

# 10<sup>th</sup> Annual Financial Executive Forum Weekly Webinar Series

October 3<sup>rd</sup> – November 7<sup>th</sup> (Thursdays)

**WELLS  
FARGO**

**Sage**



**Marsh McLennan  
Agency**



**Cherry  
Bekaert**



**CORDIA**  
RESOURCES®  
by  **Cherry Bekaert**

# Our 10<sup>th</sup> Annual Financial Executive Forum Webinar Series program offering: 6 weekly sessions, with up to 12 hours of CPE credit, including 2 hours of VA Ethics.

- ▶ **Oct. 3 | 8-10 A.M.**      **CFO Roundtable**  
Presented by **Cordia Resources by Cherry Bekaert** (2 CPE Hours)
- ▶ **Oct. 10 | 8-10 A.M.**      **Anchoring Your Foothold in GovCon and DCAA's Hot Topics**  
Presented by **Cherry Bekaert** (2 CPE Hours)
- ▶ **Oct. 17 | 8-10 A.M.**      **VA Ethics**  
Presented by **Jennifer Louis, AICPA** (2 CPE Hours)
- ▶ **Oct. 24 | 8-10 A.M.**      **Managing Your Risk: Innovation in Employee Benefits & Business Insurance**  
Presented by **Marsh McLennan Agency** (2 CPE Hours)
- ▶ **Oct. 31 | 8-10 A.M.**      **Economic Outlook and Capital Markets Update**  
Presented by **Wells Fargo** (2 CPE Hours)
- ▶ **Nov. 7 | 8-10 A.M.**      **How AI and Digital Networks Will Shape the Future of Accounting**  
Presented by **Sage** (2 CPE Hours)



# CPE Webinar Rules

## CPE Compliance:

- ▶ Polling questions will appear throughout the webinar to be compliant with **NASBA** requirements
- ▶ You need to answer at least 75% of the 8 polling questions to **receive full CPE credit** for each session
- ▶ You will be **muted** during the webinar presentation
- ▶ Please use the **Q&A** feature to submit your questions to the panelist
- ▶ Please use the **chat** feature to communicate any technical difficulties
- ▶ Please complete the **session survey** using the link included in the post event email
- ▶ **Your CPE certificates** will be issued within 2 weeks of this course. Any questions, please reach out to Cherry Bekaert Learning at [cbhlearning@cbh.com](mailto:cbhlearning@cbh.com)



# Sponsors



**Ben Kane**

*Sr. Market Director*



**Gary Maher**

*Senior Channel Executive*



**Traci Shepps**

*Partner,  
Government Contracting Industry Practice Leader*



**Doug Smith**

*Managing Director*



**Alli Gregory**

*Employee Health & Benefits Consultant*

## Hosts

---



**Joe Greeves**

*Managing Director*



**Grant Palmer**

*Partner*



# Today's Agenda

## October 24<sup>th</sup> – Managing Your Risk: Innovation in Employee Benefits & Business Insurance presented by Marsh McLennan

- ▶ 8:00 to 8:10 A.M. | Kick-off & Welcome
- ▶ 8:10 to 9:00 A.M. | People Risk
- ▶ 9:00 to 9:05 A.M. | Break
- ▶ 9:05 to 9:55 A.M. | Business Risk
- ▶ 9:55 to 10:00 A.M. | Q&A and Close

# Meet Our Speakers



## Alli Gregory

*Consultant, Employee Health & Benefits  
Marsh McLennan Agency*



## Gerald Escobar

*Employee Benefits Consultant  
Marsh McLennan Agency*



## Michael Cooper

*Consultant  
Marsh McLennan Agency*



# Meet Panel #1: Employee Health & Benefits

## FACILITATOR

## PANELISTS



**Gerald Escobar**

*Employee Benefits  
Consultant, Marsh  
McLennan Agency*



**Zak Kornblum**

*Pharmacy Clinical  
Director, Marsh  
McLennan Agency*



**Peter Schultz**

*Director of Actuarial and  
Underwriting Services,  
Marsh McLennan  
Agency*



**Kate Valette**

*Vice President, Clinical  
Director Workers'  
Health 360, Marsh  
McLennan Agency*



# Meet Panel #2: Business Insurance

## FACILITATOR

## PANELISTS



**Michael Cooper**

*Consultant, Marsh  
McLennan Agency*



**Mario Paez**

*National Cyber Risk  
Leader, Marsh  
McLennan Agency*



**Max Richardson**

*Executive Vice  
President, Business  
Insurance, Marsh  
McLennan Agency*



**Mike Rickard**

*Senior Vice President,  
Business Insurance,  
Marsh McLennan  
Agency*



**Alyson Rossi**

*Senior Vice President,  
Regional Risk Manager,  
Marsh McLennan  
Agency*





# Thanks for Attending!

If you'd like to connect with one of our subject matter experts, please reach out to Michael or Alli who will facilitate

Michael Cooper

[Michael.Cooper@marshmma.com](mailto:Michael.Cooper@marshmma.com)

336-392-7340

[Michael's LinkedIn](#)



Alli Gregory

[Alli.Gregory@marshmma.com](mailto:Alli.Gregory@marshmma.com)

484-269-0914

[Alli's LinkedIn](#)



Marsh McLennan Agency Presentation for the Financial Executive Forum  
October 24, 2024

# Managing Your Risk: Innovation in Employee Benefits & Business Insurance



**Gerald Escobar**  
Vice President  
EH&B Practice



**Peter Schultz, FSA, FCA, MAAA**  
Vice President  
Actuarial & Underwriting



**Zak Kornblum, PharmD**  
Pharmacy Clinical  
Director  
EH&B Practice

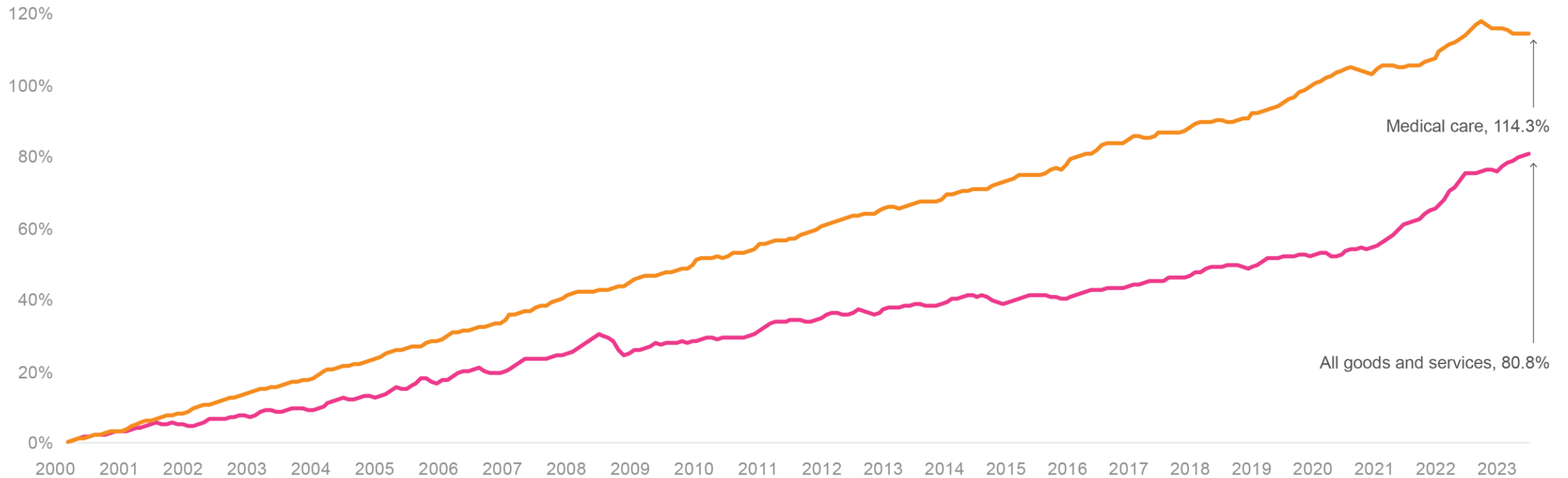


**Kate Valette, BSN, RN**  
Clinical Consultant  
EH&B Practice

## Session 1

- Addressing the accelerated expense trend of health benefits
- Bending the cost curve around Pharmacy spend and your fiduciary responsibility
- Data-driven decisions to be a best-in-class and competitive employer

# Cumulative percent change in Consumer Price Index for all urban consumers (CPI-U) for medical care and for all goods and services, January 2000 – June 2023



Note: Medical care includes medical services as well as commodities such as equipment and drugs.

Source: Peterson-KFF Health System Tracker, "How does medical inflation compare to inflation in the rest of the economy?" 2023, [Link](#)

# To address rising costs without burdening employees, employers are thinking about value

Employers are taking action to offer competitive, attractive, and inclusive benefits to support employee well-being. But that's not all. Employers must also prepare for faster health cost growth for years to come. Pursuing cost management strategies that can slow cost growth over the longer term and minimize cost increases for employees will be key for planning.

## Strategies employers are using to slow health cost growth – without shifting cost to employees

Programs aimed at enhancing the management of specific health conditions



Focused actions to manage the cost of specialty prescription drugs



Greater focus on virtual care offerings, beyond standard telemedicine



Steering members to quality care with a navigation or advocacy service (beyond health plan's standard service)



Steering members to quality, high-value care via high-performance networks, centers of excellence, etc.



Enhanced clinical management model (above the health plan's standard model)



Limiting plan coverage to in-network care only (in at least one plan)



Strategies focused on utilization of high-quality primary care (e.g., advanced primary care)

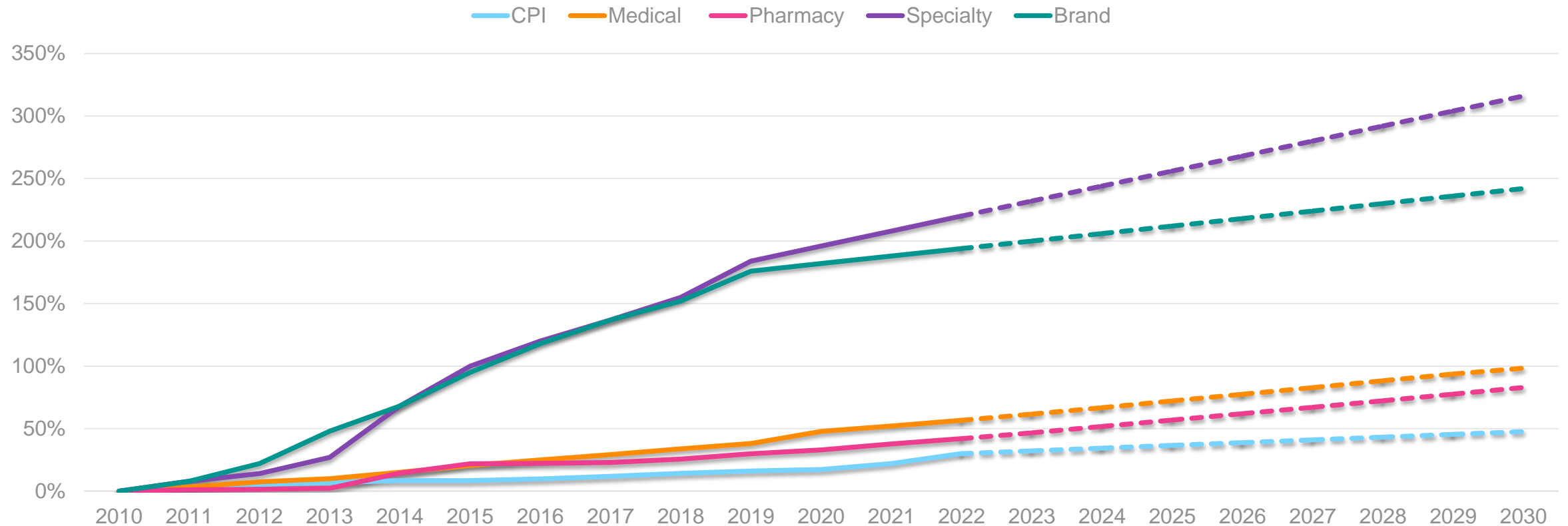


■ Currently use strategy ■ Seriously considering implementing within 2 years



# It's Only Going to Get Worse...Quickly

Per capita % cost change relative to year 2010, by category by year



Sources: Bureau of Labor Statistics – CPI by year (2000 – 2022), Centers for Medicare & Medicaid Services – Historical National Health Expenditure data (2010 – 2022), Projected National Health Expenditure data (2023 – 2030), Express Scripts Prescription Price Index (2008–2019), Congressional Budget Office – Economic Outlook for 2020 to 2030.

**Core Health Data**



**Pharmacy**



**Medical**



**Point Solution**



**Eligibility**



**Disability**



**Leave**



**Workers' Compensation**

**Workers' Data**

**Data Lake**

**Your future is limitless.<sup>SM</sup>**

This document is not intended to be taken as advice regarding any individual situation and should not be relied upon as such. Marsh & McLennan Agency LLC shall have no obligation to update this publication and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting or legal matters are based solely on our experience as consultants and are not to be relied upon as actuarial, accounting, tax or legal advice, for which you should consult your own professional advisors. Any modeling analytics or projections are subject to inherent uncertainty and the analysis could be materially affected if any underlying assumptions, conditions, information or factors are inaccurate or incomplete or should change. d/b/a in California as Marsh & McLennan Insurance Agency LLC; CA Insurance Lic: 0H18131. MarshMMA.com

# Managing Your Risk: Innovation in Business Insurance

Prepared for the Financial Executive Forum

October 24<sup>th</sup>, 2024

A business of Marsh McLennan



# Introductions

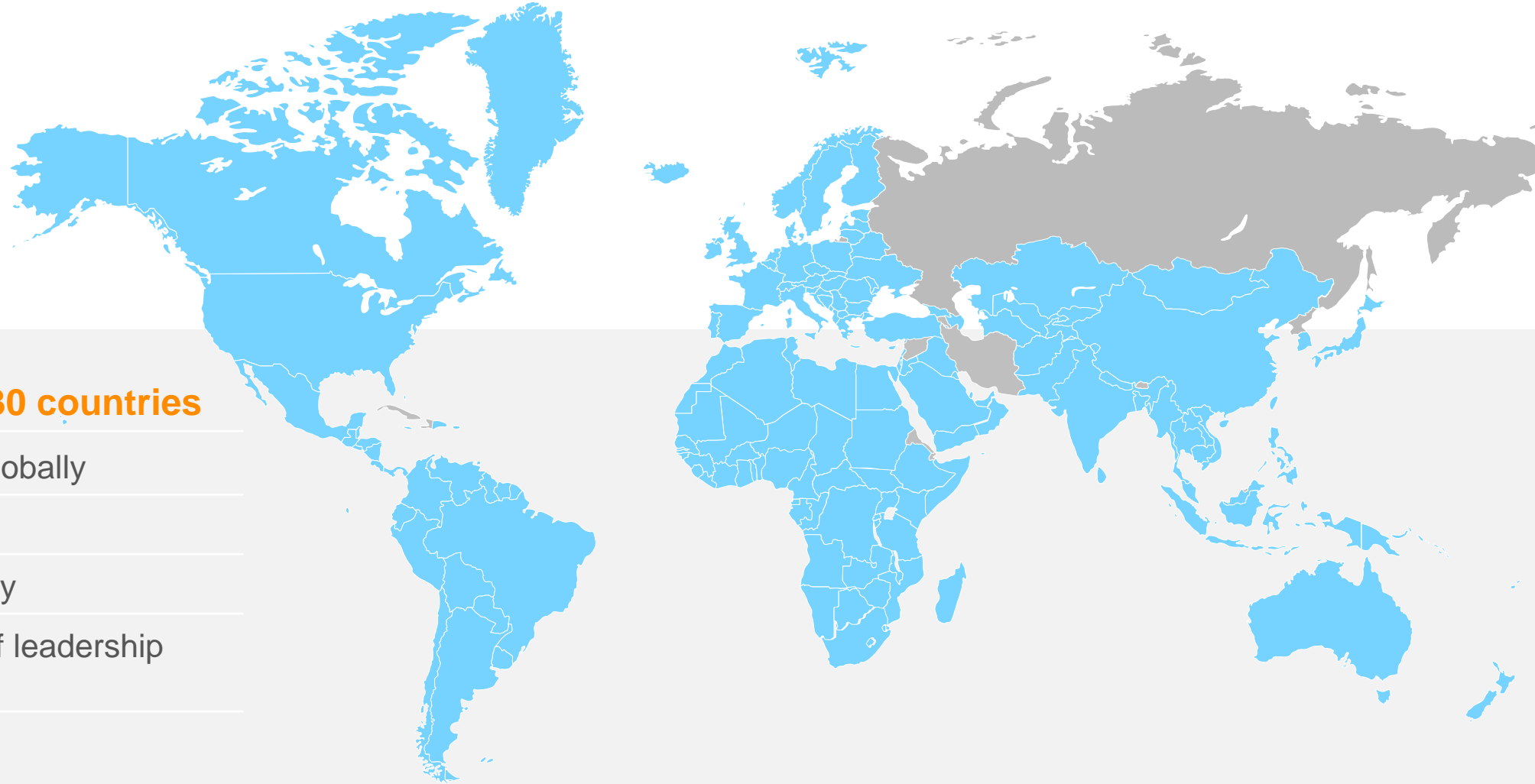
Business Insurance Presenters

Team



<b>Mike Ricard, SVP Business Insurance</b>	<b>Max Richardson, President Business Insurance, Mid- Atlantic</b>	<b>Alyson Rossi, SVP Executive &amp; Professional Liability Practice</b>	<b>Mario Paez, National Cyber Risk Leader</b>	<b>Michael Cooper, Consultant</b>
------------------------------------------------	--------------------------------------------------------------------------------	--------------------------------------------------------------------------------------	---------------------------------------------------	---------------------------------------

# Marsh McLennan's **global** scale and scope



Clients in more than **130 countries**

**85,000+** colleagues globally

**\$23B** annual revenue

**Fortune 250** company


**150+ year history** of leadership and innovation


# MarshMcLennan


The world leader in risk, strategy, and people.


## Risk & Insurance Services


## Consulting

 **GuyCarpenter** Reinsurance and intermediary advisory services.

 **OliverWyman** Management, economic, and brand strategy consulting.

 **Marsh** Insurance broking and risk management.

 **Mercer** Talent, health, retirement and investment consulting.

 **MarshMcLennan Agency** Business insurance, employee health & benefits, retirement & wealth, and private client services.

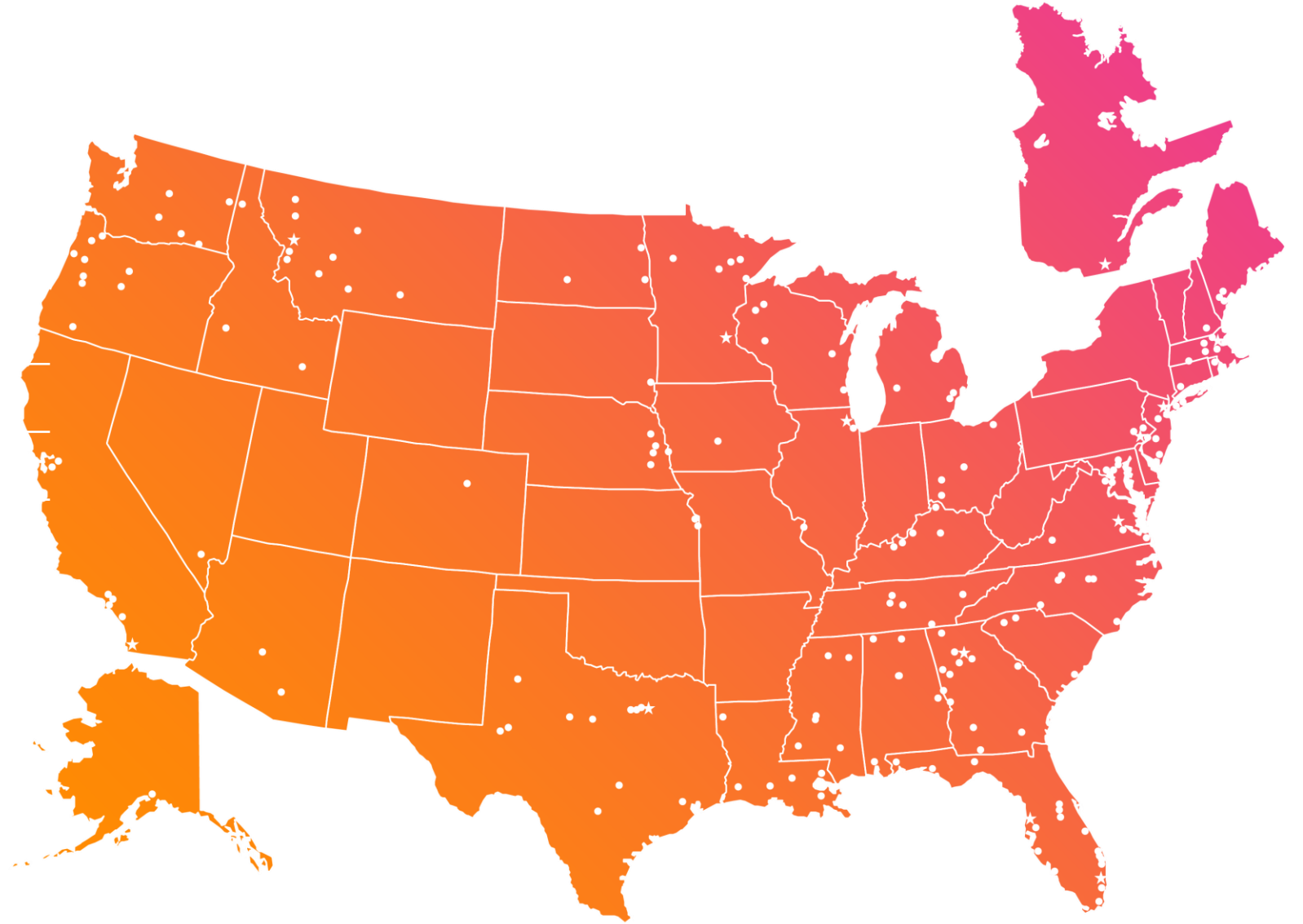
# MMA today

**11,000+** colleagues

**200+** local offices

Local specialists, global resources, endless opportunities.

**We're MMA.**





# Business Insurance

Protecting every facet of business with scalable resources



Industry and risk-specific proprietary products and solutions



Specialized resources and expertise backed by the support of Marsh's global network



Risk management and resiliency support across a wide array of issues and concerns



# You need more than a one-size-fits-all business policy.



Global resources



Industry-specific proprietary products



Analytics and benchmarking



Cyber coverage and resiliency solutions



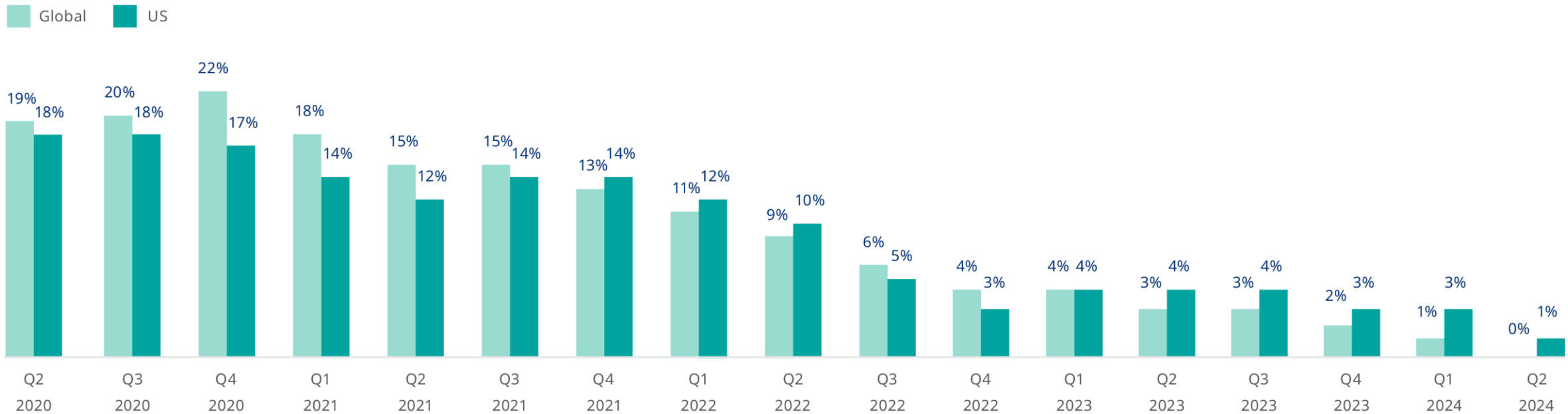
Risk services and claims



# Q2 2024 market observations

The global composite rate tracked in the [Marsh Global Insurance Market Index](#) was flat for the first time in 27 quarters, the first time in nearly seven years. However, U.S. commercial insurance prices rose 1% in the second quarter of 2024, trending down from 3% in the two prior quarters.

## U.S. composite insurance pricing change

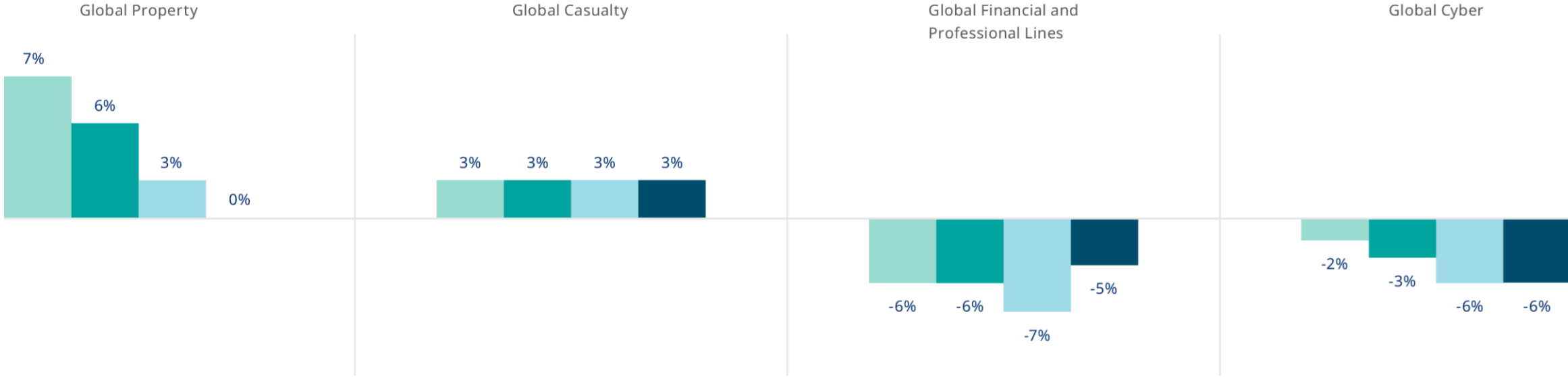


Source: Marsh Specialty and Global Placement

# Q2 2024 market observations

## Global composite insurance pricing change by major coverage line

Q3 23 Q4 23 Q1 24 Q2 24



Source: Marsh Specialty and Global Placement



# Property coverages

- Strong focus is now on properly calculated business interruption values.
- This is due to persistent fragile supply chain issues that delay post-loss recovery efforts.
- Severe weather risks also remain a dominating factor as we continue into hurricane season.

Sentrisk™ is a supply chain mapping solution providing unparalleled visibility and site-level assessment to **uncover your risks** that can develop into informed actions and long-term benefits.

# Casualty coverages

## Rate trends



### Automobile/fleet

Average rate increases were **9%** and higher double-digit increases for business classes with tougher risk profiles and/or adverse claims experience.



### General liability

Rate increases are averaging 4%, and higher for certain business classes, especially when the insurer doesn't also write the workers' compensation coverage.



### Umbrella/excess

Umbrella/excess liability risk-adjusted rates increased **10%**, compared to **11%** in the first quarter.



### Workers' compensation

Rates generally remained flat or in negative territory with decreases of around **-1%**.



# Aviation, environmental, international

## Rate trends

### Aviation

- Rate increases are averaging 3-8% with the hard market modestly decelerating. Loss-free risks can achieve flat renewals.
- Underwriters are expressing more interest in new business.
- Supply chain challenges and delays continue to inflate claim costs.

### Environmental

- Average rate increases were 0–5% for contractor’s pollution, 0%–15% for site pollution, 5-20% for combined-form liability, and 5-10% for combined pollution/professional liability.
- The EPA and many state agencies continue to propose and push through new environmental regulations, appearing to take advantage of the favorable political climate for environmental protection.

### International

- Renewal pricing remains stable on many international placements; however, property rates are on the rise.
- Defense Base Act (DBA) pricing continues to tumble as another new market entered the arena that has heated up the competition for government contractor placements.
- We are seeing a great deal of foreign direct investments (FDI) in the U.S.

# Surety

- The surety industry has seen increased claim activity over the last six months. Most of the claim activity is from small contractors with fewer financial resources.
- Residential starts are up 13% year-over-year and are predicted to remain at these levels through 2027.
- Non-residential starts are up 4% and are expected to remain stable through 2027.

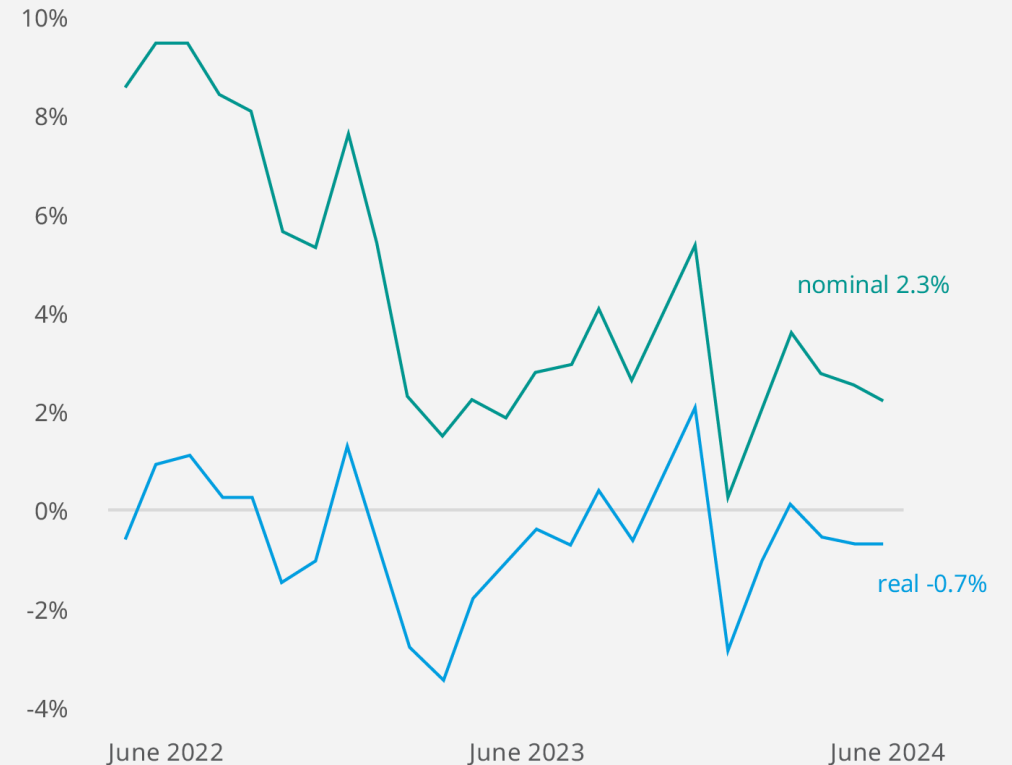


# Trade credit insurance (TCI)

- The increased need for TCI has continued through the summer with the Federal Reserve on break.
- Competition in the market has continued to see rates be more competitive than in the last two years.
- Carriers are being more aggressive on single line TCI. This makes rates more competitive through carriers on these single debtor insurance policies.

Retail sale indicators show that cost is increasing but overall volume is forcing companies to find new ways to approach credit through TCI.

## Retail Sales, nominal and real, year-over-year



Source: Allianz Trade: "The North" by Dan North



# Workplace violence

- **California employers** are encouraged to familiarize themselves with the requirements and implement necessary procedures to comply with Senate Bill 553.
  - This bill was signed into law and went into effect on July 1, 2024, mandating the creation of a Workplace Violence Prevention Plan.
- As noted previously, enhancing safeguards for business continuity during global and domestic social conflict should be at the forefront of most organizations' minds.
- Establishing incident response protocols, prioritizing response actions, and understanding insurance coverage options will all improve a business's resiliency in times of uncertainty.



# Safeguarding business continuity and resiliency

## Finding a path to adaptability

- Enhancing [safeguards for business continuity](#) during global and domestic social conflict should be at the forefront of most organizations' minds.
- Establishing incident response protocols, prioritizing response actions, and understanding insurance coverage options will all improve a business's resiliency in times of uncertainty.
- Schools, health care, municipalities, retail, restaurants, hospitality, and businesses with a high dependency on global supply chains are especially impacted.



# Cyber Liability Landscape

## Risk Environment & Insurance Marketplace

An Overview for the Financial Education Forum

**Mario Paez**, MBA, RPLU, CIPP/US  
Executive Vice President  
National Cyber Risk Leader

**Alyson Rene Rossi**, J.D., MLIS  
Senior Vice President, Executive Pro  
Regional Risk Manager, MMA Mid-Atlantic



# Webinar Overview and Objectives



**Informative** webinar focused on providing an overview of key themes relative to Cyber Liability risk



**Delve** into the coverage provided by a Cyber Liability insurance policy



**Designed** for executive leaders to provide high level knowledge relative to the market, risks, exposure, insurance and mitigation



**Share** best practices for mitigating cyber risks



**Provide** an overview of recent events and loss amounts experiences

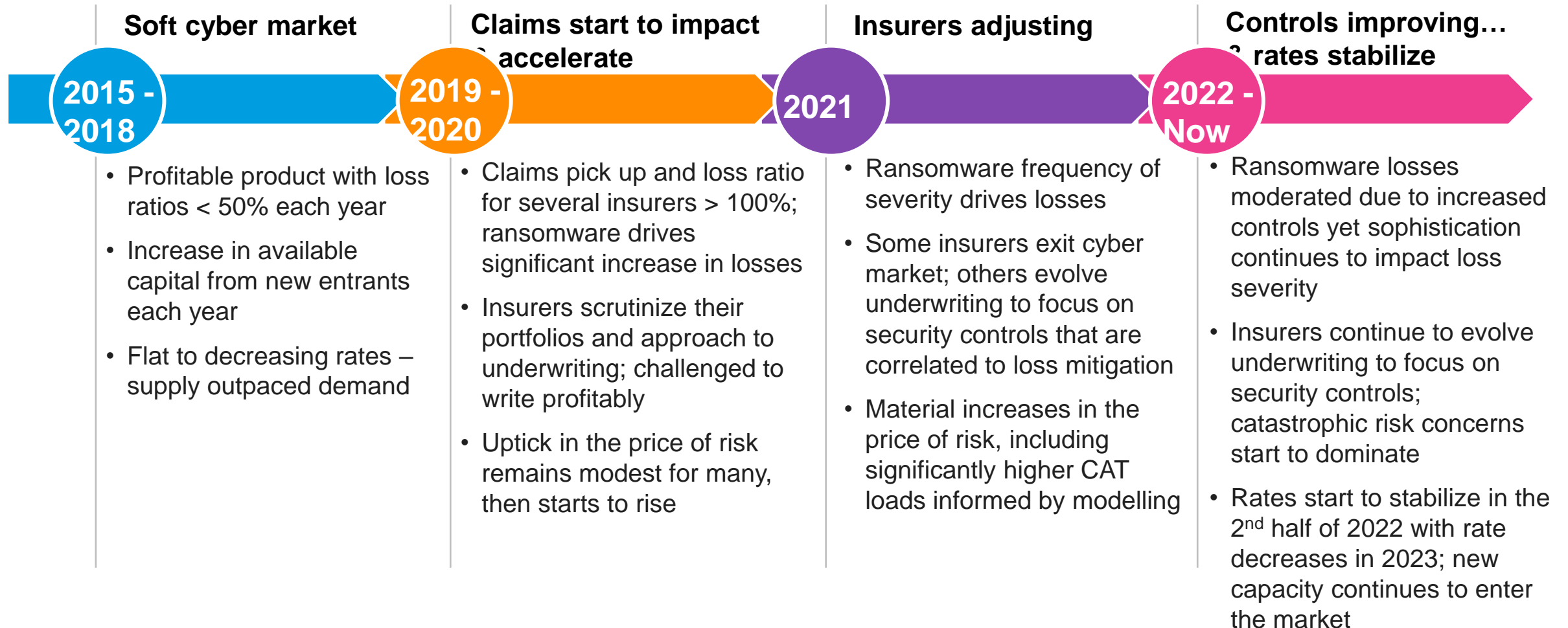


**Advise** attendees of the resources and tools offered by Marsh & McLennan Agency

# Cyber Liability Market Update

# Macro Cyber Trends: Cyber Market Dynamics

Frequency and severity of losses drove a rapid shift in the marketplace



# Cyber Insurance Market Snapshot

Cyber market maturing as insurers analyze loss development and mitigation efforts



## Claims & Risk Environment

- **Aggregation exposure and supply chain risk** continue to be top of mind
- **Cyber Events**
  - 16% increase in cyber claims reported through Q2 2024
  - Average demand size for ransomware has increased but number of companies paying is down\*
- **Privacy & regulatory** claims frequency rising in connection with broader privacy regulations & rights

## Pricing & Purchasing

- **Rates stabilizing**
- US clients continue to **increase total limits** purchased and **evaluate SIRs**
  - 13% of clients increased total limits in August
  - 18% of clients reduced SIRs in August
- Organizations continue to focus on making objective, data-based decisions regarding limits and SIRs to maximize program efficiency.

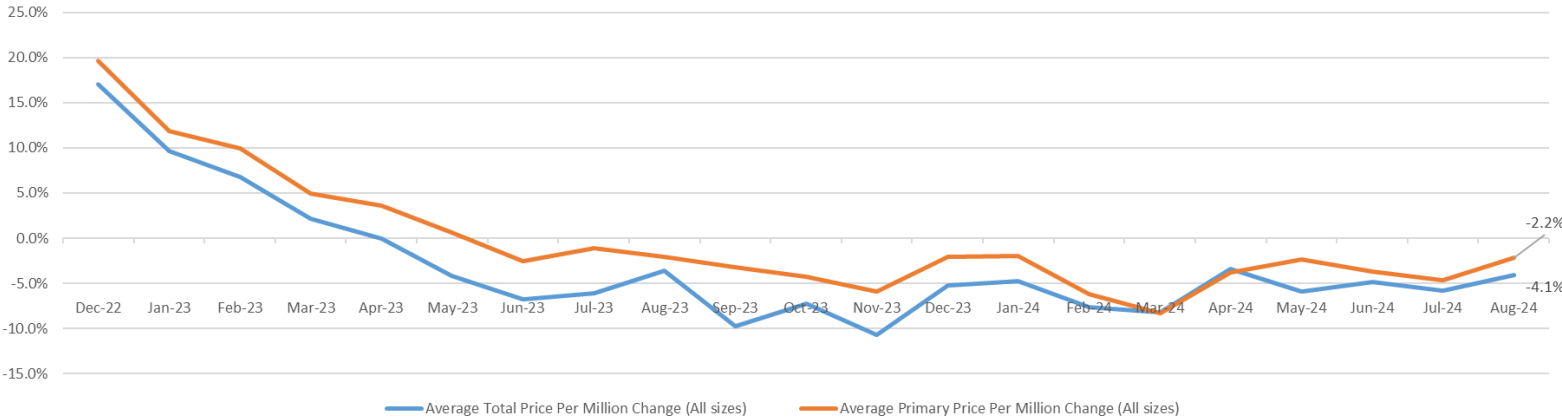
## Coverage & Underwriting

- **Approach to catastrophic cyber risk & war exclusions** varies widely by insurer
- **Coverage for newer privacy regulations** may be restricted pending controls & specific insurer appetite – current focus is wrongful collection, BIPA, and pixel tracking
- **Important to highlight cybersecurity updates & improvements** over past year – especially those in the top 12 controls

# Competitive Rate Trend Through August

Premium reductions continue despite evolving claims and risk environment

Average US Cyber Price Per Million Changes Over Time  
 Source: Marsh Global Placement & Specialties, Data and Analytics, PlaceMAP  
 Marsh Clients



Total price per mil	-9.9%	-2.9%	-4.1%	0.6%
Primary price per mil			-2.2%	

Total price per mil	-6.6%
Primary price per mil	-3.3%

\*\*Includes 23% of renewals with limit changes

### Takeaways:

1. Premium decreases continue into August
2. Clients are using savings to invest in additional cyber limits.
3. Opportunity to evaluate cyber limits against total cost of risk.

# Cyber Risk Environment

Constantly changing, but key themes remain



## Catastrophic risk:

- **Aggregation** exposure and **third party risk** is top of mind, as cyber risks stem from:
  - **Common vulnerabilities** – hardware or software
  - **Common dependencies** – digital supply chain vendors (such as cloud providers or software/SaaS)
- **Geopolitical tensions** add to market uncertainty, forcing additional discussions around how cyber insurance contracts should respond to scenarios arising out of conflict and war
- **Reinsurance pressure** is influencing carriers' approach to catastrophic risk, especially when it comes to coverage



## Privacy regulations:

- **GDPR** fines are growing (~\$877M Amazon, ~\$267M WhatsApp, ~\$68M Google, ~\$41M H&M, ~\$24M Marriott)
- **CCPA & CPRA** and similar legislation allow for private rights of action with per consumer statutory damages and require additional compliance efforts
- **BIPA** litigation is expensive and is on the rise. First jury trial resulted in damages of \$44M
- **Pixel tracking** litigation continues for organizations collecting consumer data; leading to class action suits.
- **Wiretapping and VPPA** complaints are increasing especially with the use of chatbots and tracking tools on websites



## Cyber incident evolution:

- **Data compromise & business interruption** continues to be the most impactful for all organizations
- **Data exfiltration** occurred in 75% of ransomware events in Q2 24, leading to other losses such as data breach or business interruption
- **Decrease in companies paying ransom demand.** 36% of companies paid a ransom in Q2 24 compared to 53% in Q2 21. This is a sign of improved controls and incident responses, despite ransomware activity increasing.
- **While ransomware claims are increasing, majority of cyber events involve unauthorized access without an extortion threat.** 88% of reported claims to Marsh US in Q2 24 didn't involve ransomware.



# Cybersecurity – Public Company Impact

## SEC Adopts Final Cybersecurity Disclosure Rules

### Rule-Making Update

- ✓ **Rulemaking Status:** The SEC announced proposed rules on **March 9, 2022**. Public comments were due **May 9, 2022** and later re-opened for a brief period ending **November 1, 2022**. The final rules were adopted on **July 26, 2023** (source: <https://www.sec.gov/news/press-release/2023-139>)
- ✓ **Categories of Disclosure:** As outlined below, the final rule includes **two categories** of cyber-related disclosures: material cybersecurity incident reporting and cyber risk management, strategy and governance disclosures
- ✓ **Effective Date:** At the earliest, December 18, 2023 for the cyber incident reporting rule and for fiscal years ending on December 15, 2023 or later for the annual cyber risk management, strategy and governance disclosures

#### Current Reporting of Material Cybersecurity Incidents

- Reports must be filed within four business days after determination of a “material” cybersecurity incident
- Exception for disclosures that would pose a substantial risk to national security or public safety, contingent on a written notification by the Attorney General
- Update disclosures regarding previously disclosed cybersecurity incidents

#### Cybersecurity Risk Management, Strategy and Governance

- Report on processes for assessing, identifying and managing material cybersecurity risks
- Describe management’s role and expertise in assessing and managing material risks from cybersecurity threats
- Outline the board of directors’ expertise and oversight of cybersecurity risks



# Third-Party Cyber Risk

Cyber risks associated with third-party technology are a growing threat. How does this impact your organization?

**60%**

of organizations work with more than 1,000 third parties

**71%**

of organizations report their third-party network contains more vendors than it did three years ago

**73%**

of organizations have experienced significant disruption caused by a third party, whether it be a data breach or ethical violation

**73%**

of organizations say their third parties have more access to organizational data assets than three years ago

**80%**

of organizations report their third-party diligence questionnaires have increased in recent years



How widespread is the use of technology in your operations?

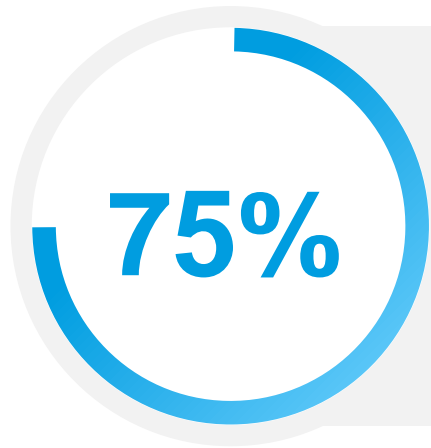


Who are your top critical vendors (both for operations and technology)?



If you were unable to access your network, how would that impact your business?

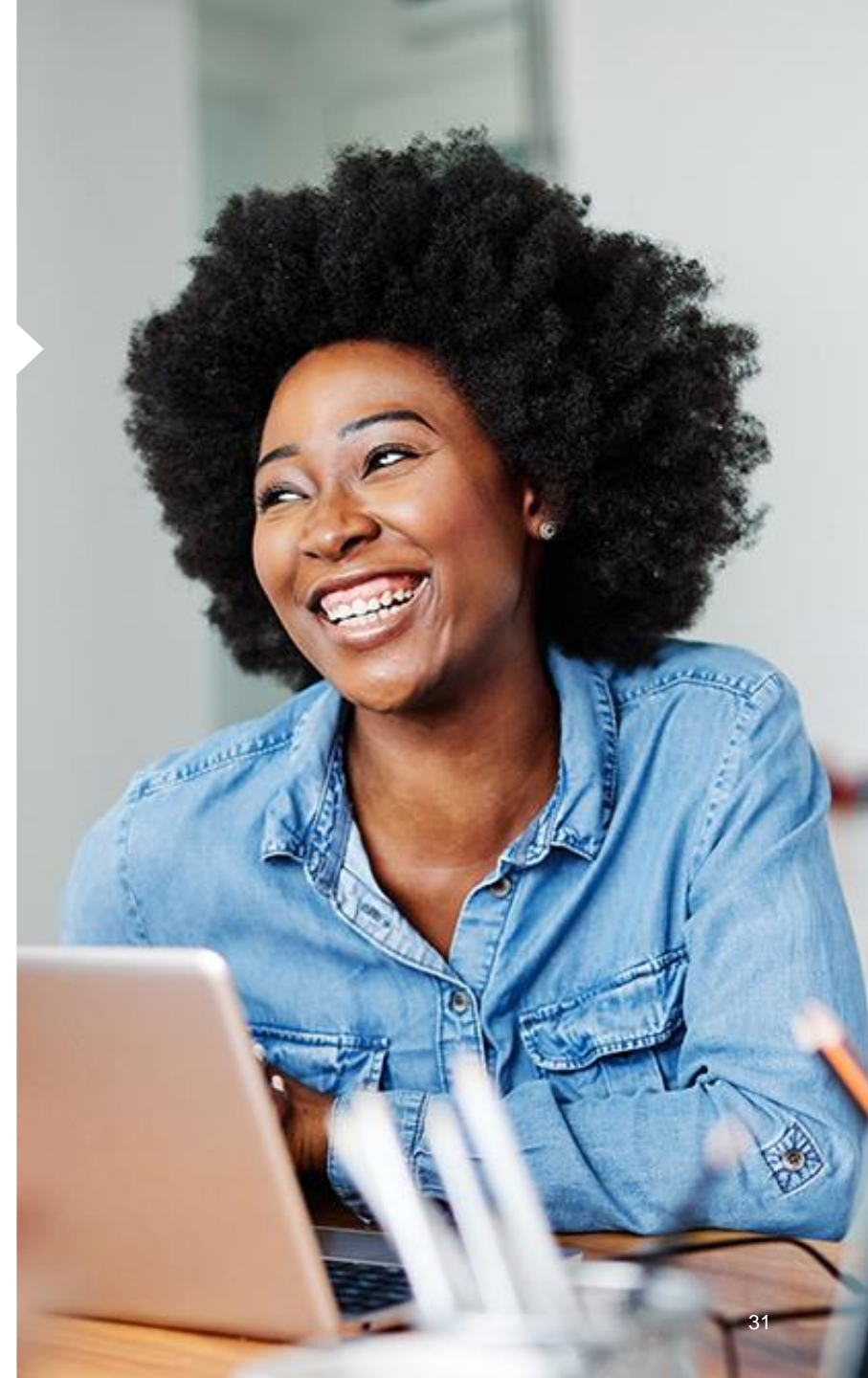
# Cyber and data risks



of business leaders are extremely or very concerned about cybersecurity and data privacy.<sup>1</sup>

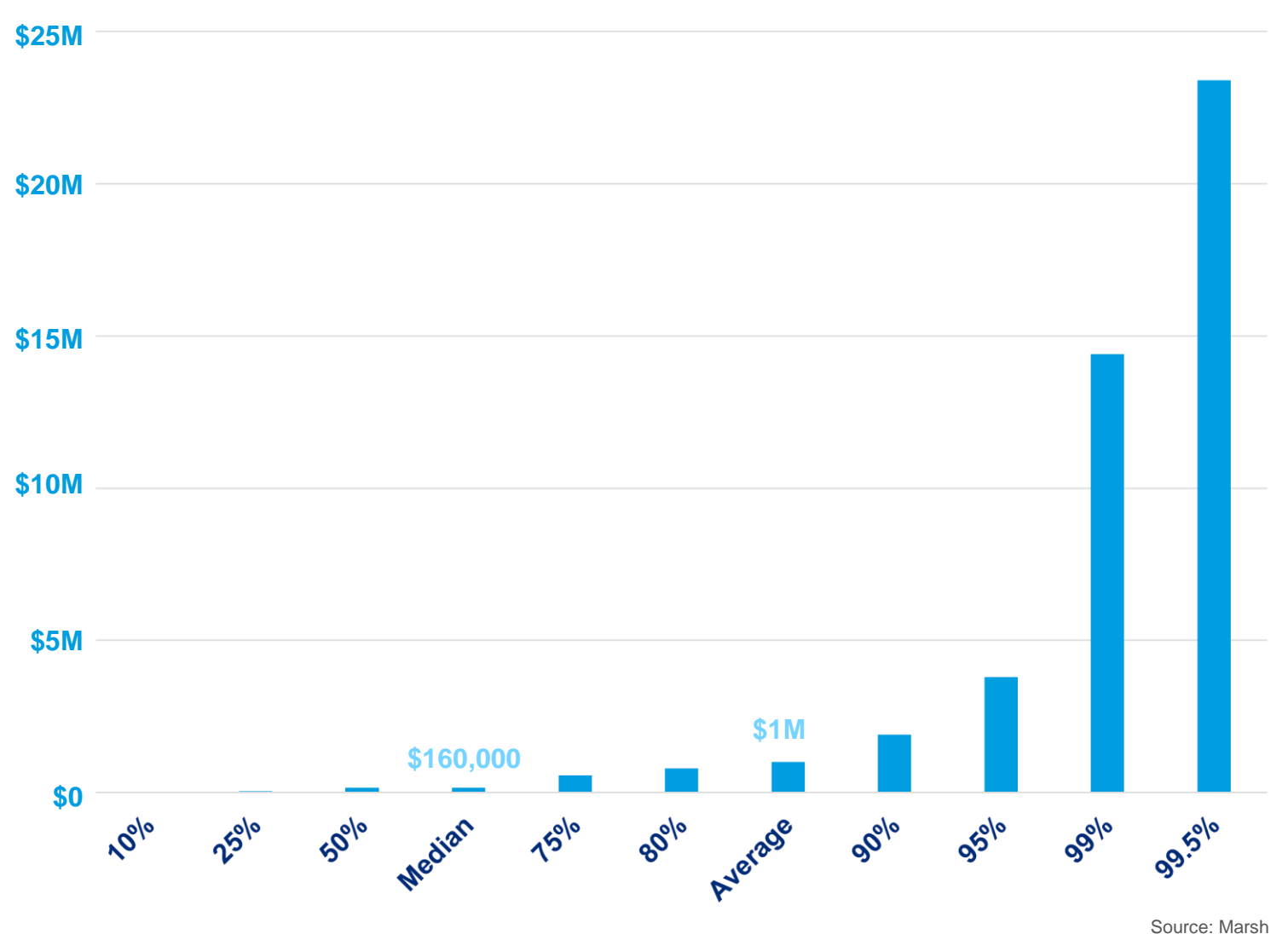
Security and data privacy seem to be two key areas of opportunity for organizations when it comes to digital protection and compliance.

<sup>1</sup> Source: 2024 Marsh McLennan Agency Business Insurance Trends Survey



# Cyber Events

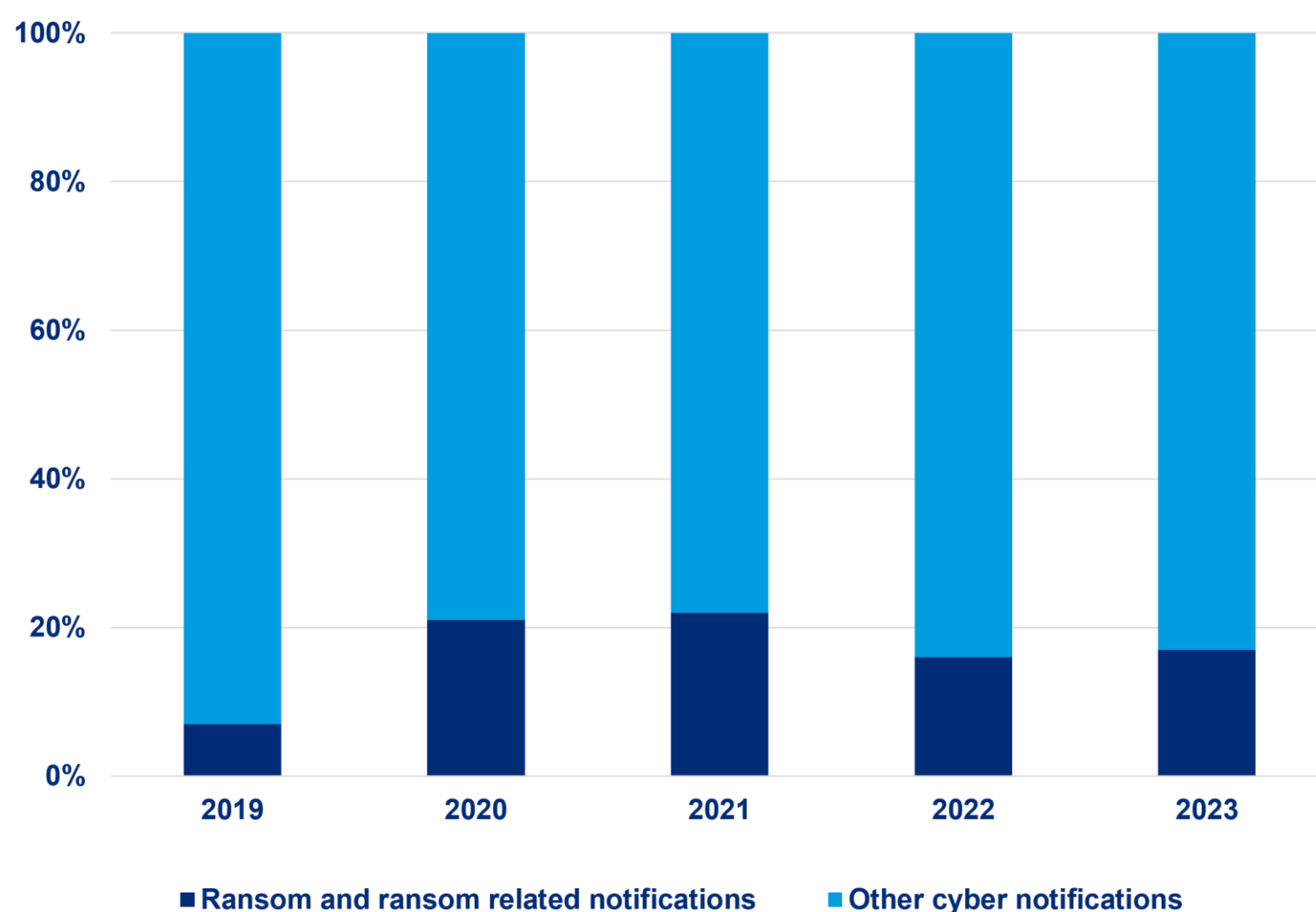
# Breach response costs average \$1 million (2019-2023)



During the last five quarters, the median cost of breach response expenses remained around \$160,000, while the average has trended upwards, from \$963,000 in the third quarter of 2023 to \$1 million in the fourth quarter, primarily due to a few large cyber events.

*Note: Distributions are lognormal to protect client's privacy. Statistics are derived from disclosure of cost incurred by clients, which may vary in terms of partial, full or non-disclosure.*

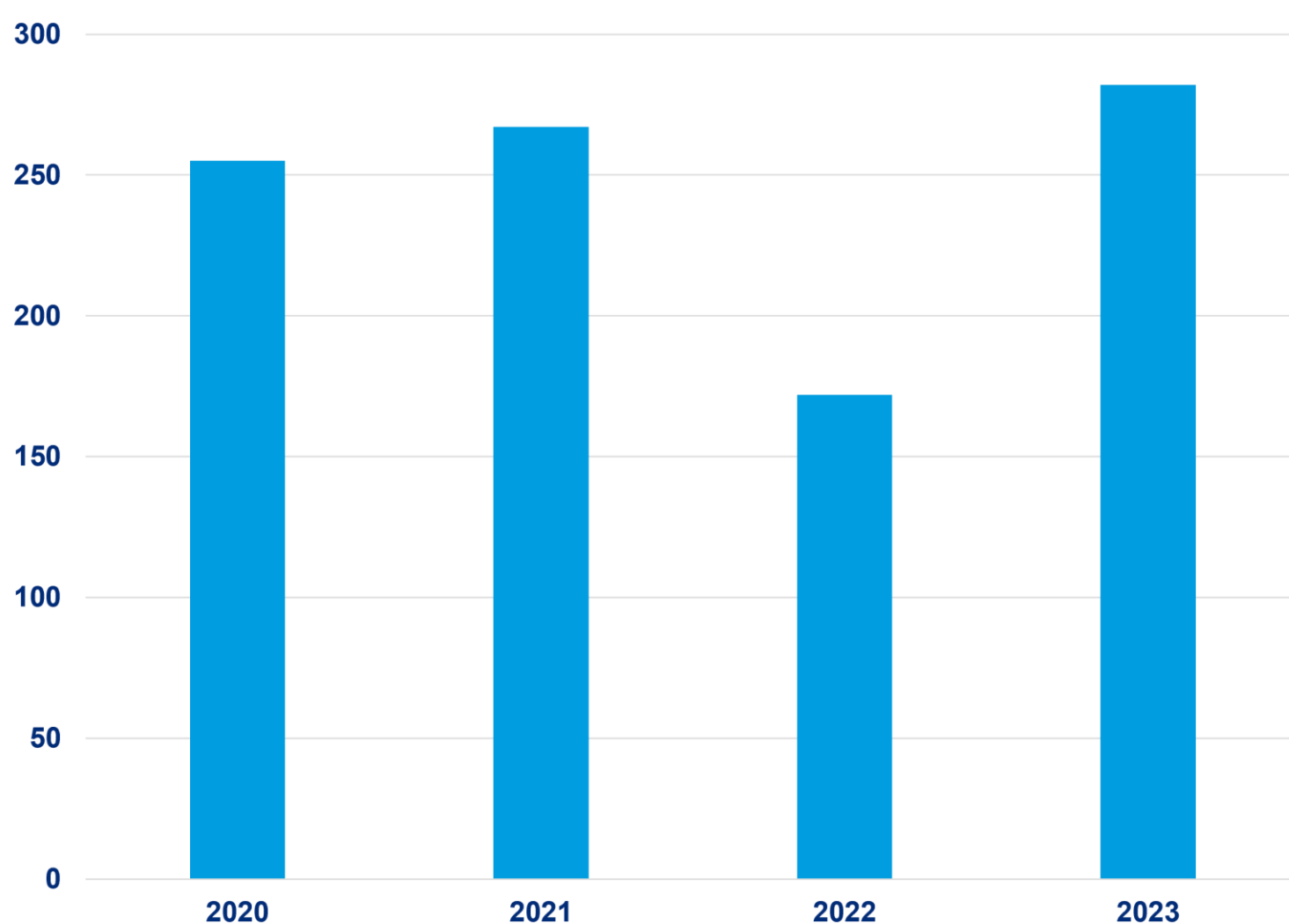
# Cyber extortion events were under 20% of total reported cyber claims in 2022 and 2023



Privacy claims and system attacks leading to unauthorized access and potentially exposed data without an extortion component comprise a much larger share of cyber events reported by Marsh clients than do those with an extortion component.

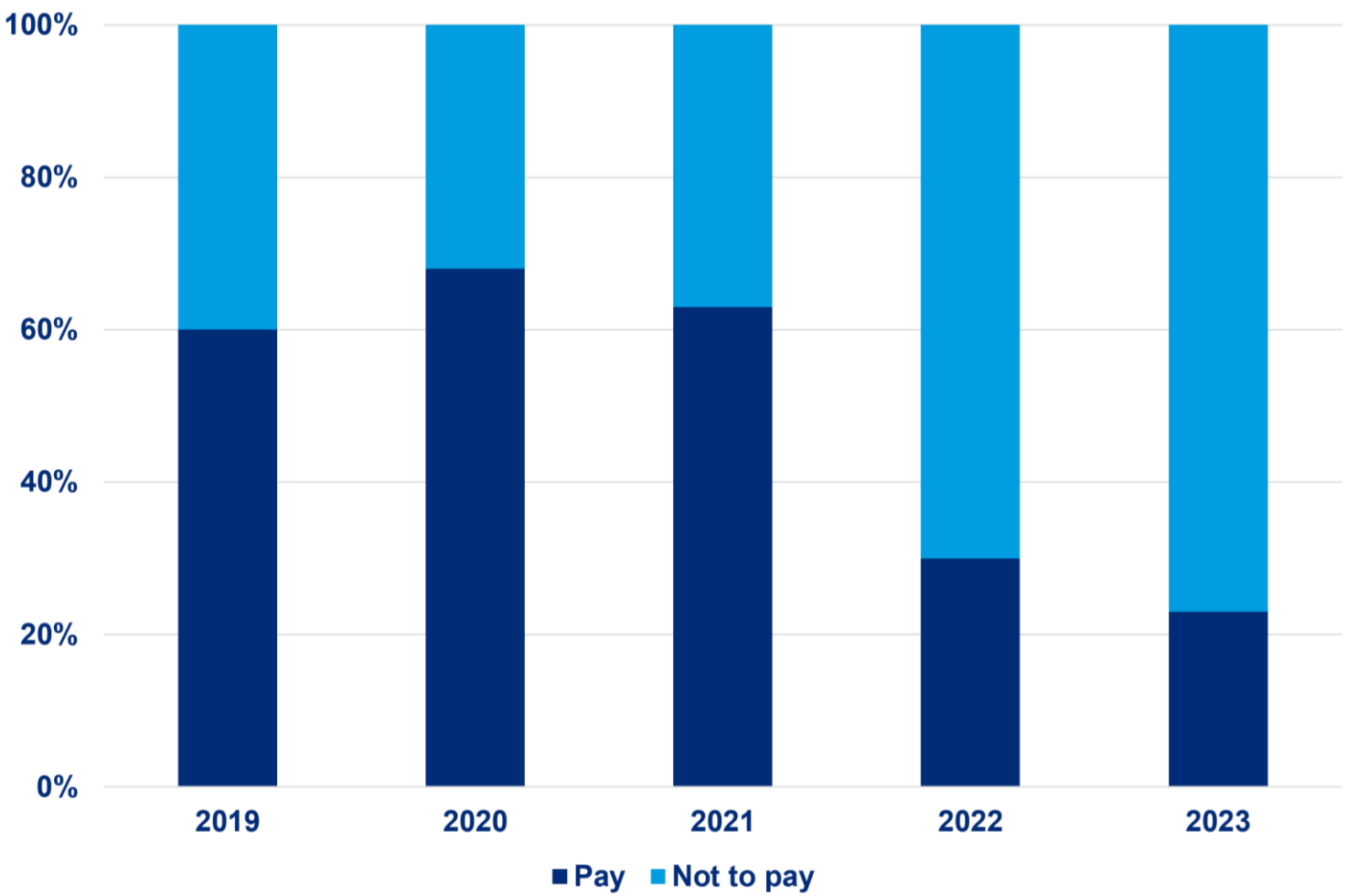


# Cyber extortion events increase in 2023 after 2022 dip



Possible reasons for the 2022 decline, include, but are limited to (temporary) move away from data encryption toward exfiltration, disruptions brought on by the start of the Russia-Ukraine war, decreased willingness of some companies to pay, and the successful “infiltration” of a particular ransomware group by the FBI.

# The percentage of companies paying ransom demands continues to decline



Marsh clients continue to invest in cyber resiliency. Examples include tabletop exercises, incident response vendor readiness, downtime procedures, out of band communication plans, and effective cybersecurity controls.

The effectiveness of such investments is indicated by the continued drop in the percentage of those opting to pay an extortion demand.

# Cyber Liability Insurance Coverage

# Cyber Coverage Parts

## First party coverage with claims examples

	DESCRIPTION	COVERED COSTS	CLAIMS EXAMPLES
<b>First Party Coverage</b> 1 <sup>st</sup> Party Insurance coverage: direct loss and out-of-pocket expense incurred by insured			
<b>Event Management / Breach Response</b>	Costs incurred responding to a network security or privacy breach.	<ul style="list-style-type: none"> <li>• Forensics</li> <li>• Notification</li> <li>• Credit Monitoring</li> <li>• Call Center</li> <li>• Public Relations</li> <li>• Legal Costs</li> </ul>	<ul style="list-style-type: none"> <li>• You suffer a data breach and incur costs ranging from IT forensic analysis, legal advice, costs to notify affected parties, credit monitoring for affected parties, and public relations assistance to help restore public trust in your firm.</li> </ul>
<b>Cyber Extortion</b>	Costs associated with a ransomware event, regardless of whether or not a ransom demand is paid.	<ul style="list-style-type: none"> <li>• Negotiation &amp; ransom payments</li> <li>• Forensics</li> <li>• Investigation</li> </ul>	<ul style="list-style-type: none"> <li>• Your employee unwittingly clicks a link in a phishing email resulting in ransomware locking out your ability to utilize business critical technology until a ransom demand is paid (or you're able to restore your network from back-ups).</li> </ul>
<b>Business Income/ Extra Expense</b>	Interruption or suspension of computer systems due to a network security breach. Coverage may be added to include system failure and can extend to contingent businesses.	<ul style="list-style-type: none"> <li>• Loss of Income</li> <li>• Costs in excess of normal operating expenses required to restore systems</li> <li>• Forensic expenses</li> <li>• Dependent business interruption</li> </ul>	<ul style="list-style-type: none"> <li>• Malware gets into the computerized factory controllers causing the line to cease operating. IT forensics must be performed to restore system operations.</li> <li>• During routine network patching duties, an IT employee accidentally crashes the critical IT infrastructure causing operational disruption when the IT systems are inaccessible.</li> <li>• A supplier you depend for delivery of your end service to customers suffers a cyber event that prevents them from delivering critical parts/services to you. You sustain a business income loss.</li> </ul>
<b>Data Asset Protection</b>	Costs to restore, recreate, or replace electronic data and other digital / intangible assets that are corrupted or destroyed.	<ul style="list-style-type: none"> <li>• Restoration of corrupted data</li> <li>• Vendor costs to recreate lost data</li> </ul>	<ul style="list-style-type: none"> <li>• After a cyber event that impairs your IT (or OT) network, costs are incurred to hire an IT forensics firm to determine whether the information can be restored. The data is recreated and restored.</li> </ul>

# Cyber Coverage Parts

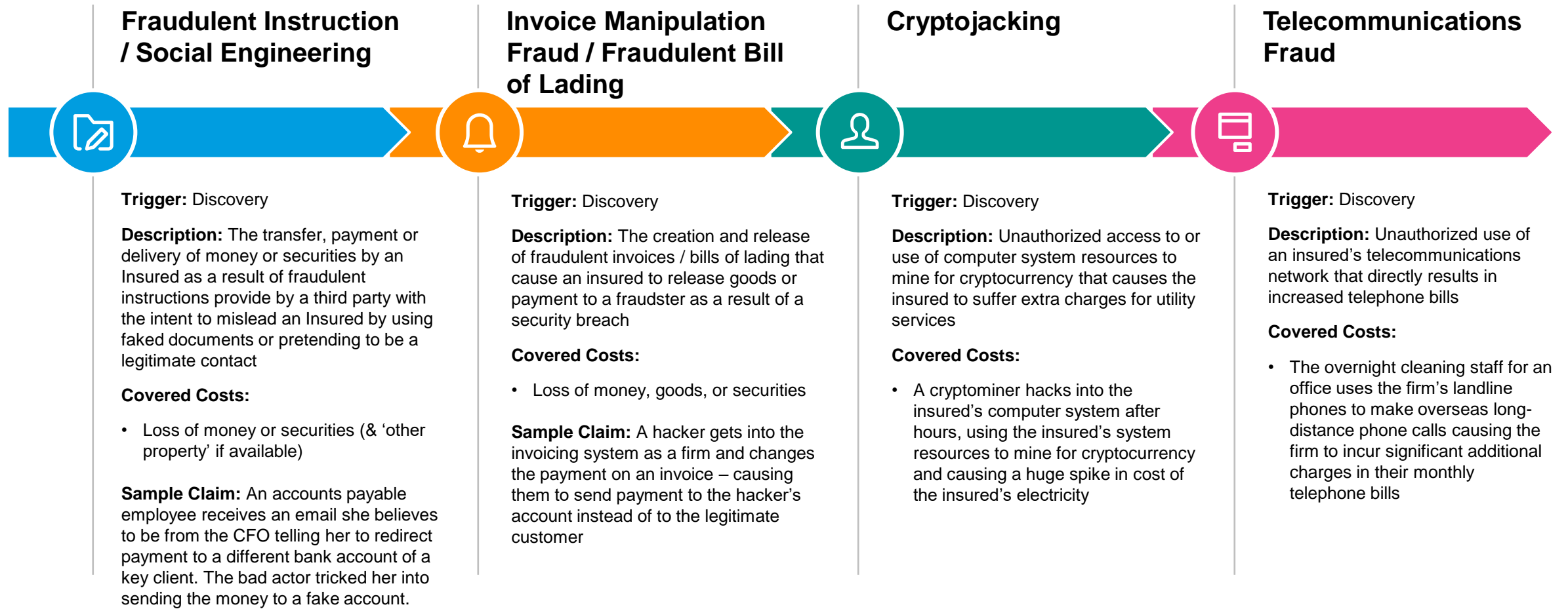
## Third party coverage with claims examples

	DESCRIPTION	COVERED COSTS	CLAIMS EXAMPLES
<b>Third Party Coverage</b> 3rd Party insurance coverage: defense and liability costs due to alleged harm caused to others by the insured.			
<b>Privacy / Network Security Liability</b>	Failure to prevent unauthorized access / disclosure of personally identifiable or confidential information; Failure of system security to prevent or mitigate a computer attack	<ul style="list-style-type: none"><li>• Liability and defense</li><li>• Bank lawsuits</li><li>• Consumer lawsuits</li></ul>	<ul style="list-style-type: none"><li>• A breach of your computer network leads to loss of sensitive customer information. Customers file suit against you for the failure to protect their private data.</li><li>• Your network security fails to prevent a self-propagating malware from being transmitted from your network to a third party. You are sued for financial damages incurred by 3<sup>rd</sup> parties.</li></ul>
<b>Privacy Regulatory Defense Costs &amp; PCI Fines &amp; Penalties</b>	Investigations and related fines or penalties assessed by Regulators or for violation of PCI data security standards	<ul style="list-style-type: none"><li>• Liability and defense</li><li>• PCI / PHI / regulatory fines and penalties</li><li>• Prep costs to testify before regulators</li></ul>	<ul style="list-style-type: none"><li>• A data breach leads to an investigation by a regulator such as the Office Of Civil Rights (OCR) for a breach of sensitive healthcare information leading to a HIPAA violation</li><li>• A EU data protection authority investigates a potential GDPR violation.</li></ul>
<b>Media Liability</b>	Including but not limited to: libel, slander, product disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, etc.	<ul style="list-style-type: none"><li>• Liability and defense</li></ul>	<ul style="list-style-type: none"><li>• You are sued by a competitor when your CEO posts disparaging comments about the competitor on a social media site.</li></ul>
<b>Tech E&amp;O</b>	Acts, errors or omissions in the performance of technology services to others for a fee; or the failure of technology products to perform as intended – resulting in a financial loss.	<ul style="list-style-type: none"><li>• Liability and defense</li></ul>	<ul style="list-style-type: none"><li>• There is an error in the code that runs your hardware product which prevents it from operating properly. Because your customer cannot use the product, they sue you for breach of contract and other financial damages.</li></ul>



# Additional Extensions

## Various Forms of Fraud/Crime



# Cyber Risk Mitigation and Incident Response

# Top Cybersecurity Controls

## The key to insurability, mitigation, and resilience

### Preparation for the underwriting process:

1. Start early! Evaluate your cybersecurity maturity by completing Marsh's Cyber Self-Assessment. Lack of key controls may put availability of coverage at risk.
2. Use Marsh Cybersecurity Marketplace Services for access to a curated portfolio of cybersecurity vendor solutions and holistic vendor procurement support.
3. Expect detailed cybersecurity questions from underwriters.



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

# Ransomware Incident Response Tips



Be mindful of electronic communications



Adhere to OFAC requirements



Maintain proper records



Do not contact the threat actors directly



Decide whether to pay the ransom/extortion demand



Determine relevance of other coverage



Consult legal counsel about notification to law enforcement



Understand insurer involvement and consent provisions

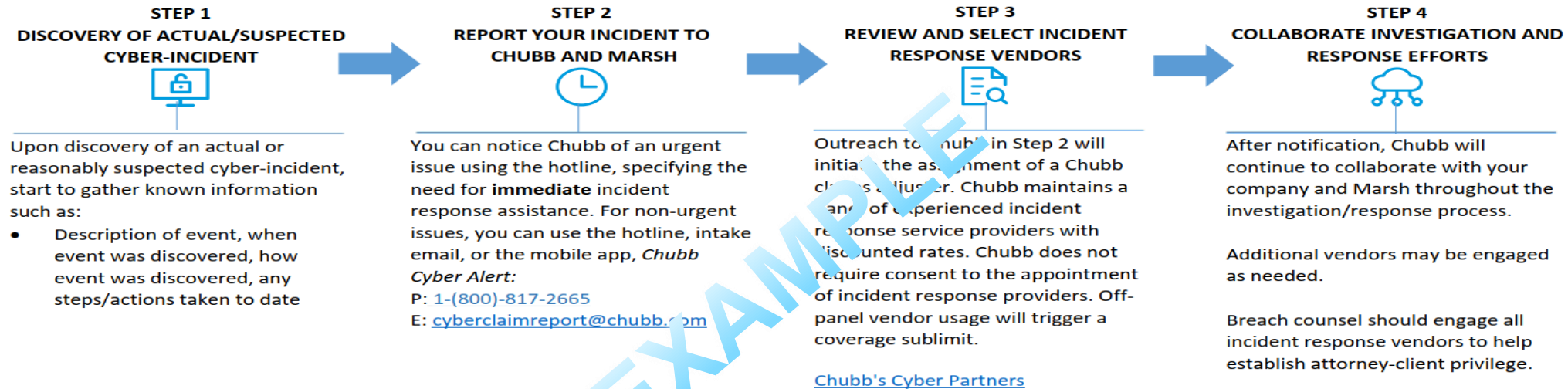


Track data recovery and restoration costs

# What to do in event of an incident

## Chubb Cyber ERM and DigiTech ERM (Cyber and Tech E&O) – Cyber-Incident Protocol

Cyber-Incident Process: what to do in the event of a cyber-incident



### Key Incident Response Notes related to Chubb's Cyber Policy

- Contact your Marsh representatives to submit formal notice under your policy
- A Marsh Claims Specialist will be assigned to your incident and can coordinate an initial triage call with incident response providers\*
- **A Non-Panel Response Provider sublimit is triggered even if you engage only one non-panel incident response provider**
- Mullen Coughlin is Chubb's preferred breach counsel firm and will run a conflict check once notice is provided via the hotline. You must inform Chubb if another breach counsel firm has been engaged at the time of hotline notification
- Keep Chubb apprised of material incident updates even if incident costs are likely within the retention. Marsh can assist in information sharing with Chubb as recommended by breach counsel
- Ransomware best practices:
  - Chubb may have additional requirements as ransomware is a constantly evolving risk due to [Office of Foreign Assets Control \(OFAC\)](#) guidance, reimbursement timing, and law enforcement notification

### Loss Mitigation Services

Chubb may provide complimentary or discounted proactive services with your cyber policy. Please contact your Cyber broker for more information.

\*Reporting the incident via the hotline does not constitute formal first notice of loss. Always contact your Marsh representatives to submit formal notice, consider other potentially applicable coverage(s), and trigger excess carrier(s) which may or may not occur simultaneously as incident unfolds. This document is a summary of the incident response process envisioned by your cyber policy. It is not meant to reflect all of the details in your policy. For specific questions please refer to your cyber policy with assistance from your cyber broker.



# MMA Cyber Resiliency Network

Marsh McLennan Agency (MMA) aims to provide timely, comprehensive, and actionable information to help you confidently address cyber risk threats and prepare you to navigate risk. MMA's Cyber Resiliency Network offers partner resources that assist you with three distinct areas of cyber risk management:

**1 Proactive information security**

**2 Privacy law compliance and risk management**

**3 Employee cyber security training and education**

As a client, you receive **exclusive access to complimentary or discounted services** from our partner network.

These services and relationships can help ensure compliance with your organization's statutory, regulatory, and contractual framework, as well as provide incident response best practices.

# Executive & Professional Specialty Practice

A team with subject matter expertise & industry insight

Our sixteen person team specializes in Executive, Professional, and Cyber & Privacy Liability across a wide array of industries, assisting privately-held, publicly-traded, and not-for-profit organizations. Our combined years of experience brings expertise and perspective from the brokerage, underwriting, claims adjustment, finance, and legal backgrounds.


## MMA by the numbers



Team members with law degrees



Team members with MBA's




One team member with (AIS) designation




Team members with Management Liability Insurance Specialist (MLIS) designations



Team members with Cyber COPE® designation




One team member with Cyber Professional Liability Practitioner (CPLP) designation




One team member with Registered Professional Liability Underwriter (RPLU) designation



Market expertise with specialization in claims advocacy



Two team members with Associate in Claims (AIC) designation



Strategies for organizational procedures to mitigate risk



# Winning in a hard market

- Choose a trusted insurance advisor
- Utilize advisors resources
- Take a team approach
- Start the process early
- Analyze and benchmark
- Choose carrier partners that align with company vision
- Consult frequently
- Conduct stewardship semi annually

# Our Next Session:

- ▶ **Thursday, Oct. 31, 8-10 A.M.**  
**Economic Outlook and Capital Markets Update** Presented by **Wells Fargo** (2 CPE Hours)
- ▶ Scan **QR Code** to sign up for next sessions and view session recordings



# Thank you to our sponsors!



Cordia Partners is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: [www.NASBARegistry.org](http://www.NASBARegistry.org).

## About Cherry Bekaert

"Cherry Bekaert" is the brand name under which Cherry Bekaert LLP and Cherry Bekaert Advisory LLC, independently owned entities, provide professional services in an alternative practice structure in accordance with applicable professional standards. Cherry Bekaert LLP is a licensed CPA firm that provides attest services, and Cherry Bekaert Advisory LLC and its subsidiary entities provide tax and advisory services. For more details, visit [cbh.com/disclosure](http://cbh.com/disclosure).

This material has been prepared for general informational purposes only and is not intended to be relied upon as tax, accounting, or other professional advice. Before taking any action, you should consult a professional advisor familiar with your particular facts and circumstances.



[cbh.com](http://cbh.com)

