use confidential information taken from the ABC Corp, introduce malicious code into the company's computer system; corrupt, damage or destroy company's computer system, or restrict or hinder access to the company's computer system.

This is a brief summary of some of the more common coverages available under Cyber policies. For actual policy language, please fully review the contract.