MARSH

June 13, 2017

Cyber Risk for Higher Education

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES

CYBER RISK TRENDS AND THREATS

CYBER RISK THREATS AND TRENDS

HIGHER EDUCATION SECTOR

What Are Cyber Risks?

If an entity:

1. Handles/collects/stores confidential information.
2. Uses technology in its operations

Higher Education Threats

Marsh is the broker for more large Higher Education institutions than any other broker. We have experience with the unique risk factors of Higher Education which include:

- Highly skilled users.
- Culture of innovation and change.
- Requirements for collaborative, open systems.
- Many different stakeholders – departments, researchers, outside funders that want their own systems but also want those systems to interact with the university's systems.
- Unique data sets
  - Personal & Financial Information
  - Health Information
  - Intellectual Property
  - Retail data

- Large databases related to students, applicants, and alumni.
- Many systems include related health systems and their data.

CYBER RISK THREATS AND TRENDS

HIGHER EDUCATION SECTOR - EXAMPLES

TOP TEN HIGHER EDUCATION BREACHES (By Record Count)

1.	Maricopa County Community College	2,300,000
2.	North Dakota University	290,780
3.	University of Maryland, College Park	287,580
4.	Butler University	163,000
5.	Indiana University	146,000
6.	Southern New Hampshire University	140,000
7.	University of Central Florida	63,000
8.	Arkansas State University	50,000
9.	Riverside Community College	35,212
10.	Iowa State University	29,780

Maricopa County Community College District: Breach response cost over $26M and required notification of 2.3M people including current and former students, staff and vendors dating back over 30 years. Data hacked included SS#s and banking information.

University of Maryland: 287,580 records including name, SS#, date of birth, and university identification number of (1) all faculty, staff and students who were in possession of a university ID anytime between 1998 and February 18, 2014; and (2) students who attended UMD between 1992 and 1998. Offered 5 years of ID theft monitoring.

Southern New Hampshire University: 140,000 records including student names, email addresses and IDs, course names, selection and instructors due to 3rd party vendor configuration error.

University of Central Florida: 63,000 records, due to unauthorized access into the university system. The data compromised included financial, medical, grades and social security numbers. One year of free credit monitoring was offered.

University of Virginia: 1,440 records including personal and financial data due to a cyberattack of the HR system. The attack was initiated by a phishing email to an employee asking for usernames and passwords to their HR system and one or more employees fell for the scam. The information compromised included data from W2 forms. The FBI led investigation resulted in arrests.

Penn State College of Engineering: Servers were hacked on two occasions by hackers believed to be in China and may have exposed sensitive data of at least 18,000 people. Notification was sent to employees and faculty.

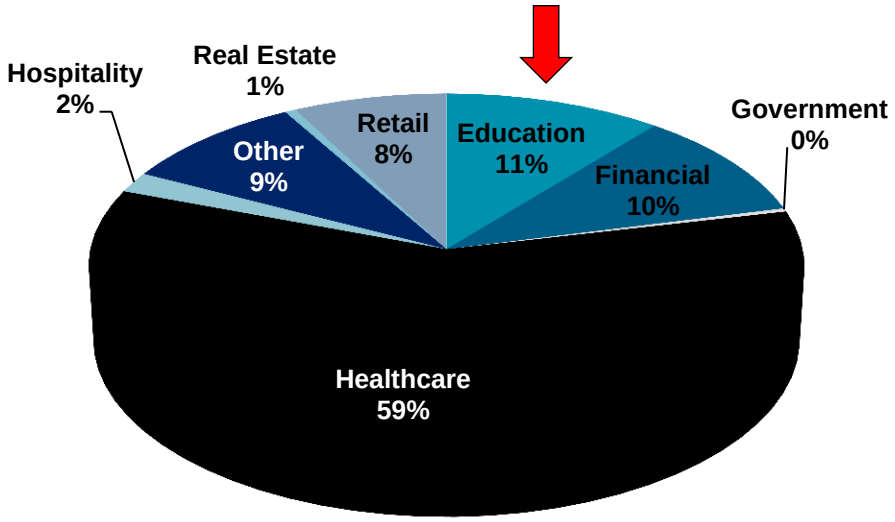
Other (Ransomware) -- June 2016 -- The University of Calgary was hit by a ransomware cyber-attack and paid out $20,000 in connection. Apparently, 9,000 student and faculty emails were incapacitated for several days.

2005 to date: More than14 million records from 771 publicly disclosed breaches.

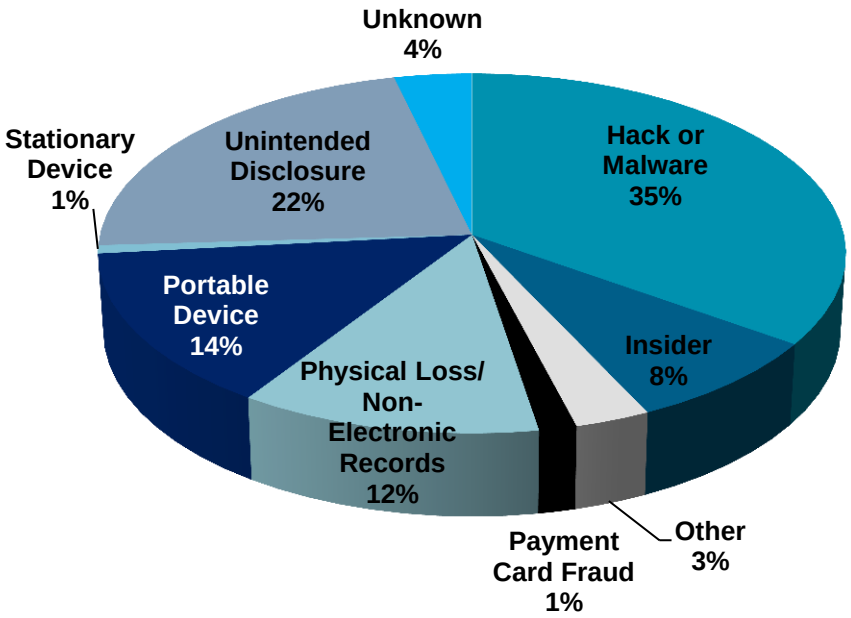
CYBER RISK THREATS AND TRENDS

BY THE NUMBERS

2015 Incidents by Industry



2015 Higher Education Incidents



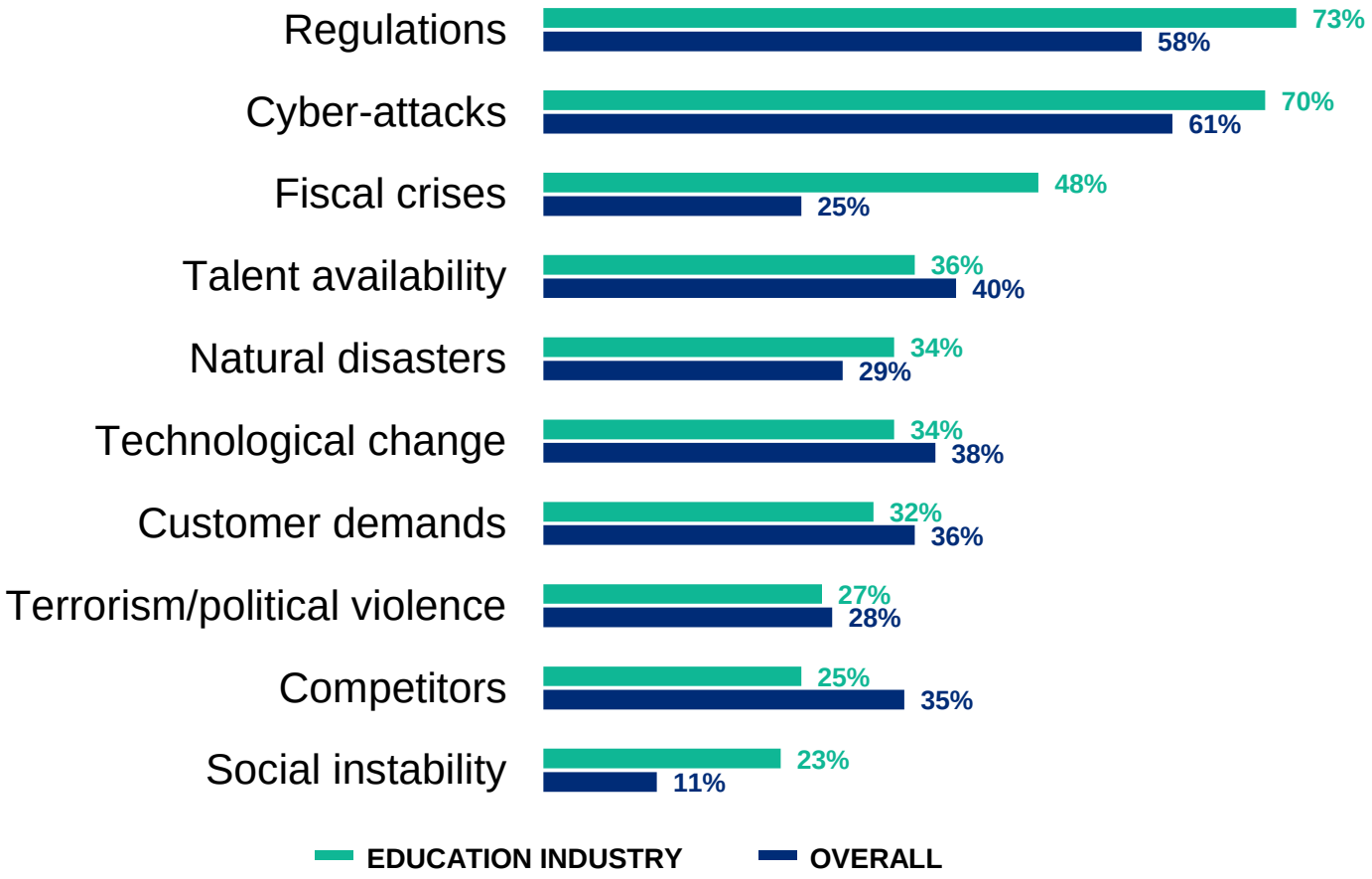
Source: Beazley – 2015 statistics

CYBER RISK THREATS AND TRENDS

HIGHER EDUCATION SECTOR – EMERGING RISK SURVEY

EMERGENCE OF CRITICAL RISKS FOR THE EDUCATION INDUSTRY

FROM WHICH OF THE FOLLOWING AREAS DO YOU THINK THE NEXT CRITICAL RISKS FOR YOUR ORGANIZATION WILL EMERGE?

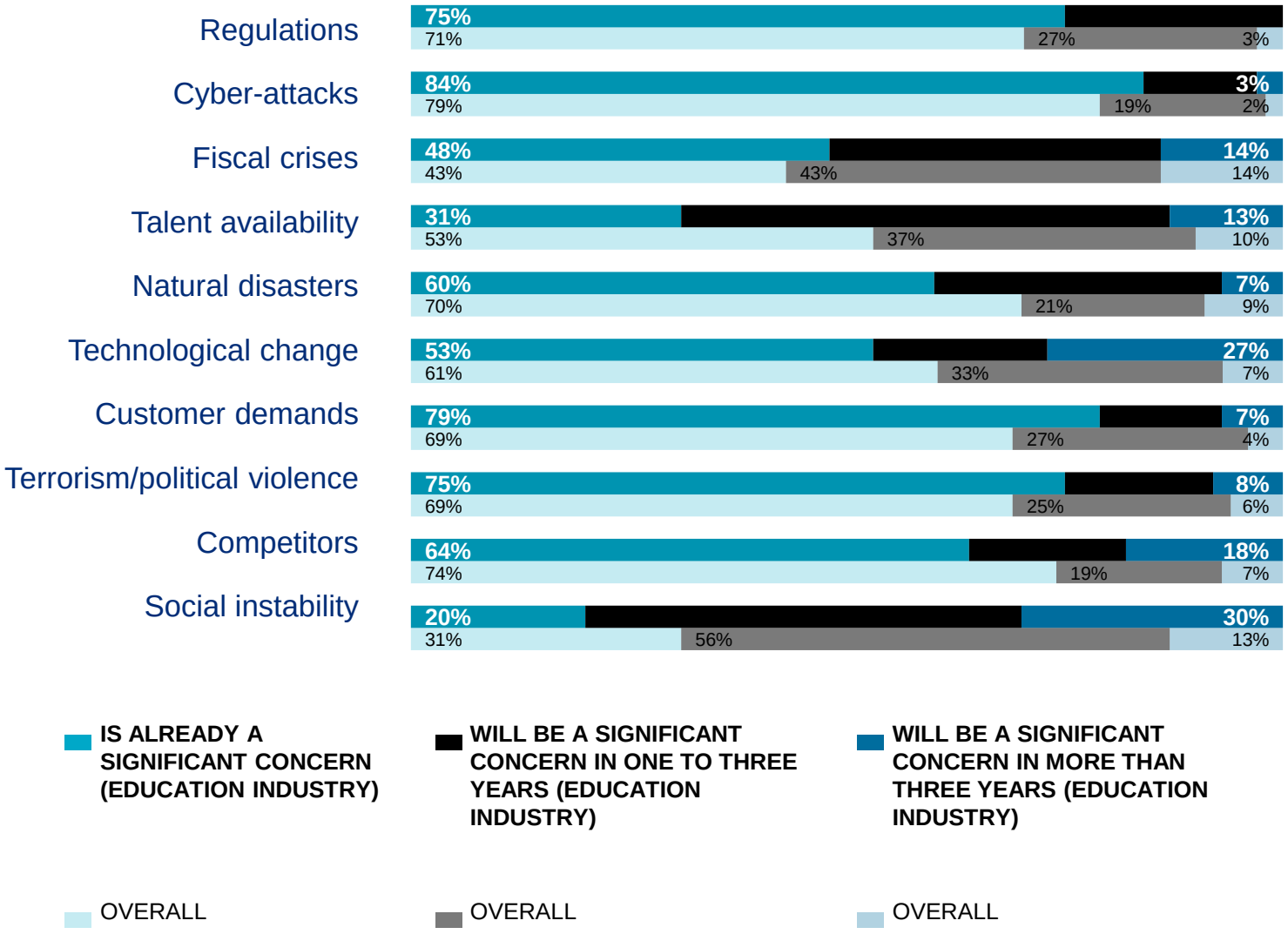


CYBER RISK THREATS AND TRENDS

HIGHER EDUCATION SECTOR – EMERGING RISK SURVEY

EMERGENCE OF CRITICAL RISKS FOR THE EDUCATION INDUSTRY

PLEASE STATE THE TIME FRAME IN WHICH YOU THINK THE NEXT CRITICAL RISKS WILL IMPACT YOUR ORGANIZATION.



UNDERSTANDING YOUR RISK PROFILE

MARSH'S CYBER RISK MANAGEMENT FRAMEWORK

Understanding your attack scenarios and risk profile is vital to addressing cyber risks. We help you identify assets, quantify the threat environment, assess your controls, and model the potential impact of events.

Key Concepts:

- Scenarios must be customized
- Assessment must be objective
- Analysis must be quantified and economic

Managing your cyber risks means preparing your business for the inevitable event. We help you optimize the security controls that protect and detect threats, and transfer exposures off your balance sheet.

Key Concepts:

- Security & Insurance go hand-in-hand
- Decision making must be coordinated between InfoSec and Risk Management

Quick, effective response to a cyber event is crucial for your business. We guide and support you through the event, and enhance your protection moving forward.

Key Concepts:

- Response is equally important as analysis and prevention
- Experience and expertise are critical to success

OVERVIEW OF THE CYBER INSURANCE SOLUTIONS

CYBER INSURANCE SOLUTIONS

KEY COVERAGE PARTS

Coverage	Description
Network Security and Privacy Liability	Defense and liability for failure to keep information private or for failure of others that have been entrusted with information to keep it private. Failure of systems to prevent spread of virus or a denial of service to those that rely on systems due to a failure in network security. Likely claimants would be customers, employees, credit card purchasers, card issuing banks.
Regulatory Action Defense	Reimbursement for costs to respond to a subpoena from federal or state regulators in connection with actual or alleged violation of privacy laws. It covers the legal defense as well as fines and penalties, if insurable by applicable law.
PCI –DSS Assessments	Written demands received from a card association or acquiring bank for a monetary assessment of a fine or penalty due to your non-compliance with PCI Data Security Standards
Tech. E&O	Defense and liability for the failure to render technology services Likely claimants would be customers and other third parties

CYBER INSURANCE SOLUTIONS

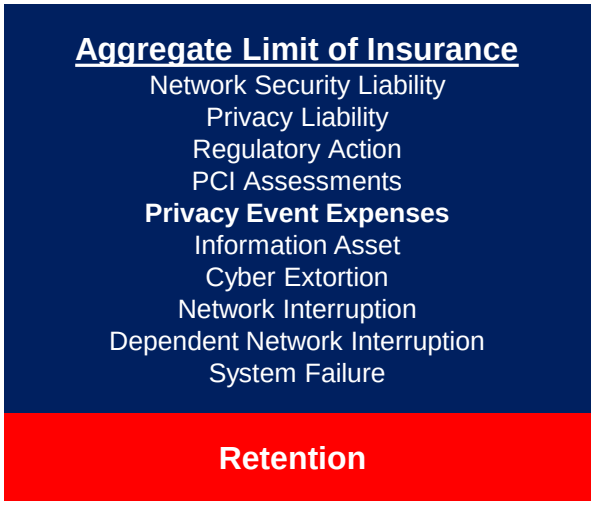
KEY COVERAGE PARTS

Coverage	Description
Privacy Event Expense	The cost of a forensic investigation to identify what has happened and whether, and / or whom, needs to be notified of the event. The engagement of privacy counsel to determine the necessary course of action to comply with privacy and other data breach legislation. The costs to notify affected individuals and, if applicable, the operation of a call center and the cost of identity / fraud / credit monitoring services.
Information Asset/Electronic Data Protection	Reimbursement for the cost to restore, replace or recreate data lost, damaged, corrupted or stolen as a result of a failure of network security or introduction of malicious code.
Cyber Extortion	Costs of consultants and extortion monies for threats related to interrupting systems and releasing private information
Network Business Interruption	Loss of income or extra expense due to a material system interruption as a result of a failure of network security, denial of service attack or other introduction of malicious code beyond a waiting period of approximately 10-12 hours.
Contingent Network Business Interruption	Loss of income or extra expense due to a material system interruption of a dependent outsourced provider's network as a result of a failure of network security, denial of service attack or other introduction of malicious code beyond a waiting period of approximately 10-12 hours.
System Failure	Expansion of the Network Business Interruption coverage trigger to include "any unplanned outage" (examples include an administrative error or programing error)

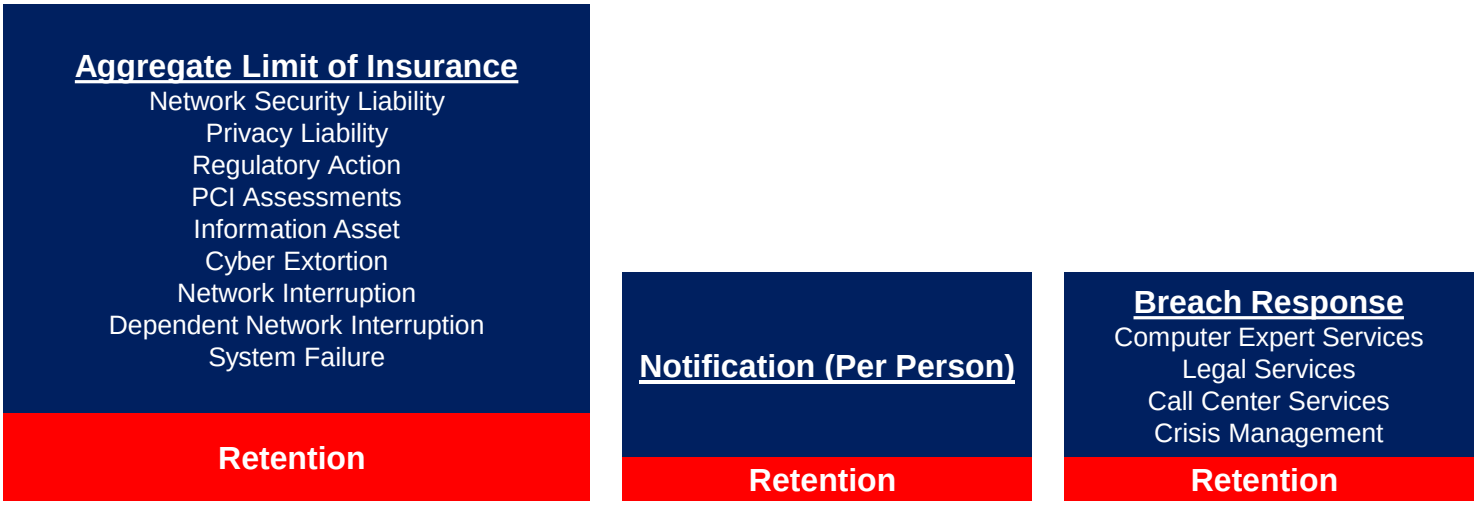
CYBER INSURANCE SOLUTIONS

KEY COVERAGE PARTS – CONSIDERATIONS FOR PRIVACY EVENT EXPENSES

Option #1 – All Limits Inside the Dollar Aggregate



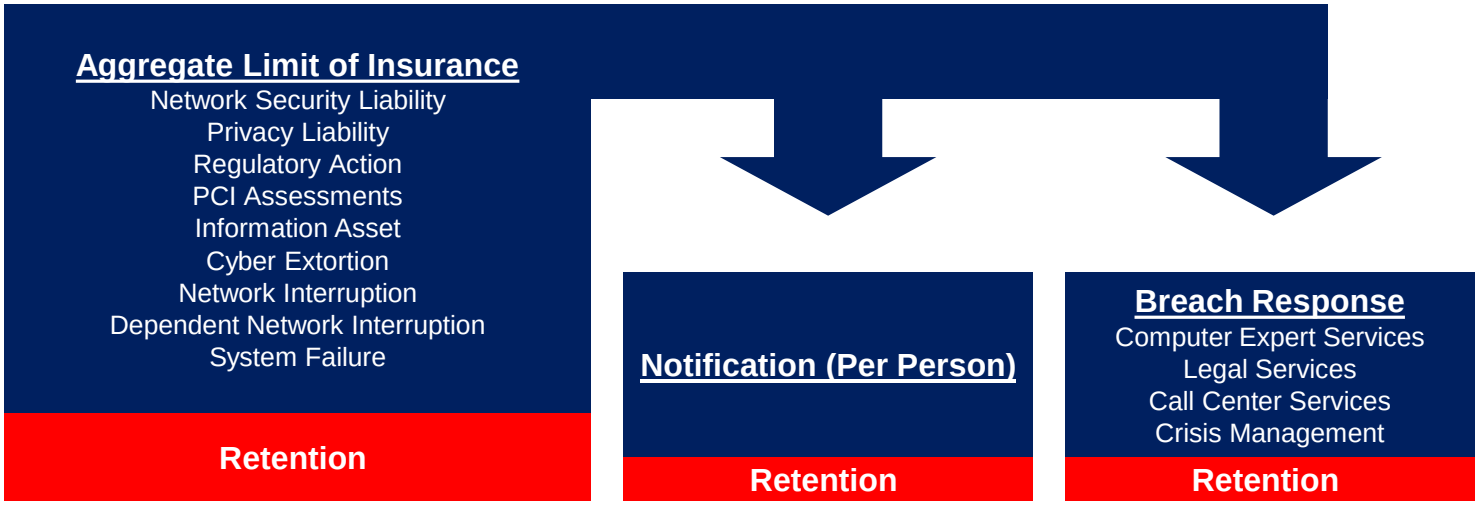
Option #2 – Privacy Event Expenses ("Breach Response") Outside the Limit



CYBER INSURANCE SOLUTIONS

KEY COVERAGE PARTS – CONSIDERATIONS FOR PRIVACY EVENT EXPENSES

BBR Boast Structure



CYBER INSURANCE SOLUTIONS

KEY COVERAGE PARTS – CONSIDERATIONS FOR PRIVACY EVENT EXPENSES

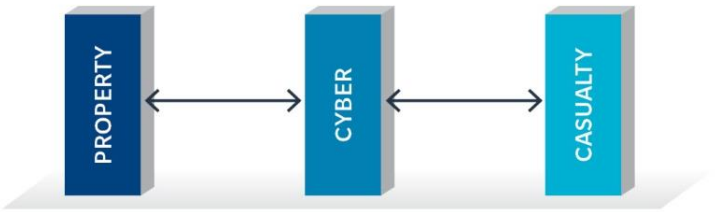
Additional Structure Considerations

UNMANAGED

- Independent towers
- No coordination

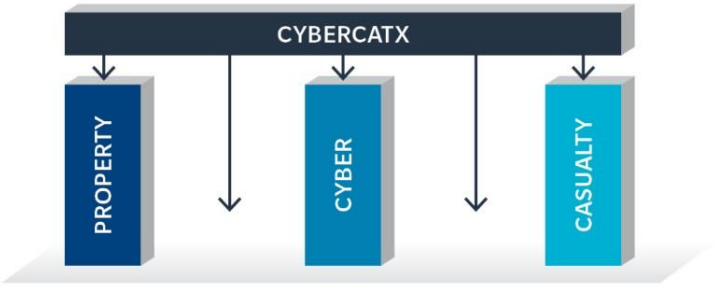
CYBERPAK-ALIGNED

- Independent towers
- Linked & aligned with CyberPak endorsements



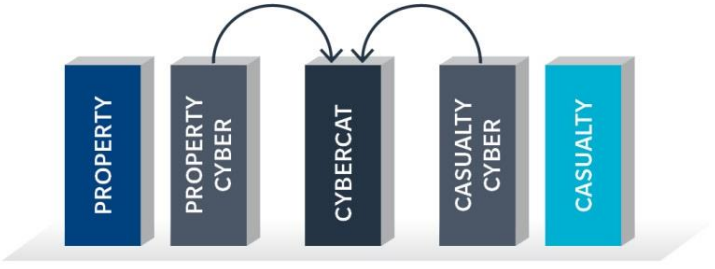
CYBERCATX

- Independent towers
- Excess/DIC protection from CyberCatX



CYBERCAT

- Cyber tower with P&C elements

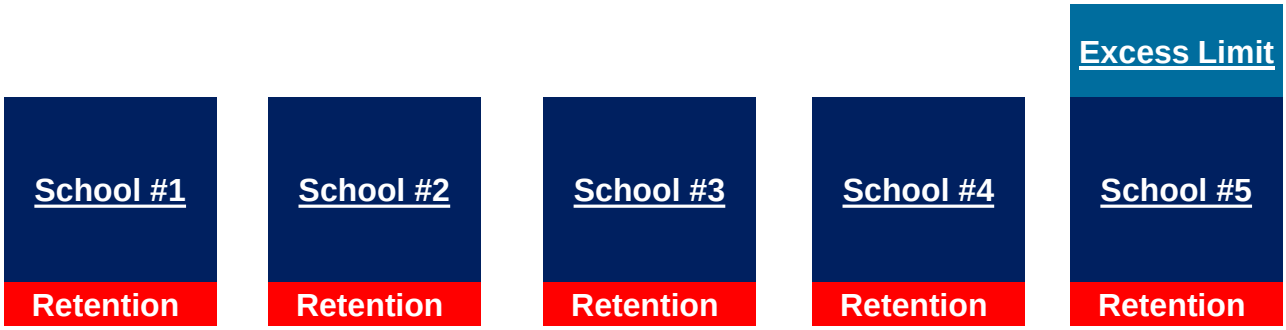


CYBER INSURANCE SOLUTIONS

KEY COVERAGE PARTS – GROUP PURCHASING PROGRAMS

Marsh has constructed several Higher Education Group Purchasing Programs that aim to provide broader coverage, best in class breach response services, and more competitive pricing than if a member institution were to purchase coverage on its own. Some potential structural considerations include (but are not limited to):

Option #1 – Individual Policies Per School: Group Purchase With One Insurer



Option #2 – Individual Policies Per School: Shared Excess Aggregate

Option #3 – Shared Group Aggregate

OVERVIEW OF THE CYBER INSURANCE MARKET

CURRENT CYBER MARKET CONDITIONS

RATE TRENDS

In Q1 2017, cyber rates decreased by an average of 1.7% for all industries within Marsh's client base. The median result was flat. What is more encouraging is that we were able to deliver decreases to 38% of our clients, compared to 16% in Q1 2016, which is more than any of the previous 4 quarters. 42% of clients renewed with an increase, compared to 79% in Q1 2016.

The retail sector's rates were down slightly, with average and median decreases of 2.1% and 2.2%, respectively. Rates in the health care sector are mixed, with an average decrease of 8.0% and a median rate increase of 1.8%. When we remove retail and healthcare renewals from the data, we were able to deliver flat renewals, on both a median and average basis. We anticipate this rate environment to continue through Q2 of 2017.

MARKET TRENDS

Competition amongst insurers is strengthening for clients in all revenue segments and all industry sectors, including higher exposure classes like retail and health care as well as emerging classes like critical infrastructure and manufacturing. Sublimits for certain cyber coverages (e.g. notification, payment card, and regulatory costs) are trending higher, with many clients exploring "full" limits for these covers. Clients continue increasing their total program size, due in part to growing recognition of the risk. Overall, insurer appetite remains strong, with a market-wide focus on growth in 2017 and many insurers developing new coverages and services.

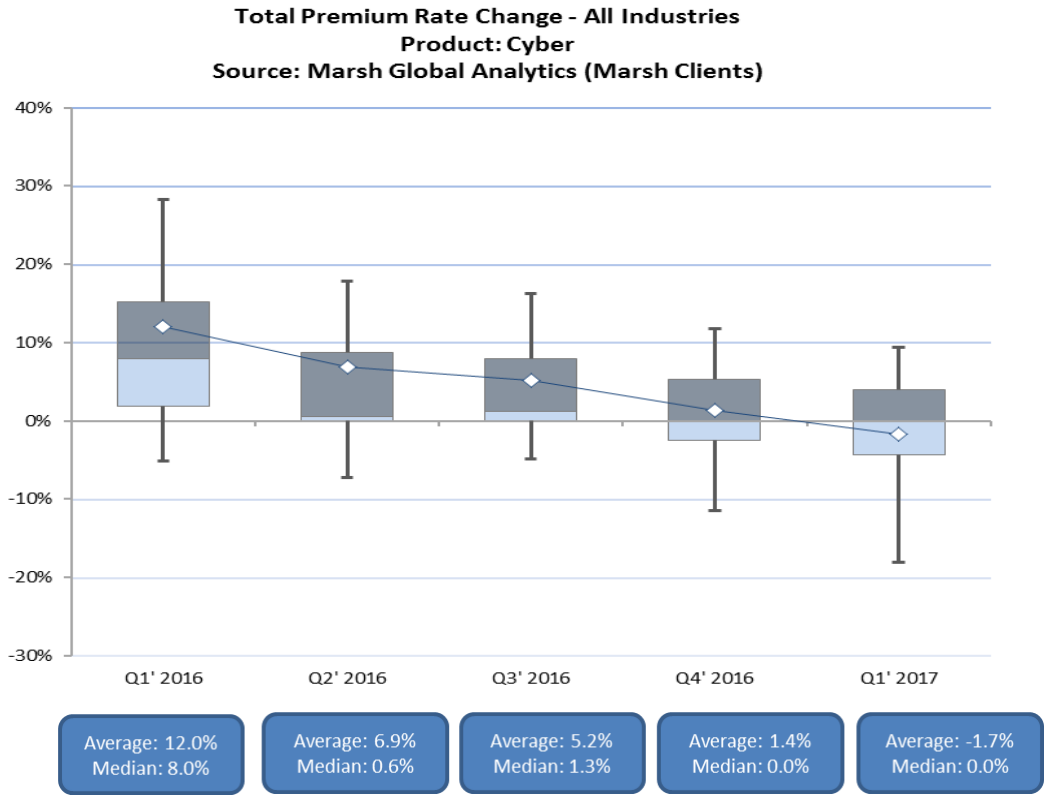
CAPACITY TRENDS

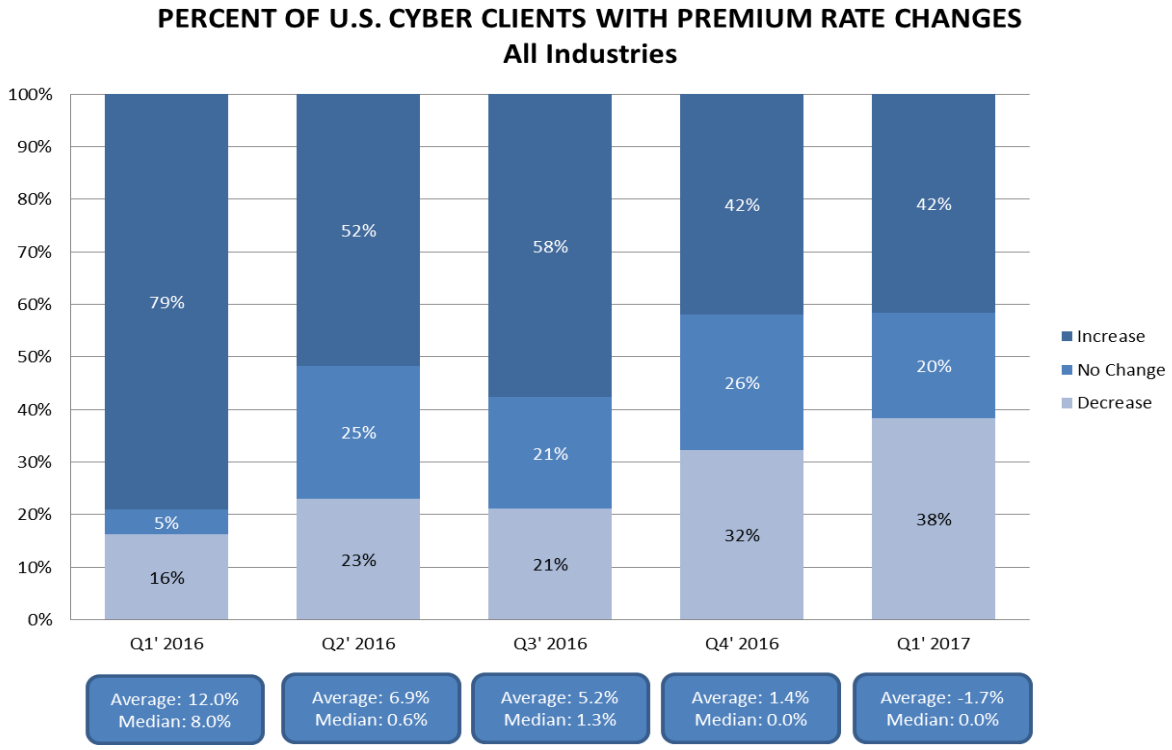
Insurers' increasing appetite for cyber risk has brought even more capacity into the marketplace, both from existing insurers as well as from new entrants and facilities. Notional cyber capacity exceeds $1.6 billion per our most recent survey, and insurers are increasingly willing to consider deploying large line sizes, either in single layers or with ventilation. In practice, total program size varies depending on industry and coverage, with many large towers placed between $200 million and $500 million in limits. In addition to Marsh's Cyber $50MM ECHO Facility, several insurers have begun offering large blocks of capacity during the last 12 months, including AIG, Chubb, and a tandem effort from Beazley and Munich Re.

CLAIMS TRENDS

Cyber claims continue their growth stemming from numerous cyber extortion and cyber crime events. Recent high profile outages have underscored business interruption events as a growing concern amongst insureds. Data breaches continue to be a challenge for clients across all segments and industries, though we have not seen any industry-wide cat events in some time. In particular, payment card industry (PCI) fines and assessments have spiked, which has in turn resulted in claims being paid by the PCI sublimits present in many programs.

CURRENT CYBER MARKET CONDITIONS





CURRENT CYBER MARKET CONDITIONS

US MARKETS

- Admiral
- AEGIS
- AIG
- Allianz
- Arch
- Argo
- Aspen
- AWAC
- Axis
- Beazley
- Berkley
- Berkshire Hathaway
- Chubb
- CNA
- CV Starr
- Endurance
- Euclid
- Hartford
- HCC
- Hiscox
- Ironshore
- Liberty Mutual
- Markel
- NAS
- Nationwide
- One Beacon
- Philadelphia
- QBE
- RLI
- RSUI
- RT Specialty (wholesale)
- SCOR Re
- Swiss Re
- Think Risk
- Travelers
- Validus
- Westchester
- XL
- Zurich

LONDON MARKETS

- AIG
- Amlin
- Antares
- ANV
- Aspen
- Axis
- Barbican
- Beazley
- Brit
- CFC
- Chanel
- Chubb
- Emergin Risk
- Equinox
- Hanover Syndicate
- Hiscox
- Kiln
- Liberty
- Markel
- Munich Re
- Navigators
- Novae
- Principia
- Ptarmigan
- QBE
- RT Specialty
- SCOR UK
- Swiss Re
- Talbot
- XL
- Zurich

BERMUDA MARKETS

- AIG (AIRCO)
- Arch
- Argo
- Aspen
- AWAC
- Axis
- Chubb
- Endurance
- Ironstarr
- Markel
- XL

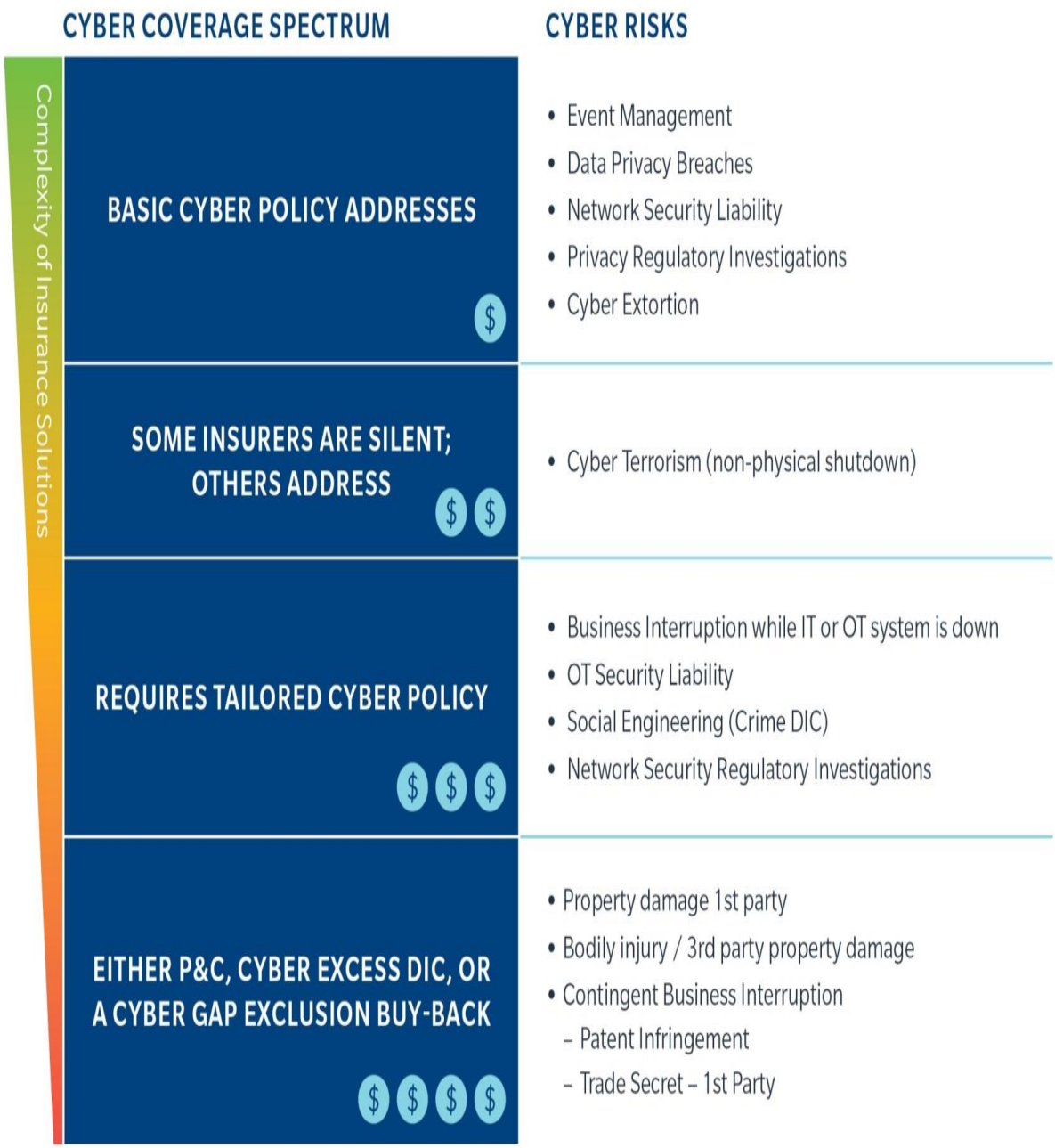
$1.6B (+) IN MARKET CAPACITY

Marsh has access to over 80 markets that provide capacity for E&O and Cyber placements. While the below chart is not an exhaustive list, it does include the most common markets participating within the space.

CYBER ECHO

New facility launched in January 2016, providing up to $50 M in capacity for stand alone cyber programs. Reinstatement of limits provision also included in the form.

CURRENT CYBER MARKET CONDITIONS



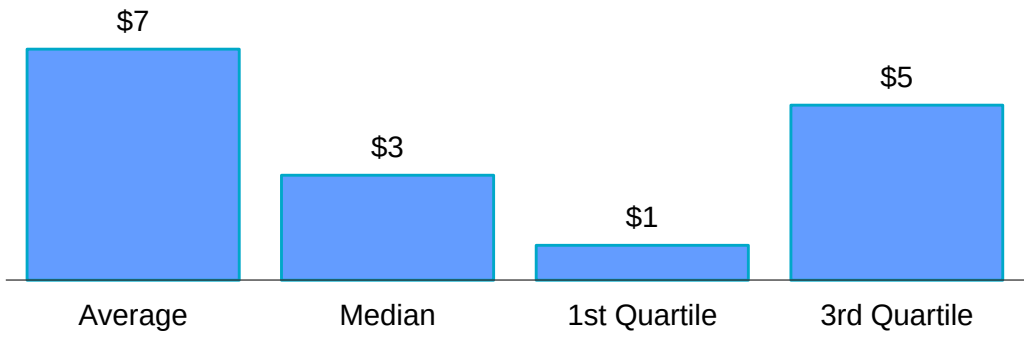
CURRENT CYBER MARKET CONDITIONS

CYBER TOOLKIT & ANALYTICS: MARSH PEER BENCHMARKING

Peer Group Summary	Higher Education
Revenue Range	All Sizes

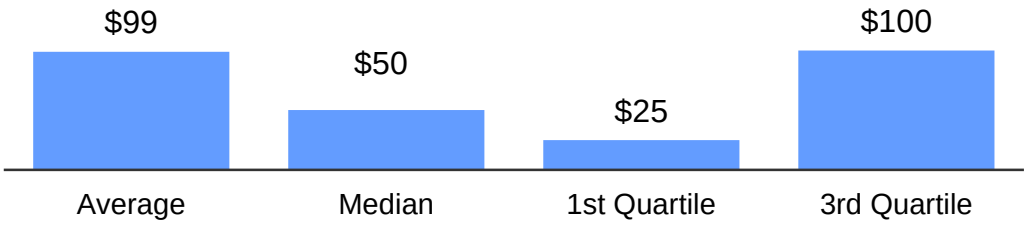
Total Limits ($Millions)

Max: $100 Min: $0.50



Retention ($Thousands) – 81 Peers

Max: $1,000 Min: $3



Peer Group Pricing Summary	1St Quartile	Median	Average	3rd Quartile
Primary Price Per Million	$8,996	$12,477	$15,301	$16,997
Total Price Per Million	$8,996	$12,477	$14,704	$16,014

SUBMISSION REQUIREMENTS AND CONSIDERATIONS

- Marsh Cyber Assessment
- Standard Insurer Application
- Insurer underwriting call/meeting with information security representative
- Sample underwriting topics:
  - Overview of Data/Information Held by the Insured
  - Data/Access Controls
  - Loss Experience
  - Regulatory Compliance
  - Security and Privacy Culture – Including Overview of Information Security Team
  - Overview of Vendor Management Practices
  - Business Continuity, Disaster Recovery and Crisis Management

RESPONSE STEPS

RESPONDING TO A DATA BREACH

Response Steps

1. Receive initial report
2. Assemble breach response team
3. Initial internal communications (who needs to know?)
4. Engage external counsel
5. Investigate
6. Validate nature and extent of the incident
7. Containment, control and correction
8. Notifications: who, when, where, how and what
9. Conclude investigation and prepare incident report
10. Retain report

What was the cause of the event?

What type of data was involved?

How do you notify victims of the event?

What is your deliverable to the victims?

Do you need to provide a call center or credit monitoring?

APPENDIX

APPENDIX A. *CLAIMS EXAMPLES/SCENARIOS*
APPENDIX B. *RISK IN CONTEXT*
APPENDIX C

CLAIMS EXAMPLES/SCENARIOS

Example #1

A state university is investigating a security breach by a vendor who, while under contract with the university, coped information from a check register database without permission. The action may have compromised the private information of 21,000 students and employees who were associated with the university over a fourteen year period.

Example #2

Insured accidentally published confidential information regarding 117,000 students on their website. The Insured hired forensic experts to determine the precise amount of information, and the number of students who were affected. Additionally, the Insured sent notification letters to all impacted students, and a call center was created to address concerns of the affected students.

Example #3

The Insured, a university, was the target of an email spear-phishing scam pursuant to which the perpetrator appears to have spoofed valid email addresses of two university administrators so that they appeared to be internal email messages. The perpetrator initiated separate communications with two different university employee recipients requesting PDF attachments of W-2 information and earning summaries for all employees. One employee responded, forwarding attachments of W-2 forms for the periods of 2015 and 2016, which resulted in the release of employee names, home addresses, Social Security Numbers, and earnings information. The insurer worked with the Insured, privacy counsel and a forensic vendor to confirm that the impersonation of employee email addresses originated from outside the university network, and that the event did not involve domain penetration, forced seizure of digital assets, or domain account/password hijacking. The insurer also worked with the Insured to recommend appropriate credit monitoring and notification services.

Example #4

A hacker broke into a university computer system holding financial data of 80,000 students, alumni, current and former employees. Those notified include students and staff who received non-salary payments though electronic fund transfers, such as financial aid awards and work-related reimbursements. Vendors whose financial information was in the system for payment purposes are also at risk.

Example #5:

Employee stole trade secrets over a period of five months from a large corporation. The trade secrets were valued at over $400 Million. The employee had been employed as a scientist at the firm for more than 10 years. The data stolen included 22,000 documents and 16,700 PDF text files. Some files involved products still in R&D mode.

Example #6

On Christmas Eve, an insured discovered that they were the victim of a ransomware attack. The ransom demanded was approximately $25,000 in Bitcoin. Privacy counsel and a forensic firm were immediately retained to work with the insured. As there is no known decryption key for this variant of malware and restoration from backup (including a determination of whether they could fully restore from backup) would take in excess of five days, a decision was made that payment of the ransom was necessary in this situation. The forensic team is currently investigating the root cause as well as whether there was any access to or exfiltration of any confidential business information, PII, or PHI

RISK IN CONTEXT – "WANNACRY MEANS GOTTAACT: LESSONS IN RANSOMWARE'S WAKE"

For many organizations, the past week brought an unwanted welcome to the new world of cyber risk. The "greeting" came from WannaCry, ransomware that disrupted the UK's health services, halted a French carmaker's production, interfered with a US logistics company's network, and shut down corporate offices in Asia, all in a matter of hours. The attackers sought an almost laughably small ransom from victims — as little as $300 per infected computer — but the ultimate disruption to the global economy will be much greater.

Endless Risks, Limited Resources

One clear lesson as we look to prevent the next cyber pandemic is that technological infrastructure may be more fragile than previously thought. That means firms must focus on the growing risk of cyber business interruption.

Greater connectivity and complexity among IT networks increases the risk that disruptions will cascade. Such effects may be felt even when your firm escapes the attack but your suppliers and providers fall victim. In fact, unplanned IT and telecom outages are the leading cause of supply chain disruptions1, and can lead to significant loss of revenue and extra expenses.

Three Critical Steps

Beyond addressing technical issues, businesses should consider these three lessons from the WannaCry attacks:

1.Build resilience through cyber response exercises. WannaCry was a novel piece of malware whose speed and impact were hard to anticipate. Firms should build flexibility, speed, and adaptability into their event-response capabilities. Test, test, and re-test your cyber response plan across your organization, and identify specialized resources and expertise as you do so. Assess new event scenarios — like complex ransomware threats — so you can quickly adapt to fast-moving events.

2.Update your risk modeling. Re-think the potential scenarios that could affect your operations, then work with business leaders to consider the potential operational and financial impacts. That can help you evaluate second- and third-order consequences — such as supply chain disruptions and associated financial costs — and determine which risks demand the most focus.

3.Review and update your cyber insurance program. Networks will continue to become more connected and businesses more dependent on data-sharing. Every business that relies on technology — and most do — should take a fresh look at their cyber insurance program. You should update policies as needed to provide coverage for business interruption and cyber extortion, and re-evaluate program limits in the face of catastrophic scenarios.

Ransomware and other evolving threats will increase in frequency and sophistication. Firms need a comprehensive cyber risk management strategy — including economic risk modeling, optimized cybersecurity and cyber insurance programs, and resilient cyber response capabilities, to ensure a quick, effective response and a timely return to normal operations.

Martin Leicht, CPCU, ARM
Assistant Vice President
Marsh | FINPRO | E&O and Cyber Practice
1166 Avenue of the Americas
New York, NY 10036
212-345-0197 | Cell 646-675-6827
Martin.Leicht@marsh.com
Marsh USA, Inc. | www.marsh.com