University of Oregon
Cyber Resilience Summit
Realities of Cyber Insurance

October 14, 2021, 1:30-2:30PM

University of Oregon
Cyber Resilience Summit 2021: Realities of Cyber Insurance

Panelist will discuss the realities of cyber insurance and the challenges driving the global cyber market with a focus on the dominant causes of market volatility, a real time update on market and claims trends, incident response management (navigating cyber incidents at large, ensuring preparedness to respond), cyber hygiene (best practices, tied to underwriter concerns) and analytical tools being used by carriers, brokers and buyers to help manage and control cybersecurity risk.

Realities of Cyber Insurance Overview

Realities of Cyber Insurance

Market Trends

Claims Trends

Incident Response Management

Cyber Hygiene

Buyer’s Perspective

Realities of Cyber Insurance Panel Overview

Catherine Brown
Senior Vice President
Education & Public Entity
UO Client Executive
Moderator

Annice Y. Ma, ARM
Vice President
Cyber Center of Excellence
Placement Advisor
Market Trends

John Scordo, Esq.
Senior Vice President
Cyber Claims Advocacy Leader
US & Canada
Claims Trends

Florence Levy, Esq.
Cyber Incident Management Director
US & Canada
Cyber Incident Management

James Holtzclaw
Senior Vice President
Cybersecurity Risk Consulting
Cyber Hygiene

Deb Donning. Esq.
University of Oregon Director of
Risk Management & Insurance
Buyer's Perspective

Market Trends

Annice Ma

Challenges Driving the Global Cyber Market Today

Ransomware

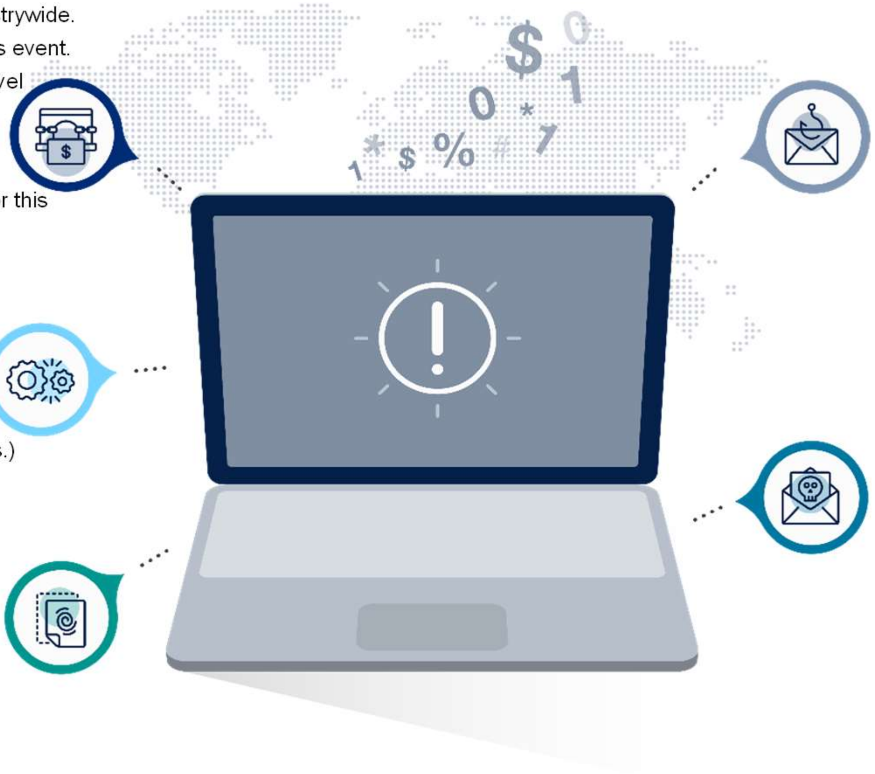
- Significant uptick since 2019, creating concern industrywide.
- Ransoms being paid in days/weeks – a short tail loss event.
- Proactive monitoring of performance at a portfolio level due to concerns of risk aggregation.
- Controls based risk selection has amplified underwriting scrutiny.
- Terms and conditions being readjusted to account for this growing trend.

Market Contraction

- Refined capital deployment strategy in response to large loss volatility and deteriorating performance.
- Insurers now see the “cyber” product line as both long tail (liability, regulatory) as well as short tail (ransom demand and breach response expenses.)
- There is now a significantly higher price for capital.

Coverage / Product

- Cyber coverage has broadened significantly in the past 7 years, e.g. Blanket Contingent Business Interruption cover, no sublimits, and customized policy language, which is now causing concerns for Insurers against the backdrop of deteriorating profitability.
- Scope of coverage is being scrutinized due to deteriorating profitability.



Frequency and Severity Beyond Ransomware

- Increasing sophistication and morphing nature of cyber attacks reshaping loss development patterns.
- An attacker only needs to be successful once; the insured 100% of the time.
- Insurers’ actuaries are revising their rating models to factor in higher frequency and severity, as well as modelling systemic events; this process improves as more data becomes available.
- Potential increases in regulatory fines & penalties, wrongful collection/ BIPA claims due to evolving privacy regulations.

Systemic Risk Driving Serious Concerns pertaining to Aggregation

- Difficulties in understanding and quantifying exposure – one vulnerability or piece of malware can affect thousands of organizations around the world.
- Increased awareness of aggregated cyber incidents and supply chain risk, causing capital volatility (Solarwinds, MS Exchange, Accellion, Kaseya, one after the other.)
- In past years when the market was soft, "systemic risk” had not been priced for – this has changed via increasing cat loads into the price of risk.

Market volatility in 2021 is creating new complexities and reinsurance implications

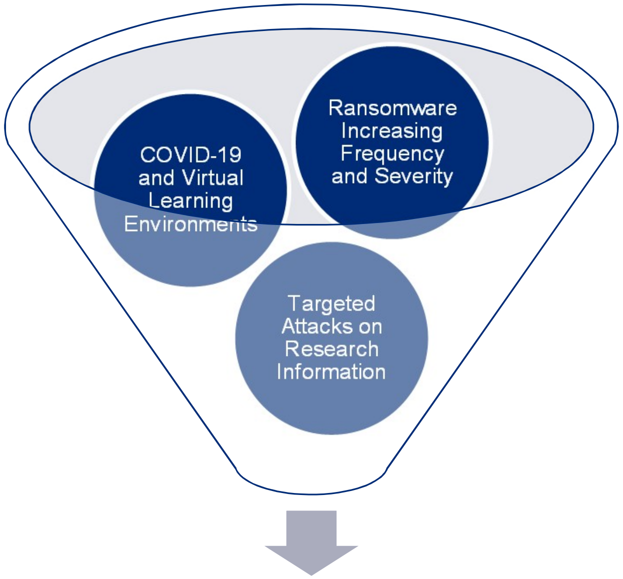
» Favors Buyer » Neutral » Favors Insurers

Cyber Insurance Market Snapshot

Claims	Rates	Capacity & Attachment	Underwriting	Coverage
⏫	⏫	⏬	⏫	⏬
Overall claims frequency and severity remains high driven by ransomware. Mild improvement in some categories but losses continue. Ransomware, systemic risk & regulations continue to drive concern.	Losses have accelerated pricing pressure even on loss free accounts with good controls. Excess pricing is increasing faster than primary, compounding increases. Expect increases to continue into 2022.	Claims activity and future uncertainty have insurers aggressively managing global capacity & increasing SIRs. Distressed classes & large towers may see capacity challenges.	Full application & responses to ransomware Q's are required; carriers using 3rd parties to externally scan environments. Also expect inquiries on recent supply chain events, biometric info, & operational technology.	Many carriers scaling back ransomware-related coverages, or not offering coverage if poor controls. More scrutiny on contingent business interruption (systemic risk) and regulatory cover (biometric information).
+55% YoY Increase In Loss Ratios, indicating an industrywide underwriting loss for 2020	**August Cyber Premiums:** **+113%** average increase **+155%** 3rd quartile increase **150%+ looking forward**	**August Cyber Renewals:** **21%** reduced limits **17%** increased limits **62%** increased SIRs Driven by insureds minimizing increases & less available capacity.	**12** Key Controls & Best Practices are now viewed by carriers as essential	⬆ in average BI / CBI waiting periods due to ransomware and supply chain attacks

Cyber Insurance Market Snapshot – Higher Education

Higher Education Cyber Risk Profile is Evolving


Ransomware Increasing Frequency and Severity
COVID-19 and Virtual Learning Environments
Targeted Attacks on Research Information

Changing Cyber Risk Profile for Higher Education

Cyber Insurance Market is Turbulent for Higher Education

- Rates are accelerated more quickly in the higher education space than the broader cyber marketplace.
- Carriers that are still willing to offer full ransomware coverage are demanding a premium for it.
- Control differentiation is critical – there are specific controls that the market sees as “minimum standards” – without these controls, some institutions may have trouble finding solutions.
- The capacity available for higher education risks is shrinking.

Rates	Capacity & Structure
Q3 Cyber Premiums: **+100%** average increase	**Q3 Cyber Renewals:** **26%** reduced limits **7%** increased limits **81%** increased SIRs Driven by insureds minimizing increases & less available capacity.

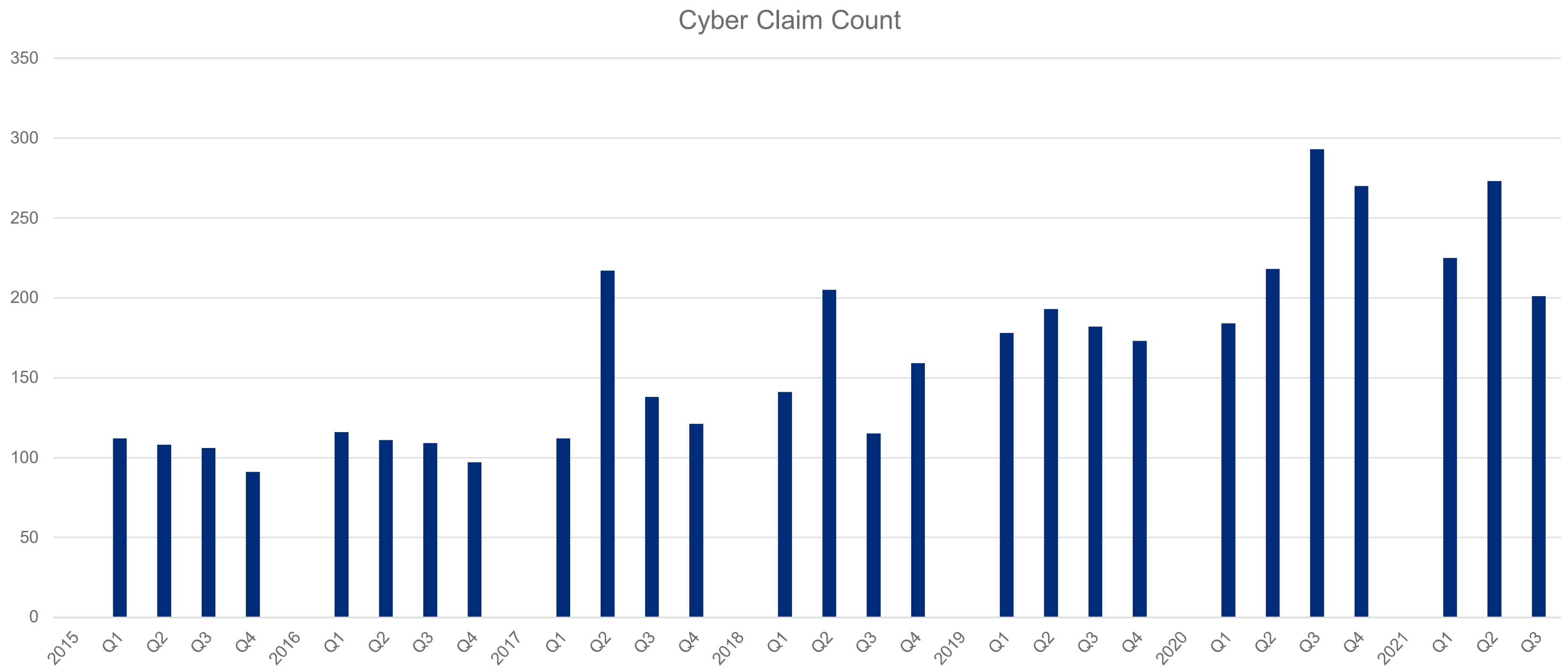
Claims Trends

Aggregated data from Marsh clients – through September 30, 2021

John Scordo

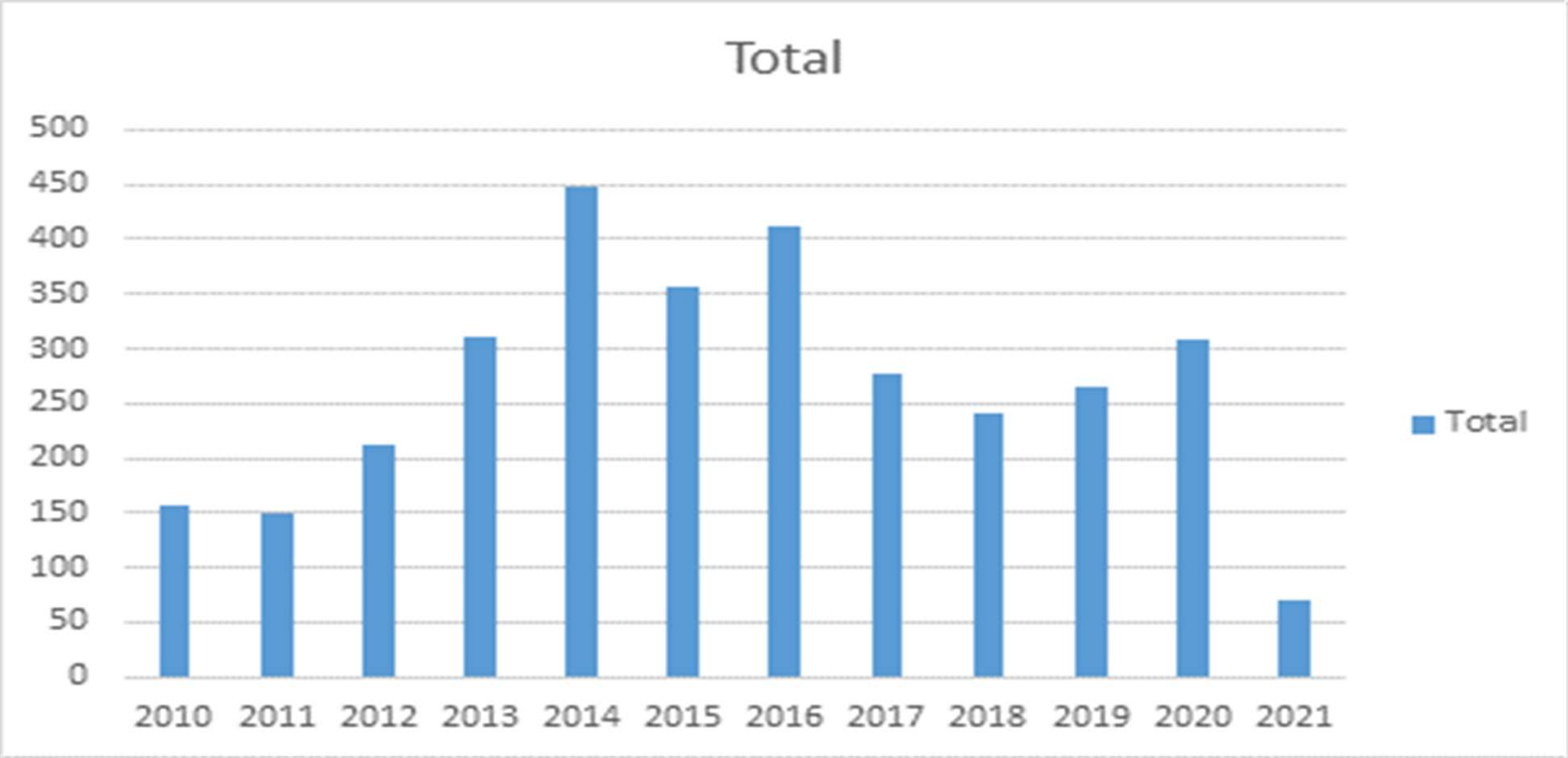
Total Cyber Claims – Marsh Clients (by quarter)

2015 – 2021

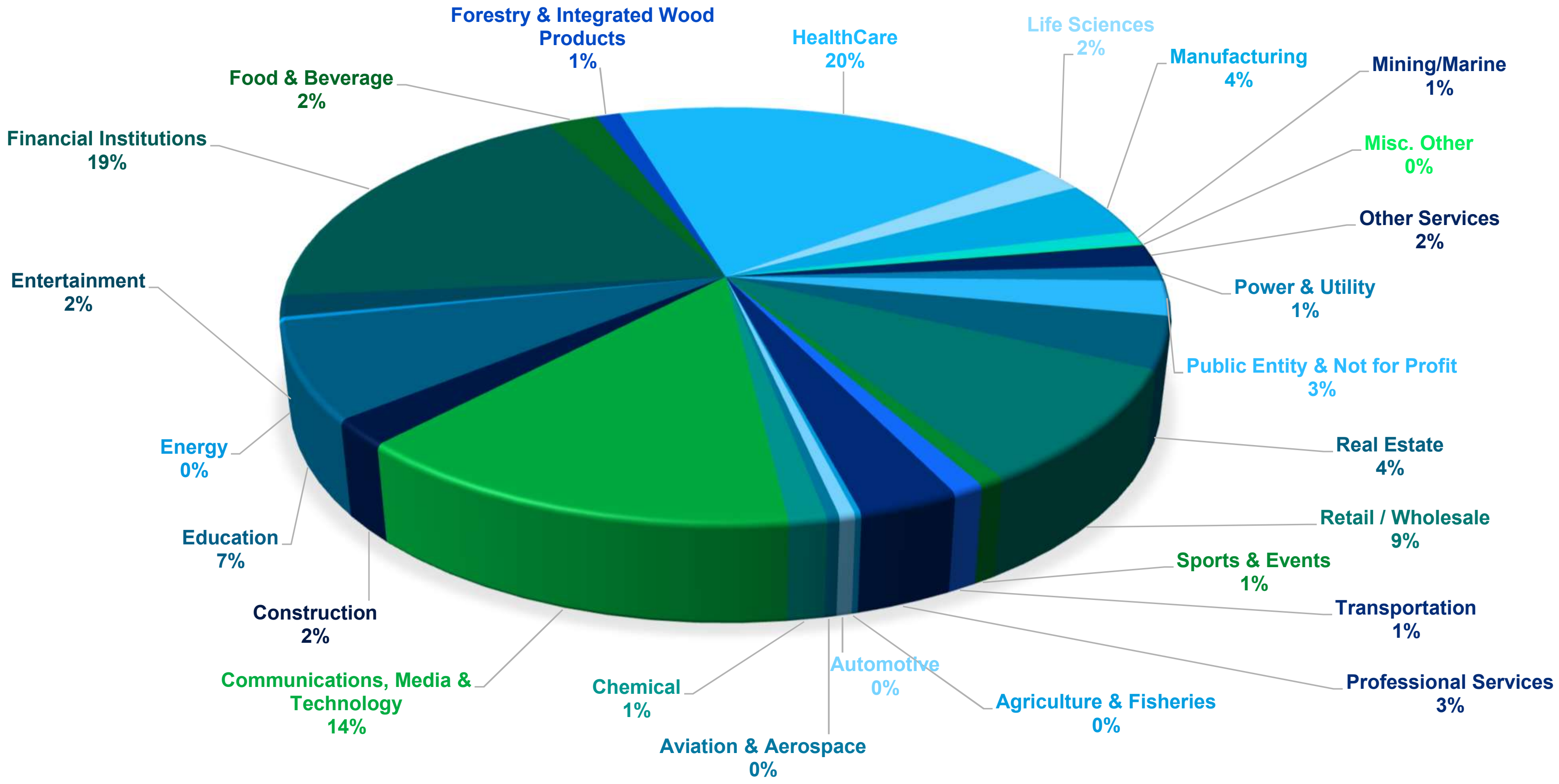


Cyber event counts for higher education

Marsh and non-Marsh clients

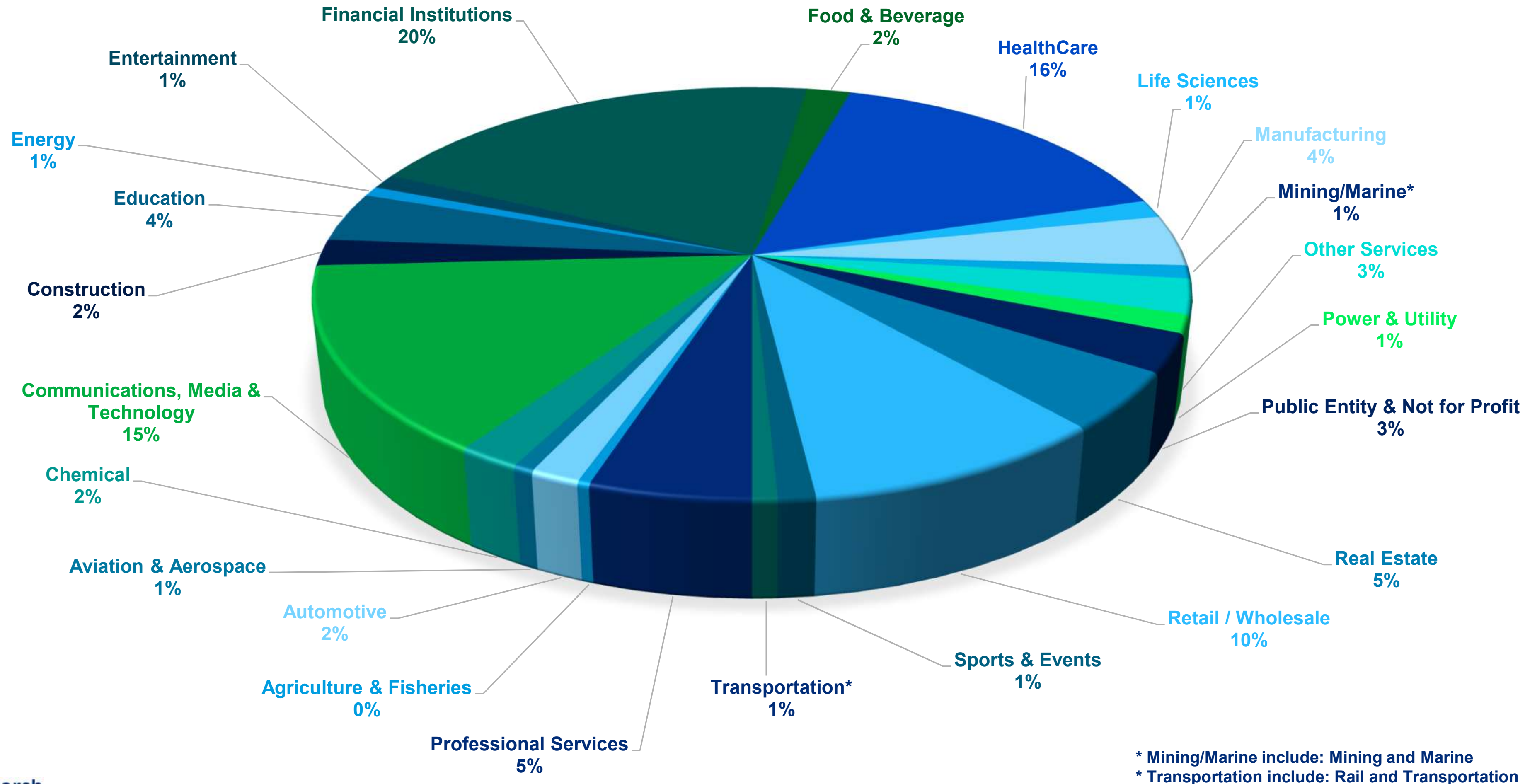


Industry 2020



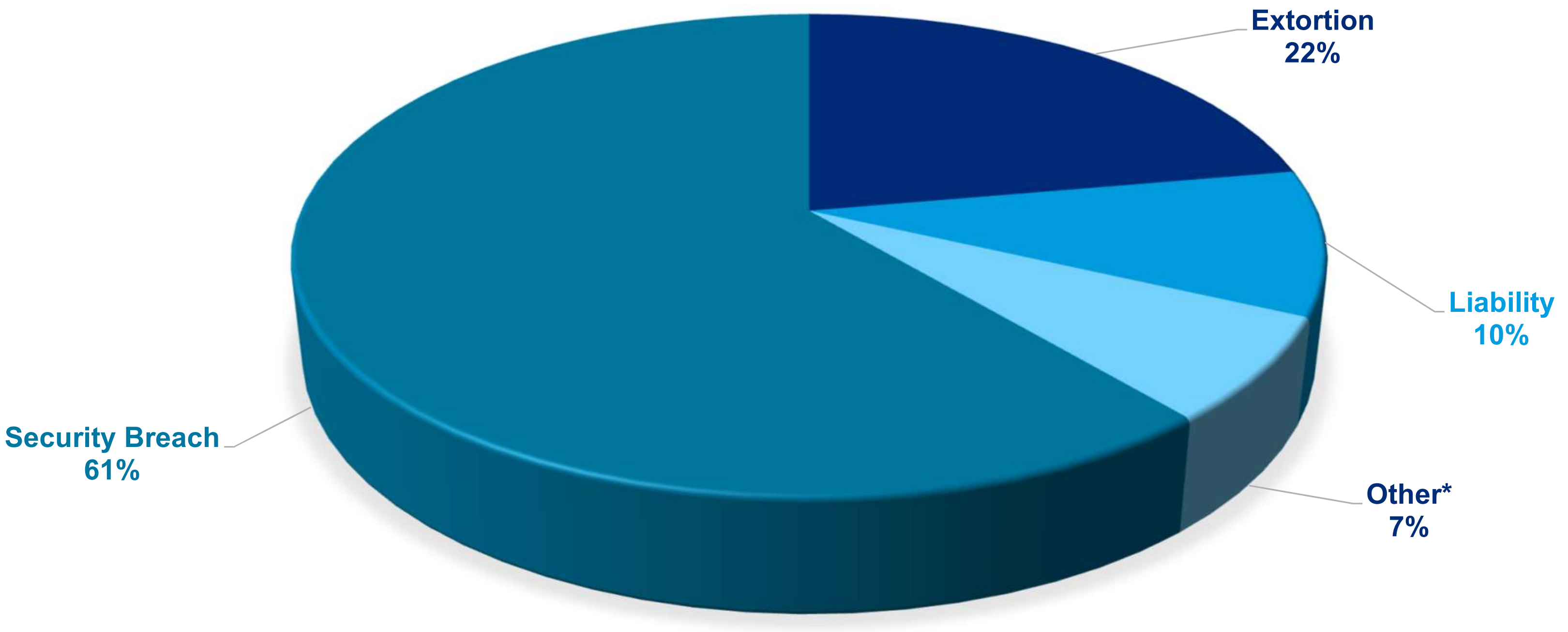
*

Industry 2021*



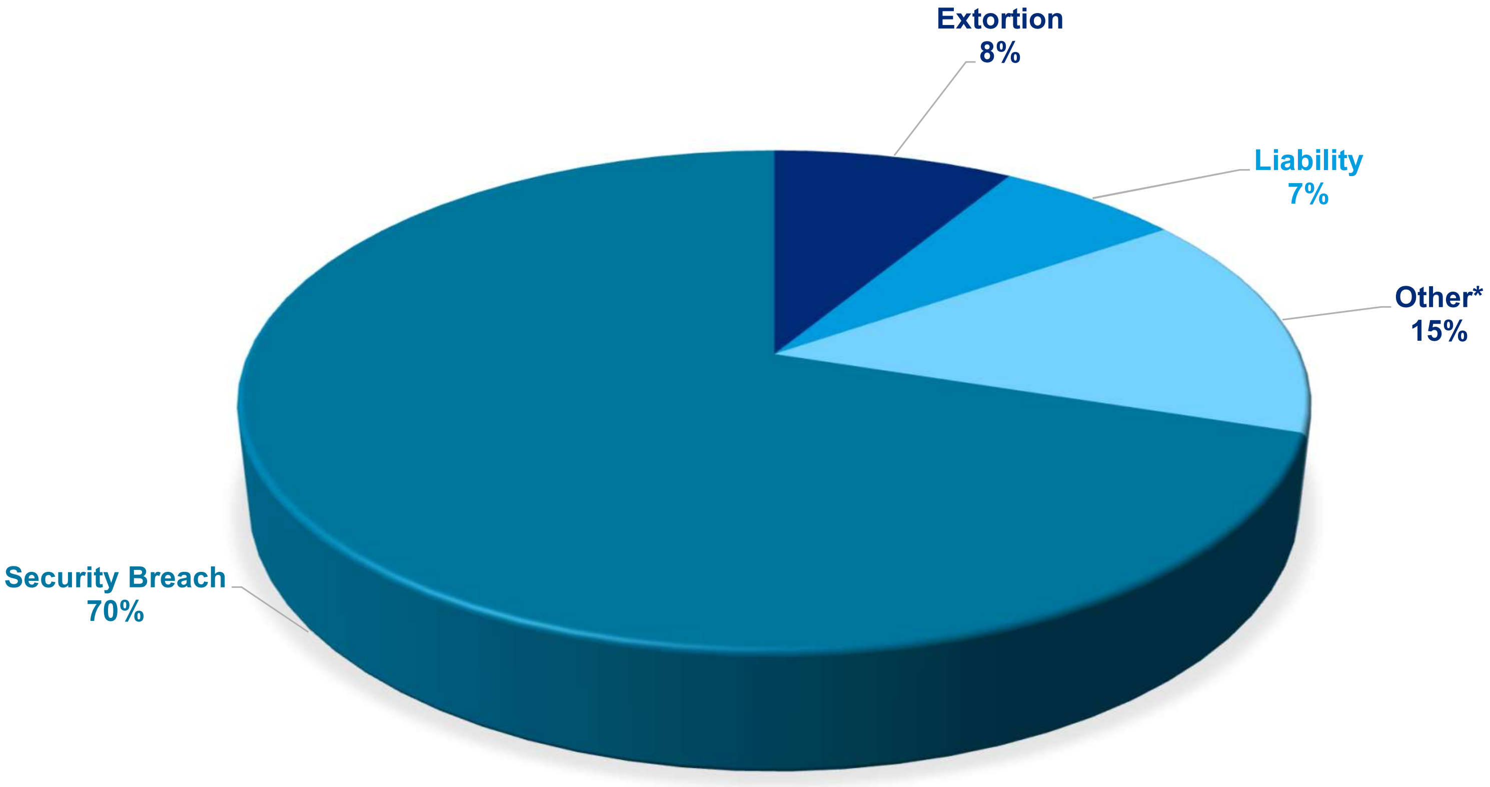
* Mining/Marine include: Mining and Marine
* Transportation include: Rail and Transportation
* Data till September'2021

Cyber Claim Type 2020



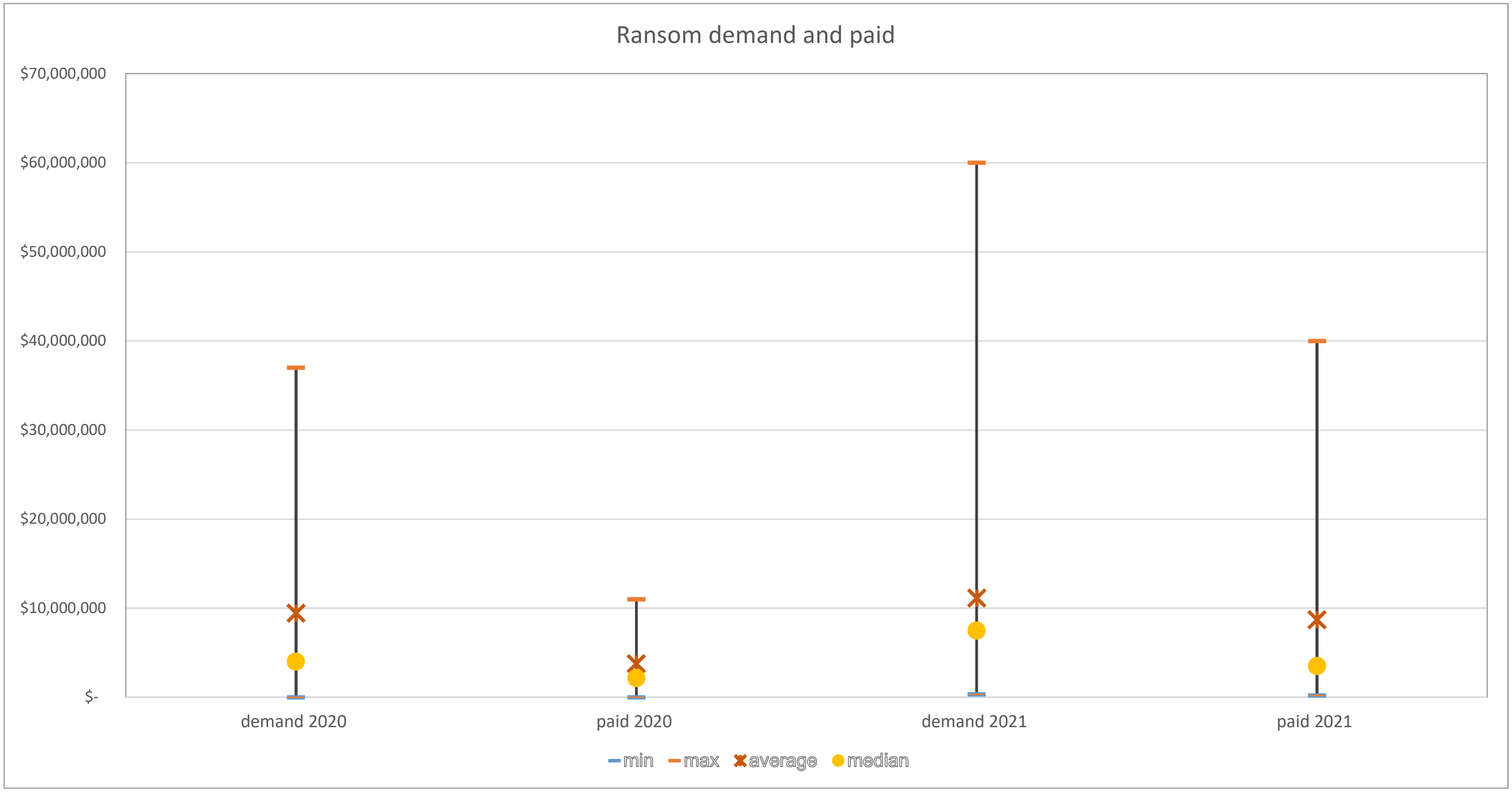
*Other includes: Fraudulent Instruction, Invoice Manipulation, System Failure and other losses

Cyber Claim Type 2021*

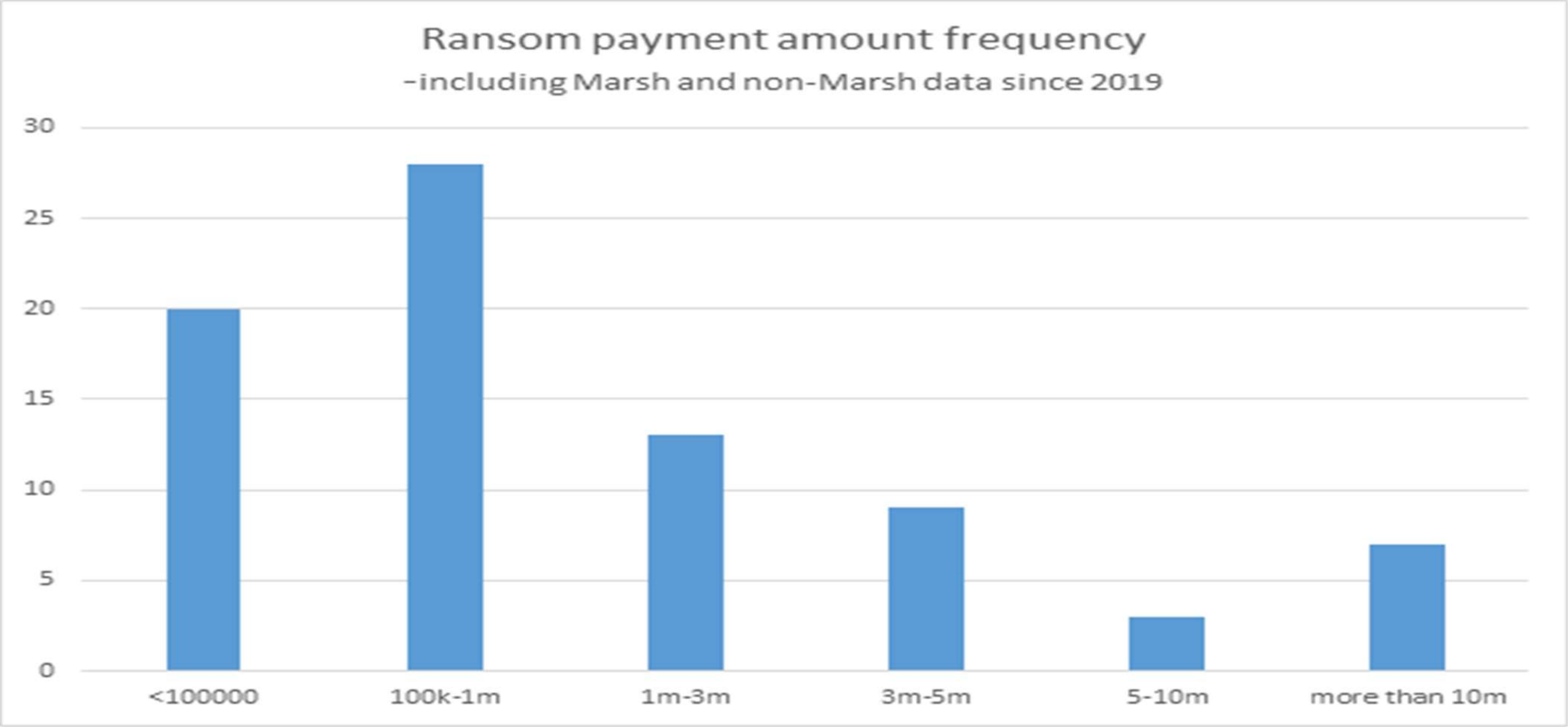


*Other includes: Fraudulent Instruction, Invoice Manipulation, System Failure and other losses
*Data till September'2021

Ransom Demands & Paid 2020 vs 2021



Ransom payment amount frequency (Marsh and non-Marsh clients)

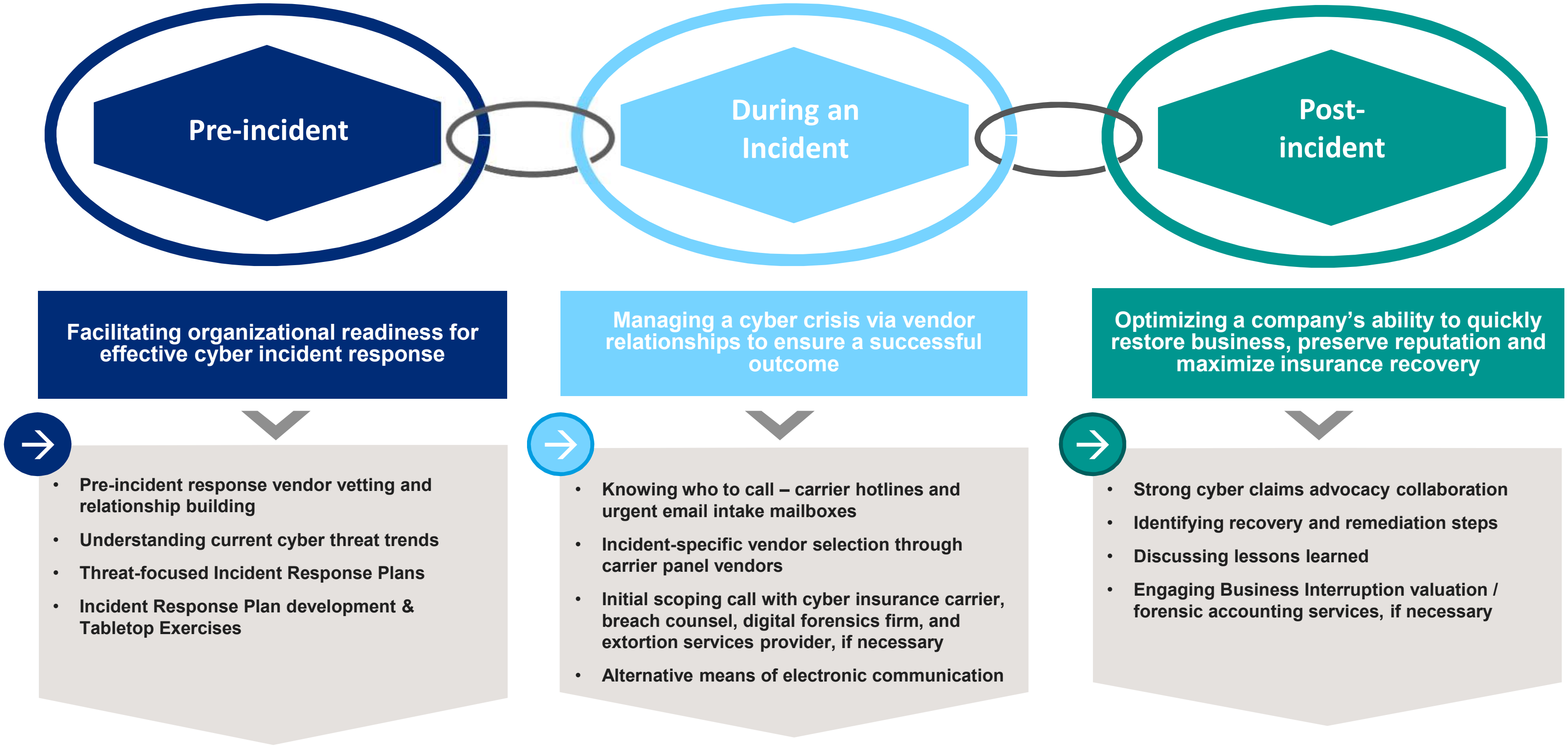


Cyber Incident Management

Florence Levy

Cyber Incident Management

Readiness, Response and Recovery



Pre-incident

Facilitating organizational readiness for effective cyber incident response

- Pre-incident response vendor vetting and relationship building
- Understanding current cyber threat trends
- Threat-focused Incident Response Plans
- Incident Response Plan development & Tabletop Exercises

During an Incident

Managing a cyber crisis via vendor relationships to ensure a successful outcome

- Knowing who to call – carrier hotlines and urgent email intake mailboxes
- Incident-specific vendor selection through carrier panel vendors
- Initial scoping call with cyber insurance carrier, breach counsel, digital forensics firm, and extortion services provider, if necessary
- Alternative means of electronic communication

Post-incident

Optimizing a company's ability to quickly restore business, preserve reputation and maximize insurance recovery

- Strong cyber claims advocacy collaboration
- Identifying recovery and remediation steps
- Discussing lessons learned
- Engaging Business Interruption valuation / forensic accounting services, if necessary

Cyber Resilience – what can you do?

Smart preparation can make all the difference

RANSOMWARE BEST PRACTICES

- Develop & test incident response plans with ransomware in mind – across key stakeholders
- Be diligent about cyber hygiene – controls are critical
- Understand the financial impact of ransomware risks & transfer residual risk

SUCCESSFUL CYBER INCIDENT RESPONSE AND MANAGEMENT

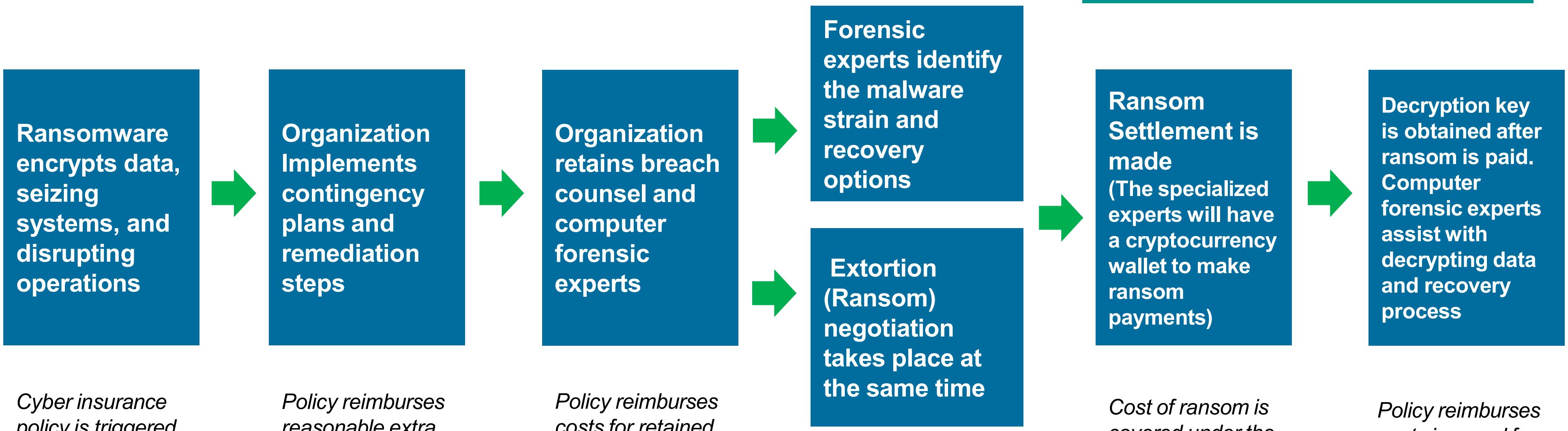
- Obtain basic facts of incident once cyber incident has occurred
- Rely on your (frequently reviewed and tested) Incident Response Plan
- Engage key incident response partners/vendors with insurance carrier approval (most insurance carriers have incident hotlines or emergency intake emails)

Ransomware

How insurance works alongside the crisis

Additional Tips:

- Do not engage with bad actors directly!
- Be mindful of electronic communications!
- Breach coach/counsel should engage additional vendors in order to preserve privilege!
- Maintain proper records!



Ransomware encrypts data, seizing systems, and disrupting operations

Organization Implements contingency plans and remediation steps

Organization retains breach counsel and computer forensic experts

Forensic experts identify the malware strain and recovery options

Extortion (Ransom) negotiation takes place at the same time

Ransom Settlement is made (The specialized experts will have a cryptocurrency wallet to make ransom payments)

Decryption key is obtained after ransom is paid. Computer forensic experts assist with decrypting data and recovery process

Cyber insurance policy is triggered as a result of "security failure"

Policy reimburses reasonable extra expenses incurred as well as business interruption loss as a result of ransomware

Policy reimburses costs for retained outside counsel and computer forensic experts, likely subject to prior Insurer approval (carrier vendor panels)

Cost of ransom is covered under the policy. Please note that there could be potential limitations due to OFAC compliance

Policy reimburses costs incurred for data restoration (costs to recreate and restore data)

Please refer to your policy for all key coverage parts, definitions, exclusions and terms & conditions.

Cyber Hygiene

Cybersecurity Controls and Improving your Cybersecurity Programs
Top 12 Cybersecurity Controls

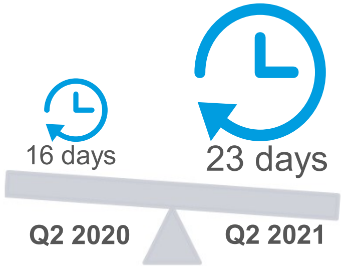
Jim Holtzclaw

Cyber Trends

Dominated by ransomware, regulations & supply chain cyber risk

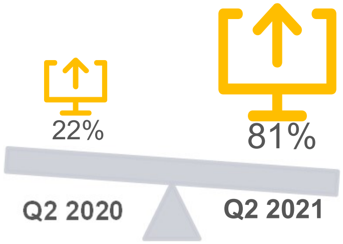
Ransomware attacks continue to increase in frequency, severity & sophistication – impacting orgs of all sizes & industries:

Average downtime:



44% YOY increase

Cases with data exfiltration:



~270% YOY increase

$ **2021 ransom headlines:**
~$800k average ransom payment

- Large insurer: $40M paid
- Oil pipeline: $4.4M paid
- Infrastructure: $50M demanded
- Food manufacturer: $11M paid
- Chemical distribution:$4.4M paid
- Tech hardware: $50M demanded

Privacy regulations are intensifying and there's still a patchwork approach:

- **GDPR** fines are growing (~$27M BA, ~$24M Marriott, ~$41M H&M)
- **CCPA** (California Consumer Privacy Act) and similar legislation (i.e. VA CDPA) allow for private rights of action and require additional compliance efforts
- **BIPA** (IL Biometric Information Privacy Act) litigation is expensive and is on the rise with increased use of biometric identifiers, especially for employee access – driving additional underwriting questions

Supply chain and systemic risk now garner more focus:

- **Aggregation** exposure a concern for underwriters
- **Systemic loss** – possible cyber risks:
  - Common vulnerabilities – in hardware or software
  - Common dependencies – vendors (such as cloud providers) and software
- **Cyber events** are driving increased scrutiny: SolarWinds, Accellion, Microsoft Exchange, & Kaseya

Sources: Coveware Ransomware Blog & Baker Hostetler 2021 DSIR Report

Top Cybersecurity Controls

The key to insurability, mitigation, and resilience

Preparation for the underwriting process:

1. Start early! Without positive responses in the top 5 control categories, coverage offered and insurability may be in question.
2. Evaluate your cybersecurity maturity by completing Marsh's Cyber Self-Assessment – where improvements are needed, leverage Cyber Catalyst vendors.
3. Expect more rigorous underwriting and more detailed questions from underwriters going forward.

Multifactor authentication for remote access and admin/privileged controls

Endpoint Detection and Response (EDR)

Secured, encrypted, and tested backups

Privileged Access Management (PAM)

Email filtering and web security

Patch management and vulnerability management

Cyber incident response planning and testing

Cybersecurity awareness training and phishing testing

Hardening techniques, including Remote Desktop Protocol (RDP) mitigation

Logging and monitoring/network protections

End-of-life systems replaced or protected

Vendor/digital supply chain risk management

Note: Each insurance carrier has their own specific control requirements that may differ by company revenue size and industry class. For more on the Cyber hygiene see: Cyber hygiene controls critical as cyber threats intensify (marsh.com)

Tighting up your IT Enterprise

12 Key Controls to implement/enhance (Slide 1 of 2)

Multifactor Authentication (MFA) for remote access and admin/privileged access

Organizations should bolster their security through MFA, which requires at least two pieces of evidence (factors) to prove the user's identity, and prevents attackers from effectively using stolen passwords. For example – a time sensitive pin code delivered through an app or via text message is often a second factor in addition to the user's password. Although no cybersecurity tools are perfect, MFA provides a substantial barrier to unwanted system access.

Endpoint Detection and Response (EDR)

It's important for companies to have up-to-date information about the security posture of any devices used by employees to receive or send corporate information, whether it's a laptop, desktop, or mobile device. EDR offers continuous monitoring and more advanced detection and automated response capabilities. The monitoring software will watch for any suspicious or irregular activities and can also facilitate rapid incident response across an organization's environment.

Secured, encrypted, and tested backups

Attackers are looking to delete backups prior to launching a ransomware attack so they can successfully cripple and extort their victims. It is essential to secure backups through encryption and isolation from the network (offline or MFA-controlled access with dedicated identities), and to establish a data restoration testing schedule to ensure that backups are working as intended.

Privileged Access Management (PAM)

Privileged accounts are the keys to a network. When attackers compromise these accounts, they gain unlimited access to the network, increasing the likelihood of causing significant harm. Organizations can control for this by limiting the number of privileged accounts, using Just-in-time (JIT) elevation or vaults, and MFA. Many organizations implement PAM solutions that automate privilege and session management.

Email filtering and web security

Malicious links and files are still the primary way to insert ransomware, steal passwords, and potentially access critical systems. Today's first line of defense includes advanced technologies to filter incoming emails, block access to malicious sites or downloads (across both onsite and remote users), and test suspicious content in a secure "sandbox" environment.

Patch management and vulnerability management

Unpatched vulnerabilities remain a leading cause of intrusions into systems, with hundreds of vulnerabilities revealed every month for multiple applications and systems. When technology environments are not patched in a timely fashion, attackers will seek to exploit vulnerabilities.

Regular vulnerability scans and rapid patch management reduces the risk of cyber attacks on the network. Such actions allow organization to apply patches or uncover existing vulnerabilities and remediate before threat actors have a chance to exploit. Most underwriters expect to see an ability to apply critical patches within 72 hours across 95% of endpoints.

Tightening up your IT Enterprise

12 Key Controls to implement/enhance (Slide 2 of 2)

Cyber incident response planning and testing

An up-to-date Cyber Incident Response (CIR) plan with a trained team and experienced senior leadership provides efficiency and effectiveness in response to cyber incidents. Practice through tabletop exercises builds resiliency. When combined with backups, other business continuity plans, and monitoring of endpoints and the network, they significantly help mitigate impacts to business operations and help to protect an organization's reputation if an event does occur.

Cybersecurity awareness training and phishing testing

Attackers have taken advantage of COVID-19, a time when people were stressed to capacity, as a guise to spread ransomware. There will always be environmental factors that attackers can exploit to deceive people. Employee cybersecurity training and phishing campaigns help ensure people remain aware of changes in the cyber environment and remain cautious.

Hardening techniques including Remote Desktop Protocol (RDP) mitigation

Attackers exploit default device settings or misconfigurations. Controlling changes and aligning with an industry recognized security baseline to harden devices are critical to prevent attackers from reaching and exploiting their targets. Particularly, the use of RDP without VPN and MFA controls should be avoided.

Logging and monitoring/network protections

Logging and monitoring network activities allows organization to identify, detect, and contain attacker's actions at an early stage. Automated tools can support human monitors as they track network events or anomalous user behavior. Efficient use of firewalls and other technologies requires well defined strategies - network segmentation, intrusion detection and prevention systems, data leak prevention systems, etc.

End-of-Life systems should be replaced or protected

End-of-life systems or technology become a risk because patches and other forms of security support are no longer offered. Once the software/technology is practically not supported it will be impacted by unfixable vulnerabilities. It needs to be either protected by compensating controls or upgraded to "supported" platforms.

Vendor/digital supply chain risk management

A significant proportion of attacks or incidents are initiated through the supply chain, whether it's a third party access that is leveraged, a trusted software update that is compromised, a malicious code that comes through a library, or a critical service that becomes unavailable. Managing cyber supply chain by monitoring risks and dependencies, and maintaining continuity plans goes a long way in reducing the overall cyber risk exposure

Buyer’s Perspective

Deb Donning

Buyer’s Perspective

1. Optimism going in (wanted to explore increased coverage)
2. Application process – more information, more applications, more expectations
3. Options minimal
4. Coverage reduced, deductible increased, exclusions increased, premium more than doubled
5. Policy release delayed
6. Concern for future ability to secure coverage at an affordable premium/self-insure?

Panel Bios

Cyber Panel Overview

Annice Y. Ma, ARM, Vice President
Cyber Center of Excellence

Annice is a client advisor within Marsh's Cyber Practice based in Los Angeles, CA. She is responsible for advising complex clients across various industries, including higher education and healthcare institutions, on the optimization of risk transfer solutions, helping clients address cyber and E&O issues at the enterprise level and strategically navigate the fast-evolving cyber and technology landscape. She specializes in the implementation of effective insurance programs through technology, risk identification, loss quantification, coverage reviews, and market analysis.

Annice also serves as a Cyber Healthcare Industry Leader, collaborating with Marsh's industry and practice leaders to generate thought leadership and guidance for brokers across the nation. She is well versed in identifying and addressing the specific needs of healthcare clients across various segments, including but not limited to, health systems and managed care providers. BS in Business Administration, University of Southern California.

Phone:	929 310 0443

Email:	annice.y.ma@marsh.com

Cyber Panel Overview

Florence Levy, Esq.
Managing Director
Cyber Incident Management Director

Florence is the Cyber Incident Management (CIM) Director within Marsh's U.S. & Canada Cyber Practice. She assists clients with cyber incident preparedness and response resources throughout the lifecycle of a cyber event, including a collaborative partnership with Cyber Claims advocacy to optimize claim recovery. Prior to her role in CIM, she was Marsh's West Zone Cyber Practice Leader, advising clients on complex cyber and commercial E&O risk and insurance while working closely with key carrier decision makers to devise optimal and customized risk transfer programs. Florence is a frequent speaker and contributor at industry events and author of content for a variety of trade publications. Member, Colorado State Bar; BA, University of Michigan, Ann Arbor. JD, University of Denver – Sturm College of Law.

Prior to joining Marsh in 2018, Florence was a Senior Vice President of JLT's Cyber and E&O Practice group, Head of the U.S. Global Technology & Privacy Practice at Lockton Companies, as well as the National Practice leader for Aon's Professional Risk Solutions team. Throughout her 20-year insurance brokerage career, she has focused solely on commercial E&O and its subsequent evolution into cyber insurance.

Phone: 303 810 7159

Email: florence.levy@marsh.com

Cyber Panel Overview

John Scordo, Esq.
Senior Vice President, Cyber Claims Advocacy Leader

As leader of Marsh's US and Canada Cyber Claims Advocacy Practice, John is responsible for assisting clients with all phases of a security or privacy event, including the initial investigation/response and hiring of forensics, breach and litigation counsel, public relations advisors and remediation/notice vendors, preparing breach notifications, responding to ransom demands, remediation and replacement of equipment, responding to various third party claims or requests for assistance, minimizing potential liability, business interruption assessment, and all phases of post-breach litigation, arbitration or mediation. John also assists with the negotiation of cyber insurance/E&O terms and conditions, and helps clients with contractual issues involving insurance and/or indemnification, and pre-event planning and compliance.

John has extensive experience in the litigation and negotiation of claims and coverages under all types of insurance, including cyber liability, first-party network security, general and professional liability, D&O, property/business interruption, crime/fidelity/ransom, E&O, employment, fiduciary and others. Before joining Marsh, he was a litigation partner at K&L Gates LLP counseling large corporate clients on all aspects of insurance recovery as well as data security issues, including privacy and protection, best practices, breach preparation and response, and post-breach regulatory liability and litigation. Prior to K&L Gates, John was a litigation partner at Day Pitney LLP focusing on insurance recovery and commercial disputes. John is a frequent presenter and author on cyber and data privacy issues, including regulation, litigation, electronic discovery, insurance coverages, and claims resolution. He also was an Adjunct Professor of Law at New York Law School where he taught *Post-Data Breach Law and Counseling.* Admitted to the bars of the States of New York, New Jersey and Florida. J.D., New York Law School, Research Editor, *New York Law School Law Review.* B.S., Rutgers University, Cook College.

Phone: 917 208 2890

Email: john.scordo@marsh.com

Cyber Panel Overview

Jim A. Holtzclaw, Senior Vice President
Cybersecurity Consulting and Advisory Services

Jim Holtzclaw is a Senior Vice President of Cybersecurity Consulting and Advisory Services at Marsh Advisory. He is a senior cybersecurity consultant with over 25 years of experience and works with a team of experts to identify, develop, implement, conduct, and execute Marsh's cyber security consulting strategy, capabilities, and services in North America.

Since joining Marsh in 2015, he has worked with the cyber practice team to develop new capabilities including cyber risk assessment, cyber risk quantification, cyber incident breach response plans, third party vendor risk management, cyber tabletop exercises, and other cyber services.

Jim's extensive career experience includes serving as the managing partner and general manager at Waverley Labs, a small specialized company focused on digital risk management and cybersecurity. Prior to Waverley Labs, Jim was the general manager of federal programs for CyberPoint International, supporting the US government through the delivery of cyber strategy and operational services. Jim was previously a vice president of enterprise security and infrastructure solutions at CRGT and held senior management positions with Booz Allen Hamilton focusing on cyber programs. Jim spent 8 years at Northrop Grumman Information Technology supporting multiple cyber clients at the National Security Agency (NSA), National Reconnaissance Office (NRO), US Cyber Command, US Army, US Air Force, US Marine Corps and commercial industry. Jim's military career spanned 21 years, during which he served as a Signal Officer. He completed his career as the Director, Army Computer Emergency Response Team with a worldwide mission of ensuring the security and integrity of the Army's IT enterprise. Jim also served as an associate professor of mathematics at the United States Military Academy, West Point, NY. M.S., Operations Research and Systems Engineering, Georgia Institute of Technology, B.S., Mathematics and Computer Science, Columbus State University.

Phone: 202 297 9351

Email: james.holtzclaw@marsh.com

Cyber Panel Overview

Deb Donning, Esq.
Director of Risk Management and Insurance
Safety and Risk Services | University of Oregon

Deb is Director of Risk Management and Insurance at UO. She has served UO for over twenty-six years, returning this past March after being away less than five years. She has over thirty years of higher education experience; working in risk management, environmental health and safety, incident response, and compliance the last twelve years. She is a member of the University Risk Management and Insurance Association (URMIA) and the Oregon State Bar. Deb received her Bachelor of Science degree in political science from Willamette University and her J.D. from the University of Oregon School of Law. She also holds the Associate in Risk Management professional designation.

Phone:	541-346-2538
Email:	ddonning@uoregon.edu

Cyber Panel Overview

Catherine Brown, Senior Vice President, Client Executive
Public Entity and Education Practice

Catherine has a career-long focus on the public entity and higher education sector, with over 35 years of industry experience. She has been with Marsh for 16 years and serves as senior advisor and client executive for the University of Oregon and several other large public entities, publically traded, privately held and multinational corporations. Catherine is responsible for identifying and responding to the emerging issues facing clients and developing and customizing specialized services to meet their needs. Catherine also has specialized expertise in the construction, real estate, retail wholesale, automotive and manufacturing industry sectors with emphasis on insurance brokerage, public entity, education and multinational risk management, alternative risk financing, self-insurance and captive insurance program management and administration, and casualty claims management, including police professional and employment discrimination case investigation, management and adjudication; owner-controlled insurance programs, risk control, analysis, financing, cost allocation, and global risk management.

Catherine began her professional career in the insurance industry at United Pacific Reliance Insurance. Her extensive career experience includes design, leadership and management of the risk management and insurance programs of several large Oregon public entities: City of Eugene, Lane County, Port of Portland and Oregon Health & Science University. She also served as claim for the City of Eugene. Catherine's vast private sector experience includes serving as the associate director and global risk manager in the U.S. and Europe rolling out Nike's risk management programs, worldwide, and as the vice president/executive director of human resources & diversity for Asbury Automotive Oregon, one of the largest retail automotive consolidators in the nation.

Phone: 503 248 6423

Email: catherine.e.brown@marsh.com