Cyber: Global Market Update and D&O Risk

CAS Spring Meeting 2025, Toronto, Canada

Monday, May 5, 2025

2:30 PM – 3:30 PM

About the Academy

Mission:
To serve the public and the U.S. actuarial profession.

Community:
Serving over 20K MAAAs & public stakeholders for 60 years

Standards:
Setting qualification, practice, and professionalism standards

Impact:
Delivering over 300 insight-driven publications & resources annually

Visit www.actuary.org to learn more.

Antitrust Notice

- The Casualty Actuarial Society is committed to adhering strictly to the letter and spirit of the antitrust laws. Seminars conducted under the auspices of the CAS are designed solely to provide a forum for the expression of various points of view on topics described in the programs or agendas for such meetings.
- Under no circumstances shall CAS seminars be used as a means for competing companies or firms to reach any understanding – expressed or implied – that restricts competition or in any way impairs the ability of members to exercise independent business judgment regarding matters affecting competition.
- It is the responsibility of all seminar participants to be aware of antitrust regulations, to prevent any written or verbal discussions that appear to violate these laws, and to adhere in every respect to the CAS antitrust compliance policy.

Presenters

Moderator

Andrew Li, FCAS – Head of Pricing, Corvus Insurance

Speakers

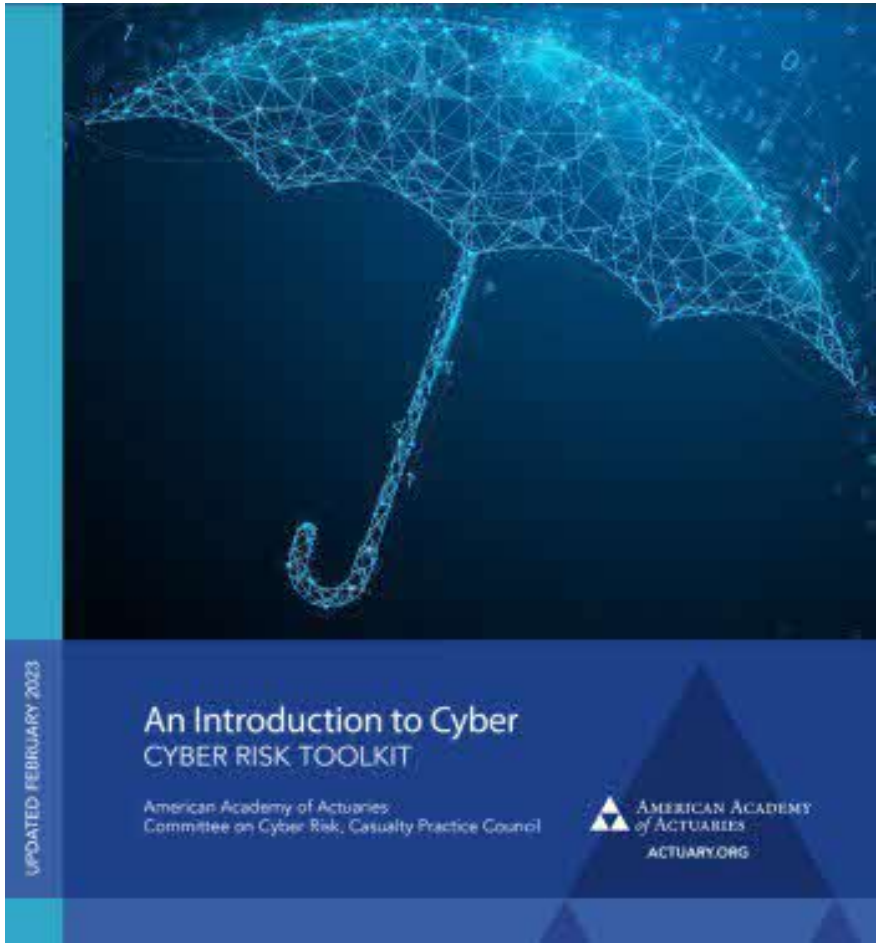
- Katie Koch, MAAA, FCAS – Vice President & Principal, Lewis & Ellis
- Isabelle McCullough, MAAA, ACAS – Cyber Reinsurance Pricing Lead, AXIS Capital
- Samuel Tashima, MAAA, FCAS, MBA – Head of Cyber Risk Consulting & Analytics - North America, Aon

Agenda

- Insurance Trends and SEC Disclosure Requirements
- Global Cyber Market
- Cyber Risk and Vendor Models

Cyber Risk Toolkit

actuary.org/cybertoolkit



Cyber Risk Toolkit

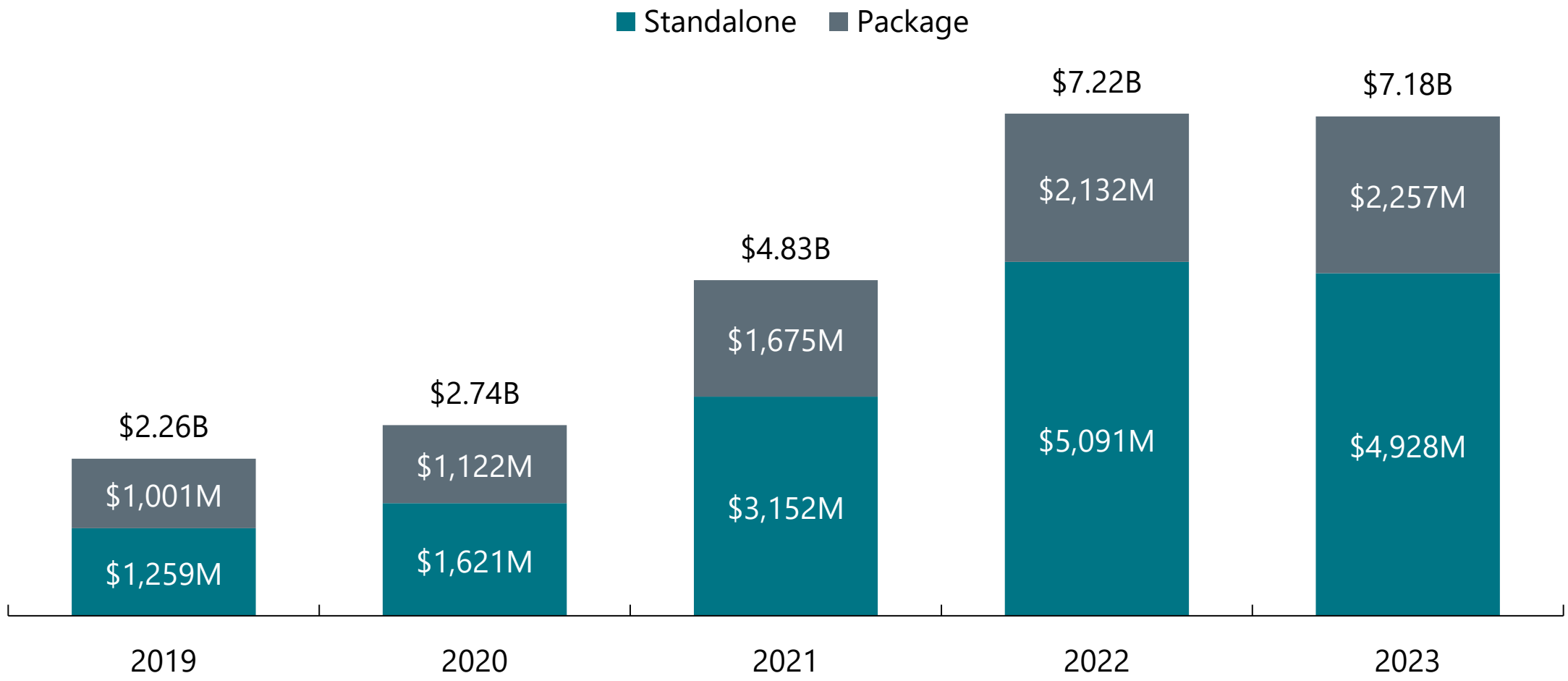
- Developed by the Academy's Committee on Cyber Risk
- Addressing issues pertinent to cyber risk and exposure that impact most lines of business
- Serving as a resource for the public, policymakers, the actuarial profession, the insurance sector, and other stakeholders
- Offering a cohesive overview of the challenges posed in the cyber insurance market, with each paper as a standalone piece
- Continuously updated to reflect new and emerging work from the committee

Cyber Insurance Landscape and Recent Trends

Samuel Tashima, MAAA, FCAS

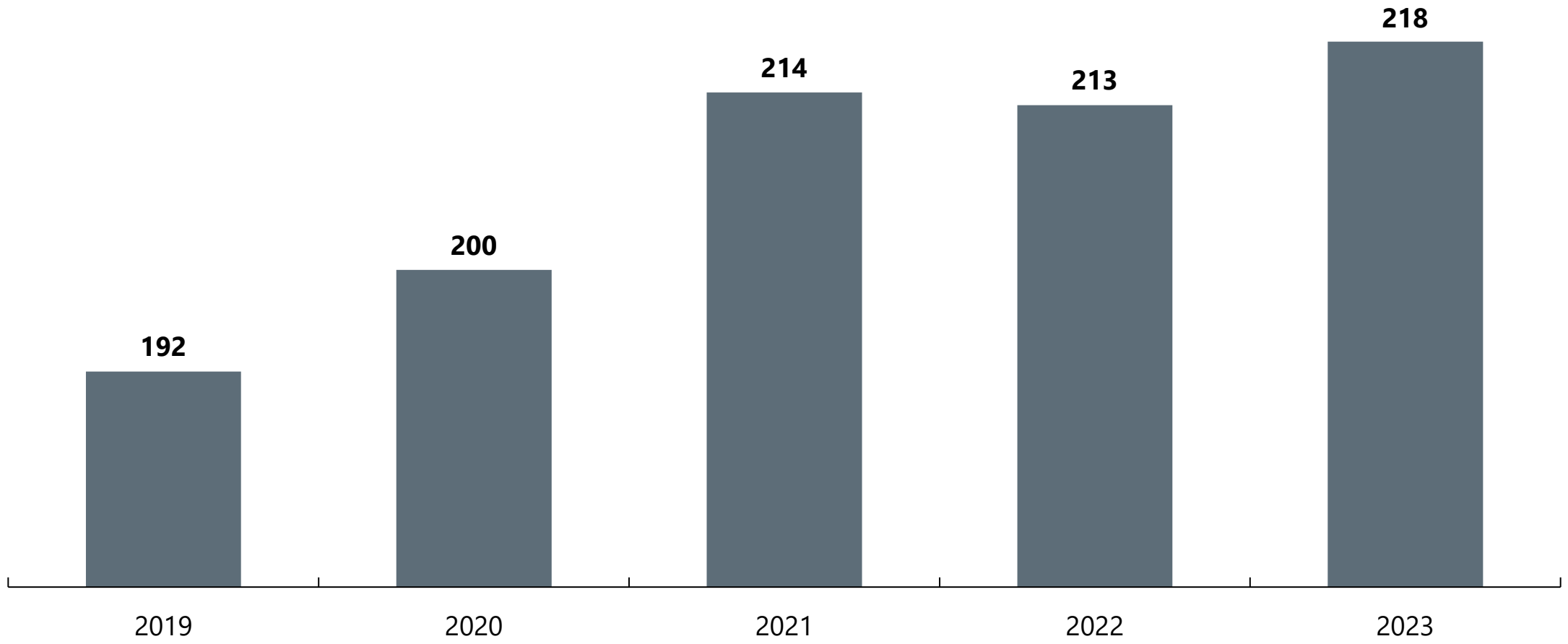
Vice Chairperson, Committee on Cyber Risk

U.S. Cyber Direct Written Premiums | 2017–2023



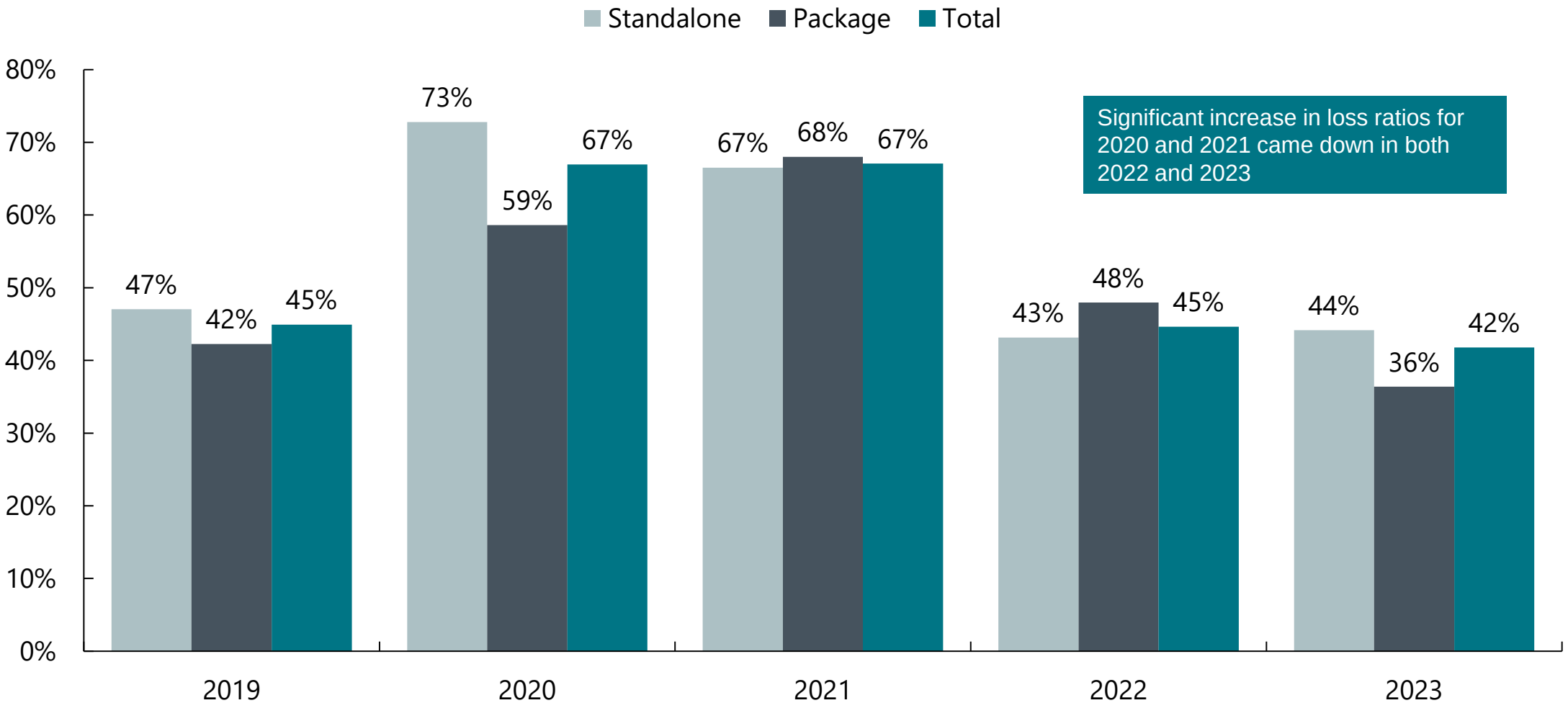
Source: Aon's U.S. Cyber Market Update: 2023 U.S. Cyber Insurance Profits and Performance

Number of U.S. Cyber Insurers | 2017–2023



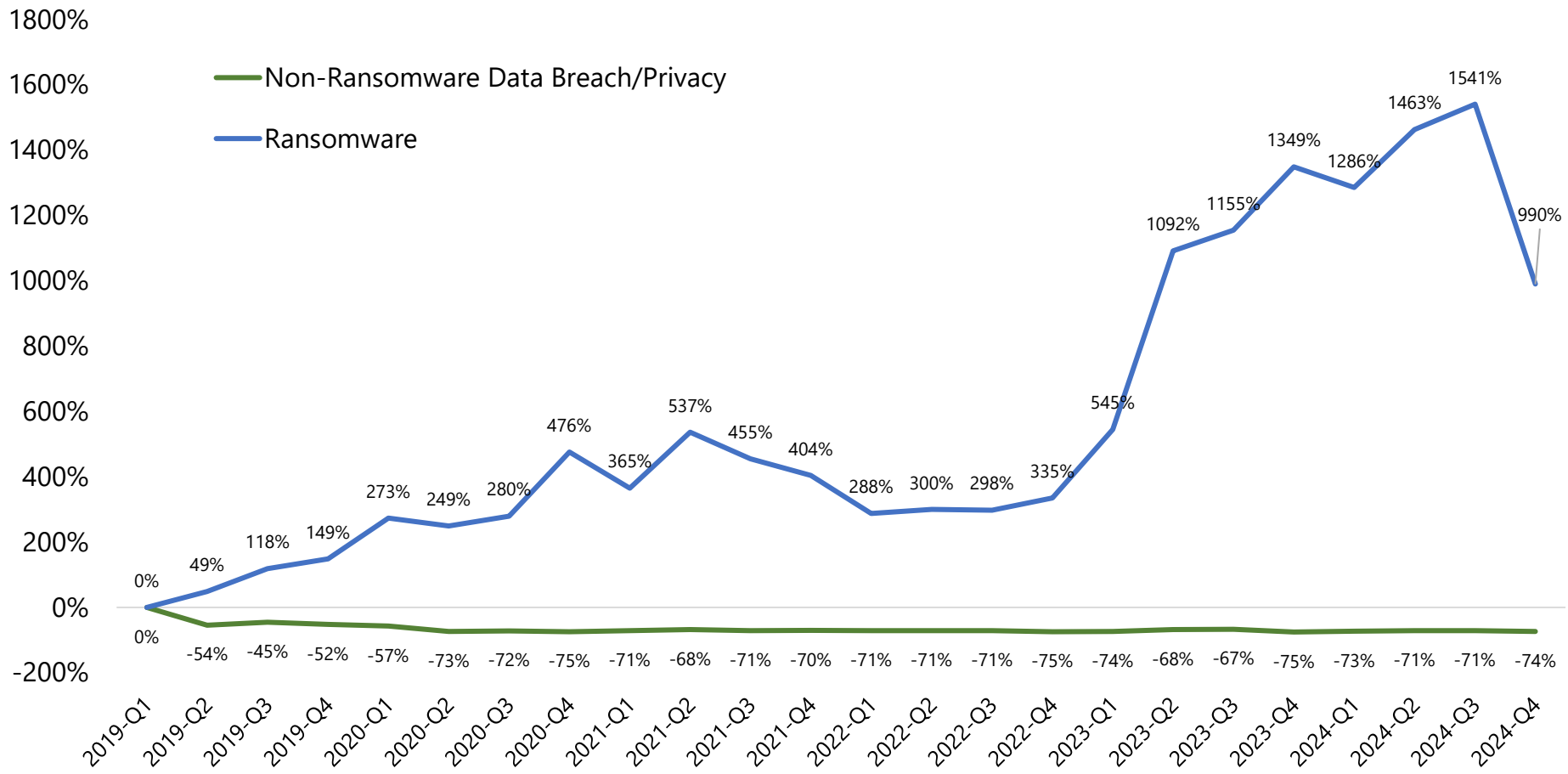
Source: Aon's U.S. Cyber Market Update: 2023 U.S. Cyber Insurance Profits and Performance

U.S. Cyber Loss Ratio | 2017–2023



Source: Aon's U.S. Cyber Market Update: 2023 U.S. Cyber Insurance Profits and Performance

Cyber Incident Rates Indexed to Q1 2019

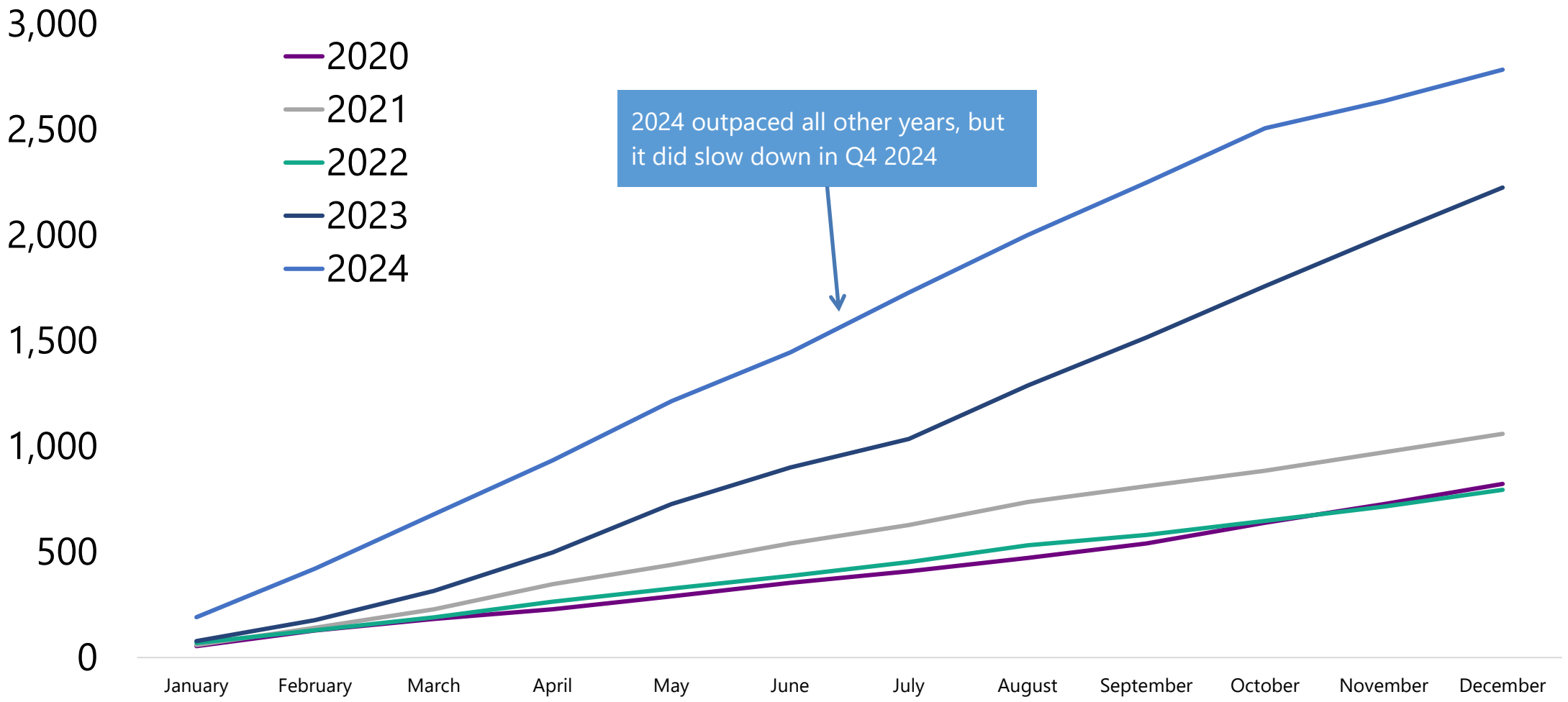


Key Observations:

- Ransomware activity was down compared to prior quarters in Q4 2024 yet continued to remain elevated compared to pre-Q1 2023
- Ransomware events were up 990% from Q1 2019 to Q4 2024
- Compared to Q3 2024:
  - Ransomware events were down by 34%; however, Q3 2024 was one of the largest ransomware quarters to date
  - Non–Ransomware Data Breach/Privacy Events were down by -8%
- The most commonly impacted industries by Ransomware in Q4 2024:
  - Business Professional Services
  - Manufacturing
  - Real Estate / Construction
  - Health care

Source: Risk Based Security, analysis by Aon. Data as of 3/1/2025; Claim count development may cause these percentages to change over time

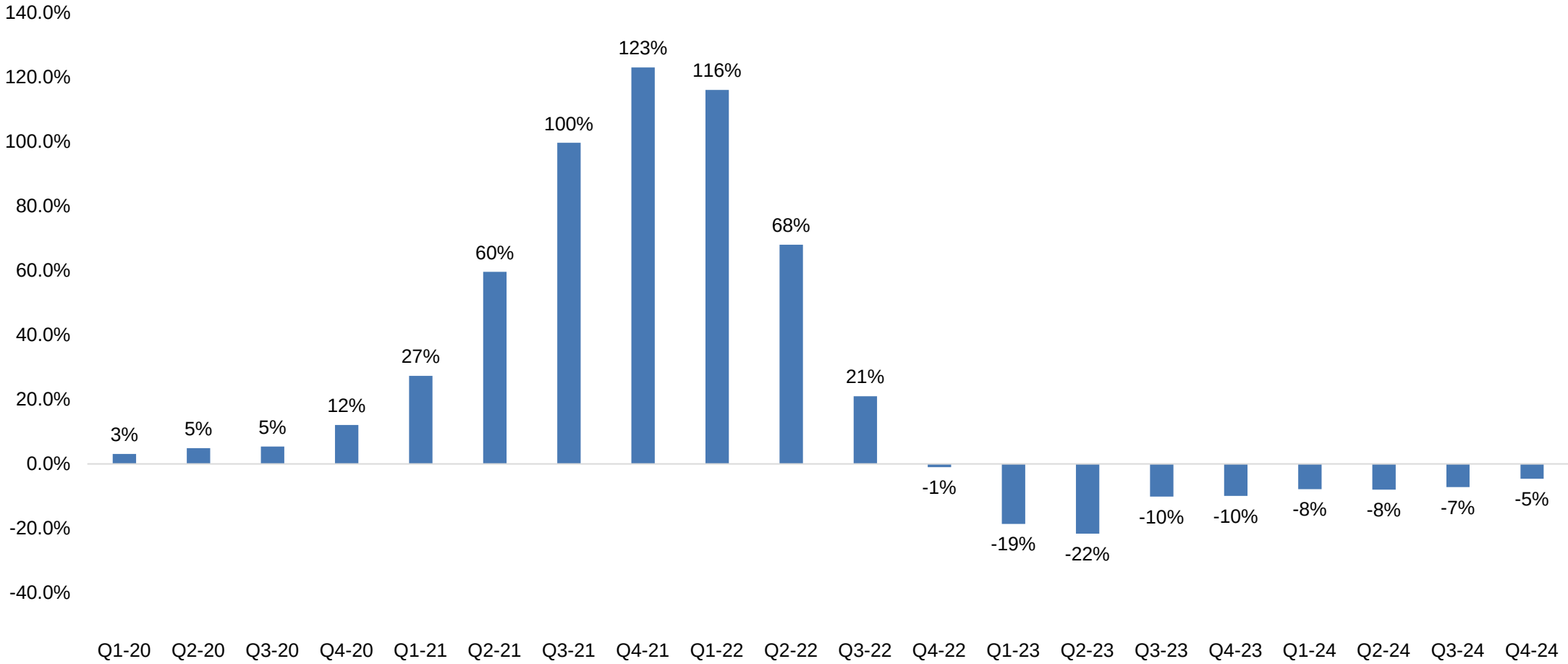
Cumulative Ransomware Frequency Growth by Month



Source: Risk Based Security, analysis by Aon. Data as of 3/1/2025; Claim count development may cause these percentages to change over time

How Are Market Rates Trending?

2020–2024 Cyber Premium Changes by Quarter
Average year-over-year change (same clients)

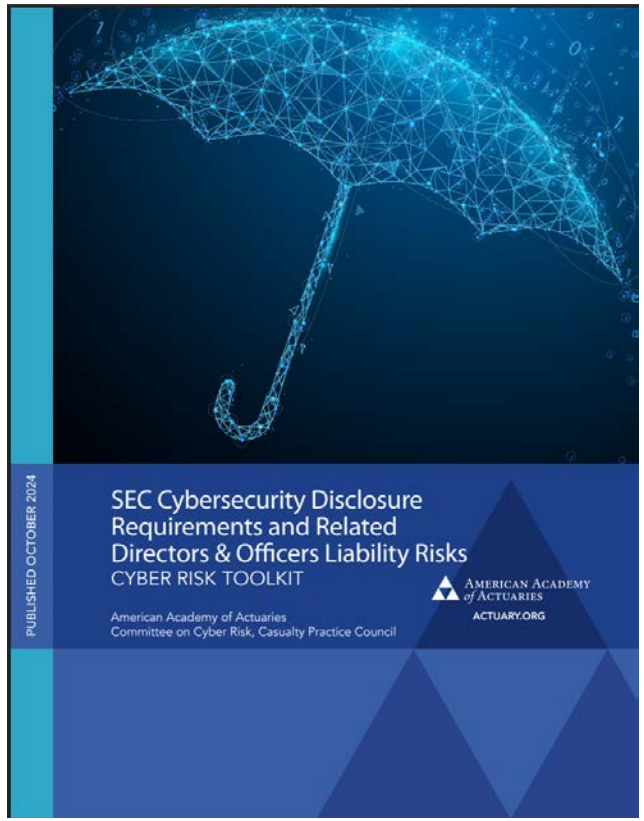


Source: Aon's E&O and Cyber Market Review – Q1 2025

SEC Disclosures and Related Matters

SEC Cybersecurity Disclosure Requirements and Related Directors & Officers Liability Risks

https://www.actuary.org/sites/default/files/2024-10/Casualty-Brief-SEC-Cyber.pdf



SEC 8-K Disclosure Laws

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure rule

Effective: 12/18/2023

*The registrant must file the Item 1.05 Form 8-K within **four** business days of its determination that the incident is **material**.*

sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214

SEC 8-K Example Disclosure—UnitedHealth Group

Item 1.05. Material Cybersecurity Incidents.

On February 21, 2024, UnitedHealth Group (the "Company") identified a suspected nation-state associated cyber security threat actor had gained access to some of the Change Healthcare information technology systems. Immediately upon detection of this outside threat, the Company proactively isolated the impacted systems from other connecting systems in the interest of protecting our partners and patients, to contain, assess and remediate the incident.

The Company is working diligently to restore those systems and resume normal operations as soon as possible, but cannot estimate the duration or extent of the disruption at this time. The Company has retained leading security experts, is working with law enforcement and notified customers, clients and certain government agencies. At this time, the Company believes the network interruption is specific to Change Healthcare systems, and all other systems across the Company are operational.

During the disruption, certain networks and transactional services may not be accessible. The Company is providing updates on the incident at https://status.changehealthcare.com/incidents/hqpjz25fn3n7. Please access that site for further information.

As of the date of this report, the Company has not determined the incident is reasonably likely to materially impact the Company's financial condition or results of operations.

https://www.sec.gov/ix?doc=/Archives/edgar/data/0000731766/000073176624000045/unh-20240221.htm

SEC 8-K Example Disclosure—Sonic Automotive

Item 1.05. Material Cybersecurity Incidents.

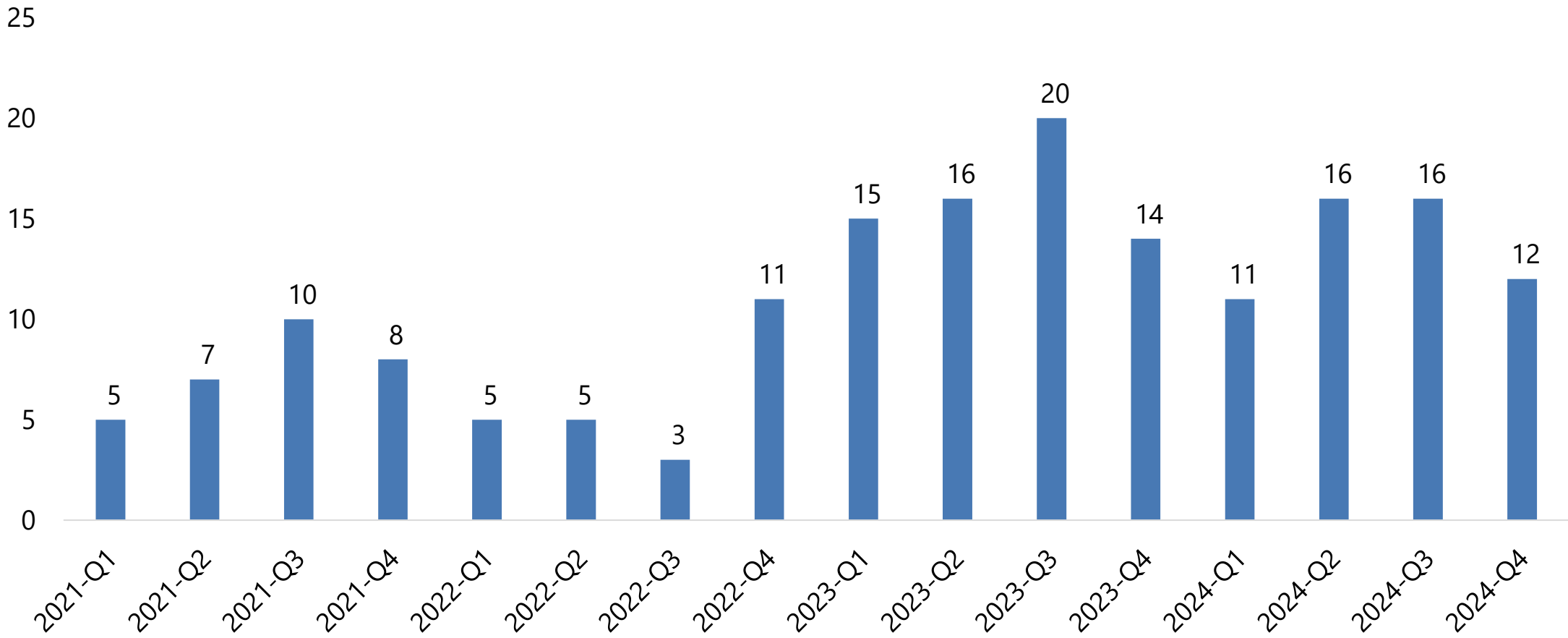
As previously disclosed in the Original Form 8-K, the Company has experienced disruptions in its access to certain information systems provided to the Company by CDK Global ("CDK") due to a cybersecurity incident experienced by CDK on June 19, 2024 (the "Incident"). As of the date of this filing, access to the Company's information systems affected by the Incident has been restored, including its dealer management system ("DMS") and customer relationship management system ("CRM"). However, the Company experienced operational disruptions throughout July related to the functionality of certain CDK customer lead applications, inventory management applications and related third-party application integrations with CDK.

The Company has concluded that the Incident had a material impact on the Company's business during and results of operations for the second fiscal quarter ended June 30, 2024 ("Q2"). The Company's GAAP earnings per diluted share for Q2 were $1.18, and the Company estimates that the Incident adversely affected its GAAP earnings per diluted share for Q2 by approximately $0.64 without taking into account any potential recoveries related to the Incident and after factoring in estimated lost income and expenses attributable to the Incident.

Based on the information available to the Company on the date hereof, the Company has concluded that the Incident is not reasonably likely to have a material impact on the Company's financial condition or its current or future business or results of operations, except as disclosed herein.

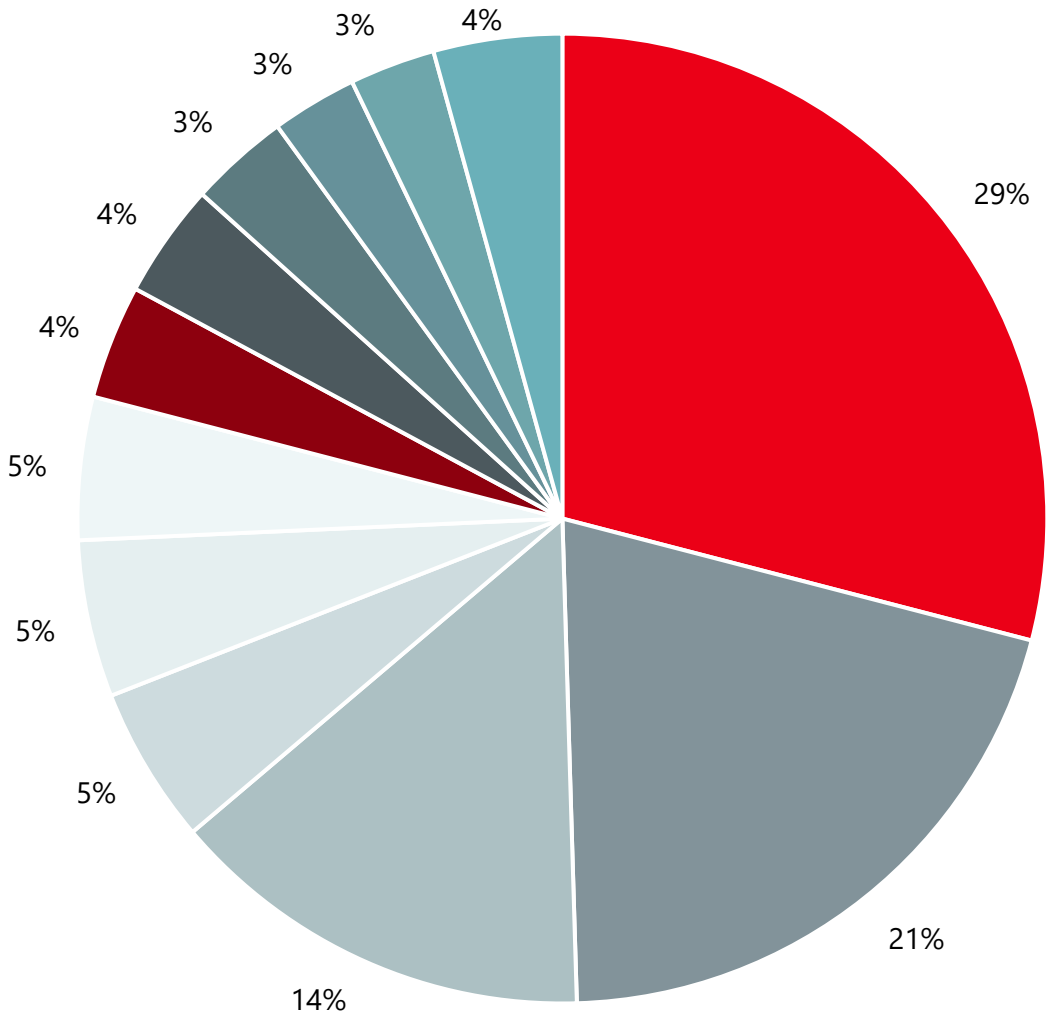
https://www.sec.gov/ix?doc=/Archives/edgar/data/0001043509/000104350924000063/sah-20240705.htm

SEC 8-K Reporting by Quarter



Source: SEC Edgar and S&P Capital IQ, analysis by Aon. Data as of 12/31/2024

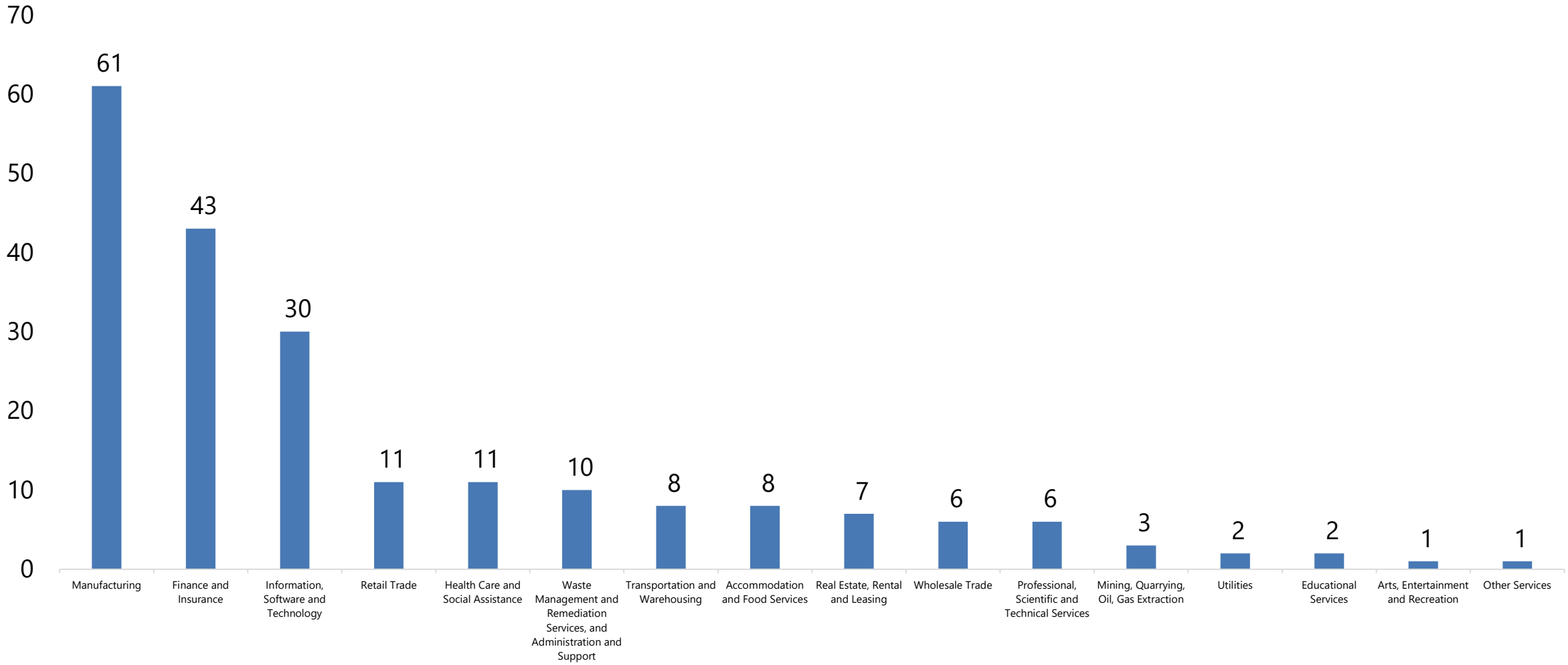
SEC 8-K Reporting of Cyber Incidents by Industry



- Manufacturing
- Finance and Insurance
- Information, Software and Technology
- Retail Trade
- Health Care and Social Assistance
- Waste Management and Remediation Services, and Administration and Support
- Transportation and Warehousing
- Accommodation and Food Services
- Real Estate, Rental and Leasing
- Wholesale Trade
- Professional, Scientific and Technical Services
- All Other

Source: SEC Edgar and S&P Capital IQ, analysis by Aon. Data as of 12/31/2024

SEC 8-K Reporting of Cyber Incidents by Industry



Source: SEC Edgar and S&P Capital IQ, analysis by Aon. Data as of 12/31/2024

SEC 10-K Disclosure Laws

New Item 106-Cybersecurity Risk Management and Governance

For the 10-K disclosures, disclosures will be due with annual reports for fiscal years ending on or after December 15, 2023.

Item 106 and Item 16K require registrants to describe their processes, if any, for **assessing, identifying, and managing material risks from cybersecurity threats,** as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect them. The new rules include a non-exclusive list of disclosure items registrants should provide based on their facts and circumstances.

sec.gov/corpfin/secg-cybersecurity

How is this relevant to actuaries?

1. Timely information as well as greater transparency into cybersecurity risks
2. Potential financial risks toward organizations (both as the insurer and insured)

SEC Charges Four Companies With Misleading Cyber Disclosures

One company, Unisys Corp., also charged with controls violations

FOR IMMEDIATE RELEASE | 2024-174

Washington D.C., Oct. 22, 2024 —The Securities and Exchange Commission today charged four current and former public companies – Unisys Corp., Avaya Holdings Corp., Check Point Software Technologies Ltd, and Mimecast Limited – with making materially misleading disclosures regarding cybersecurity risks and intrusions. The SEC also charged Unisys with disclosure controls and procedures violations. The companies agreed to pay the following civil penalties to settle the SEC's charges:

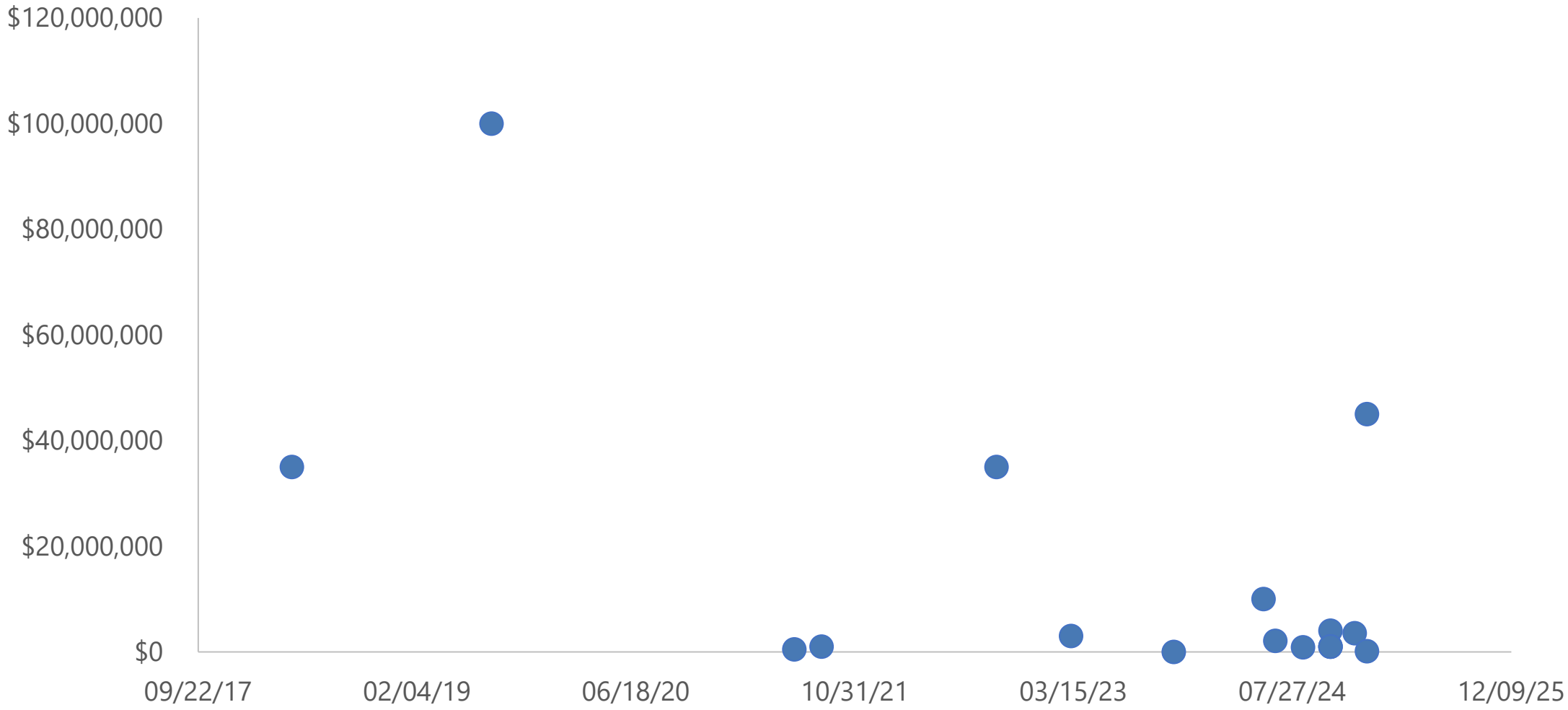
- Unisys will pay a $4 million civil penalty;
- Avaya. will pay a $1 million civil penalty;
- Check Point will pay a $995,000 civil penalty; and
- Mimecast will pay a $990,000 civil penalty.

sec.gov/newsroom/press-releases/2024-174

SEC Fines and Penalties

Entity	Reason	Date	Fine / Penalty / Settlement	Source
Altaba (Yahoo!)	Failure to Disclose	04/24/2018	$35,000,000	www.sec.gov/news/press-release/2018-71
Facebook	Misleading Disclosure	07/24/2019	$100,000,000	www.sec.gov/news/press-release/2019-140
First American Financial Corporation	Disclosure controls and procedures violations	06/15/2021	$487,616	www.sec.gov/news/press-release/2021-102
Pearson plc	Misleading Disclosure	08/16/2021	$1,000,000	www.sec.gov/news/press-release/2021-154
Morgan Stanley Smith Barney	Failures to Safeguard Personal Information	09/20/2022	$35,000,000	www.sec.gov/news/press-release/2022-168
Blackbaud	Misleading Disclosure	03/09/2023	$3,000,000	www.sec.gov/news/press-release/2023-48
SolarWinds Corporation	Internal Control Failures / Misleading Investors	10/30/2023	TBD	www.sec.gov/news/press-release/2023-227
R.R. Donnelley	Disclosure and Internal Control Failures	06/18/2024	$2,100,000	www.sec.gov/news/press-release/2024-75
Equiniti	Failure to protect client funds	08/20/2024	$850,000	www.sec.gov/newsroom/press-releases/2024-101
Unisys	Misleading Disclosure	10/22/2024	$4,000,000	www.sec.gov/newsroom/press-releases/2024-101
Avaya	Misleading Disclosure	10/22/2024	$1,000,000	www.sec.gov/newsroom/press-releases/2024-101
Check Point	Misleading Disclosure	10/22/2024	$995,000	www.sec.gov/newsroom/press-releases/2024-101
Mimecast	Misleading Disclosure	10/22/2024	$990,000	www.sec.gov/newsroom/press-releases/2024-101
Flagstar Bancorp	Misleading Disclosure	12/16/24	$3,550,000	https://www.sec.gov/enforcement-litigation/administrative-proceedings/33-11343-s
Ashford Inc.	Misleading Disclosure	01/13/25	$115,231	https://www.sec.gov/enforcement-litigation/litigation-releases/lr-26215
Robinhood	Internal controls, cybersecurity, and data	01/13/25	$45,000,000	https://www.sec.gov/newsroom/press-releases/2025-5

SEC Fines and Penalties Over Time



Notable Securities Class Action Settlements from Cybersecurity / Privacy Incidents

Entity	Loss Type	Approximate Settlement Date	Settlement	Source
Altaba (Yahoo!)	Securities Class Action	03/02/2018	$80,000,000	classifiedclassaction.com/wp-content/uploads/2018/03/In-re-Yahoo-Inc-Securities-Litigation.pdf
Altaba (Yahoo!)	Derivative Lawsuit	01/04/2019	$29,000,000	www.dandodiary.com/2019/01/articles/cyber-liability/yahoo-data-breach-related-derivative-suit-settled-29-million/
Equifax	Securities Class Action	02/13/2020	$149,000,000	www.dandodiary.com/wp-content/uploads/sites/893/2020/02/Equifax__Settlement_Stipulation.pdf
SolarWinds	Securities Class Action	11/28/2022	$26,000,000	www.solarwindssecuritieslitigation.com/
Google	Securities Class Action	02/06/2024	$350,000,000	www.reuters.com/legal/google-pay-350-million-revolve-shareholders-data-privacy-lawsuit-2024-02-06/
Okta	Securities Class Action	06/11/2024	$60,000,000	securities.stanford.edu/filings-documents/1079/OI00107949/2024611_r01x_22CV02990.pdf

An Overview of the Global Cyber Re/insurance Market

Isabelle McCullough, MAAA, ACAS
Member, Committee on Cyber Risk

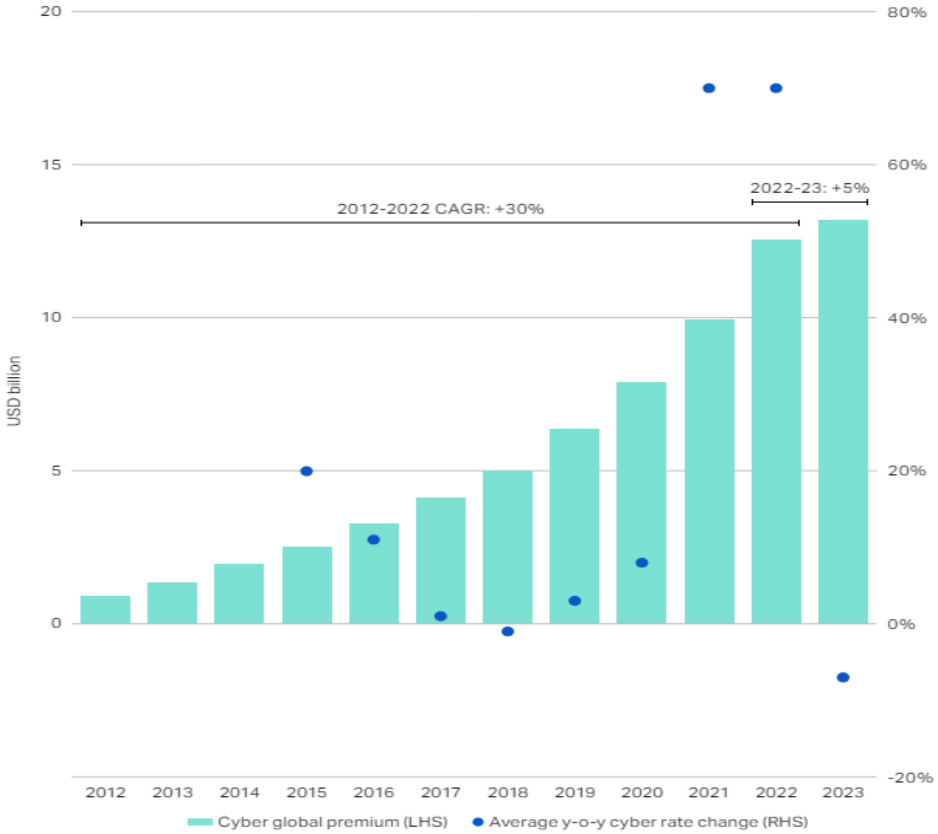
Global Market—Overview

Cyber Market—GWP & Historical Growth

- Est. **2024** global market size: **$14-15bn** USD GWP
- Est. annualized growth rate 2012-2022: **30%***
- 2022-2023 growth: **5%**
- **Exposure v. rate** growth: 2021/22 exposure decrease

*compares to overall P&C growth rate in the single digits over the same period

Source: Howden Re, 2024 Cyber Report https://www.howdengroupholdings.com/sites/default/files/2024-06/howden-2024-cyber-report.pdf



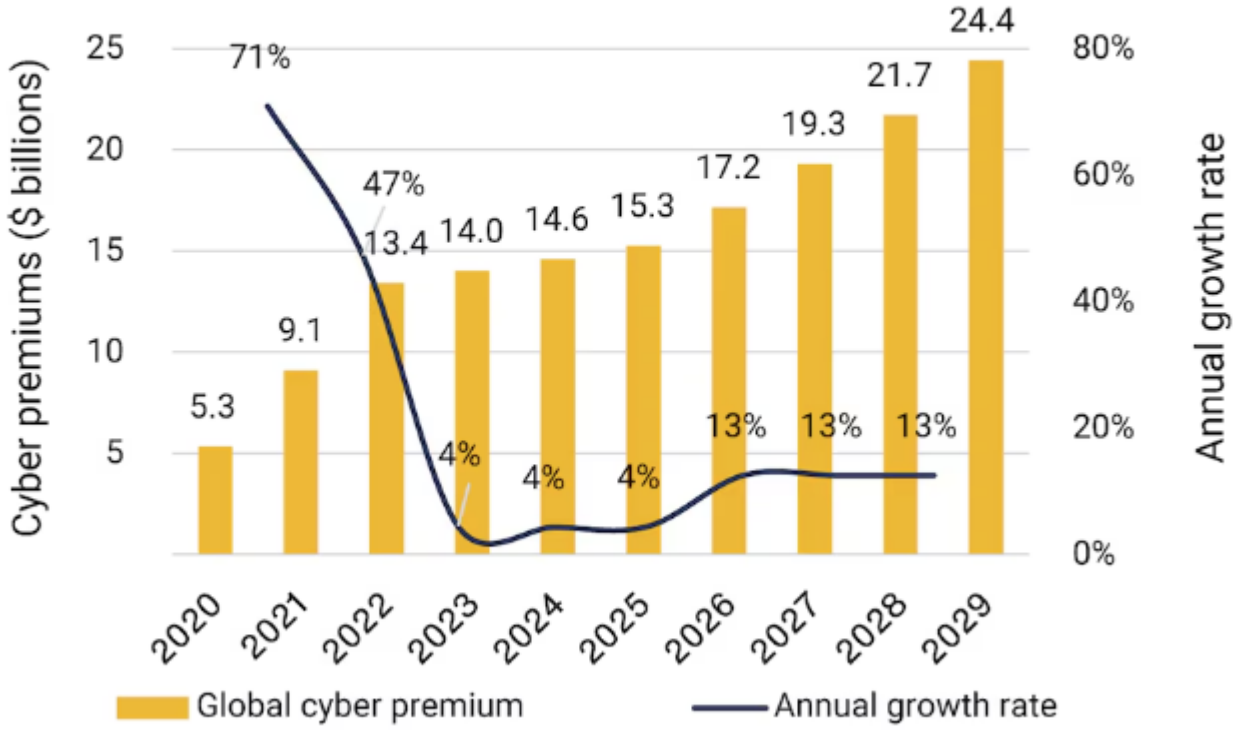
Cyber Market—Projected Future Growth

- Projections of future growth have been moderated from prior estimates due to **2023 & 2024 slowdown** in growth
- Market now expected to increase from approx. $14.6bn in 2024 to **over $24bn in 2029**
- *Note: estimates vary by source due to uncertainty in future growth rates*

Source: Aon

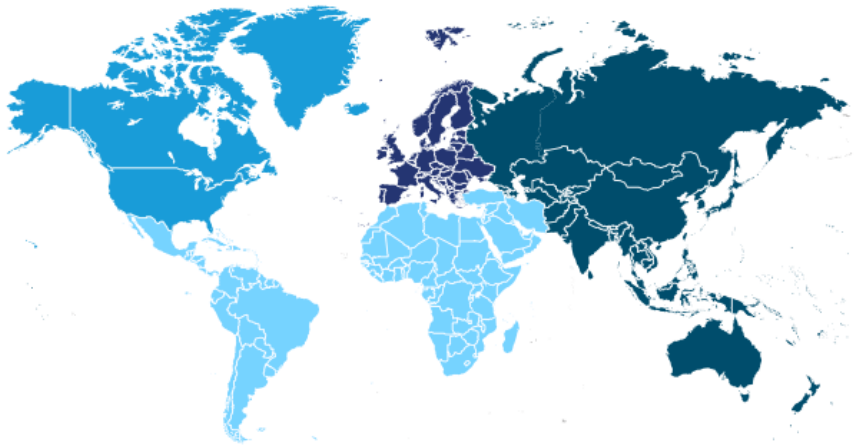
Global cyber insurance premium projection (Aon)

12.5% CAGR is expected, from 2026

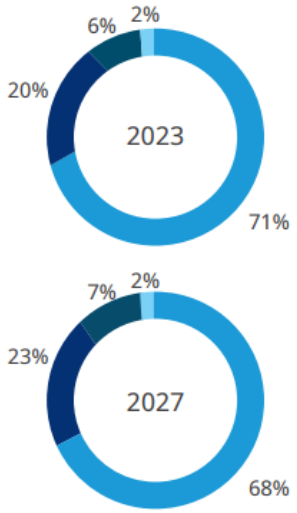


Source: Aon

Cyber Market—Regional Size



Regional percentage of global GWP



Regional GWP in USD billions	2019	2023	2025	2027
North America	4.4	10.1	13.5	19.7
Europe	0.9	2.8	4.3	6.6
Asia/Oceania	0.4	0.9	1.3	2.0
Rest of the world	0.2	0.3	0.5	0.7

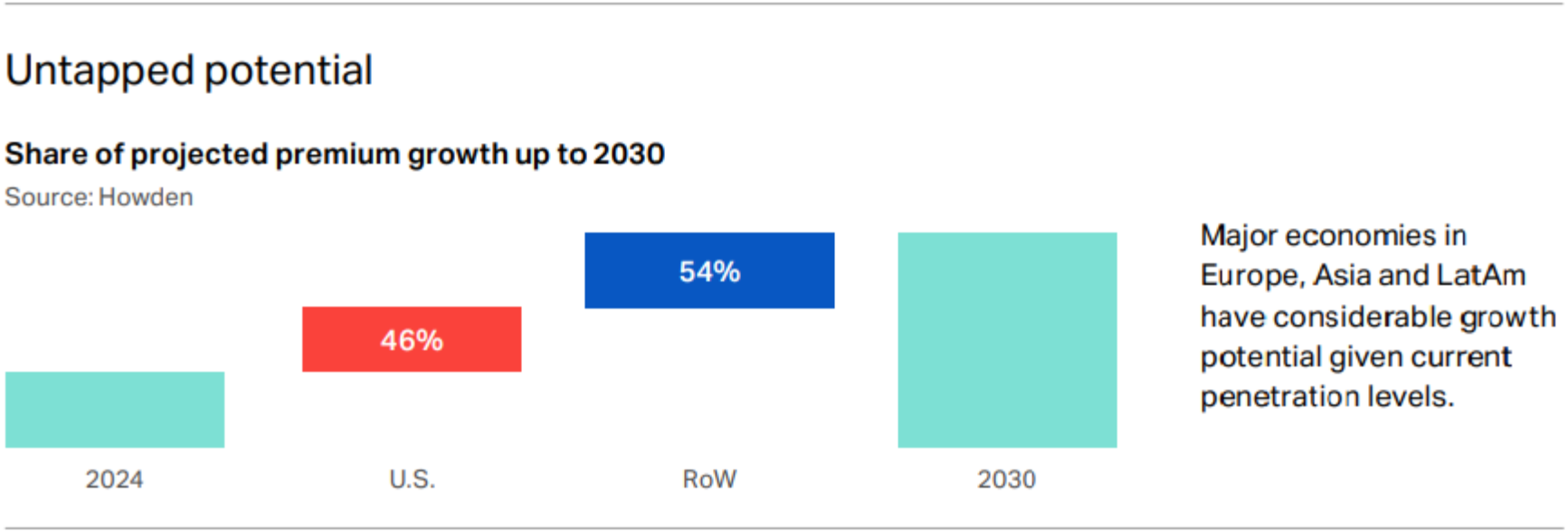
Source: Estimates by Munich Re

North America continues to be the largest market, followed by Europe.

Market expected to shift slightly away from North America by 2027 as Europe, Asia/Oceania markets outpace North American growth.

Source: "Closing the cyber risk protection gap", Zurich and Marsh McLennan, Sept 2024. https://www.zurich.com/media/news-releases/2024/2024-0905-01

Cyber Market—Regional Growth Projections



Source: Howden Re, 2024 Cyber Report https://www.howdengroupholdings.com/sites/default/files/2024-06/howden-2024-cyber-report.pdf

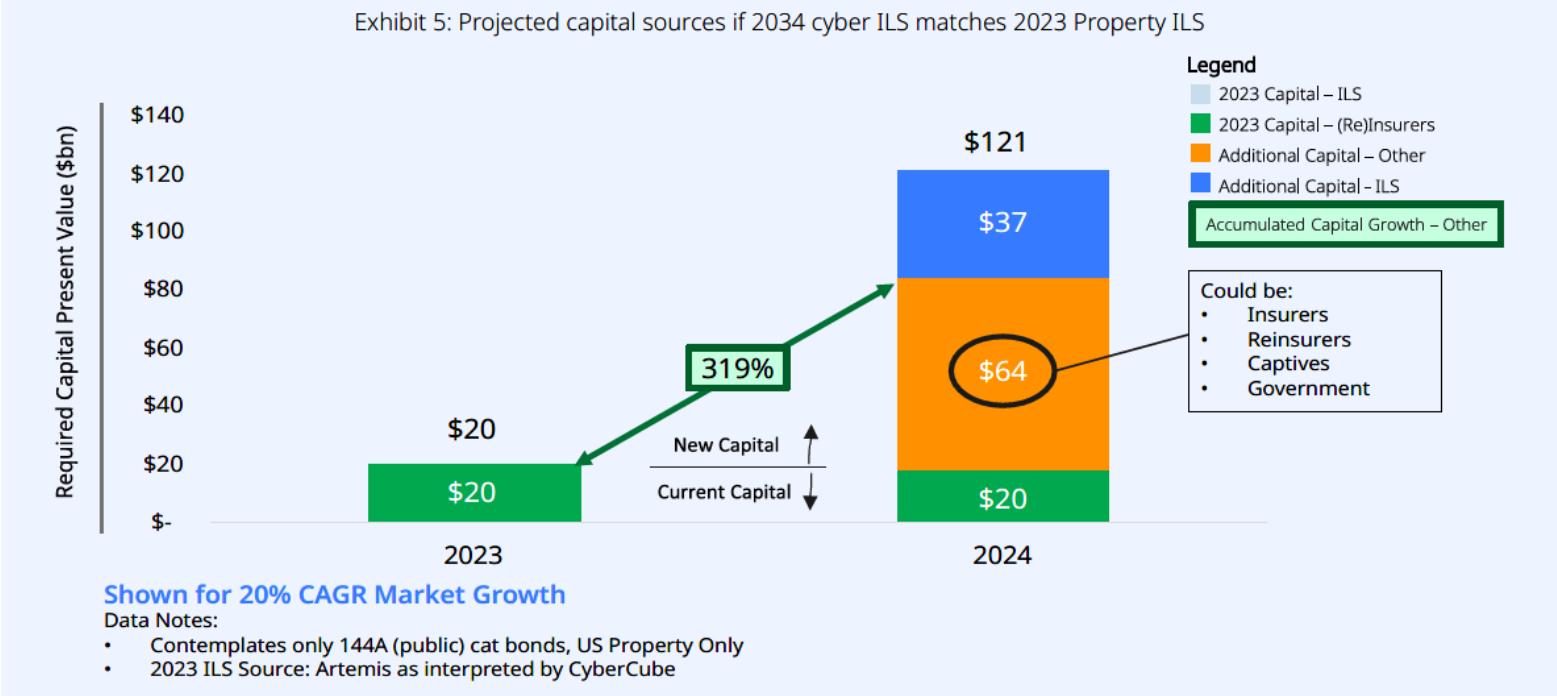
Cyber Market—Regional Growth Projections

Regional growth in cyber re/insurance markets have driven premium increases		
Gross premium written growth (%)		
	CAGR 2019-2023 (%) primary insurance	CAGR 2019-2023 (%) reinsurance
North America	35%	57%
Europe, Middle East, and Africa	35%	53%
Asia-Pacific	68%	69%
Latin America	88%	53%
Total	38%	56%
Data is based on our cyber insurance survey of global multiline insurers and large reinsurance groups. CAGR--Compound annual growth rate. Source: S&P Global Ratings.		

https://www.spglobal.com/ratings/en/research/articles/241127-cyber-insurance-market-outlook-2025-cycle-management-will-be-key-to-sustaining-profits-13323968

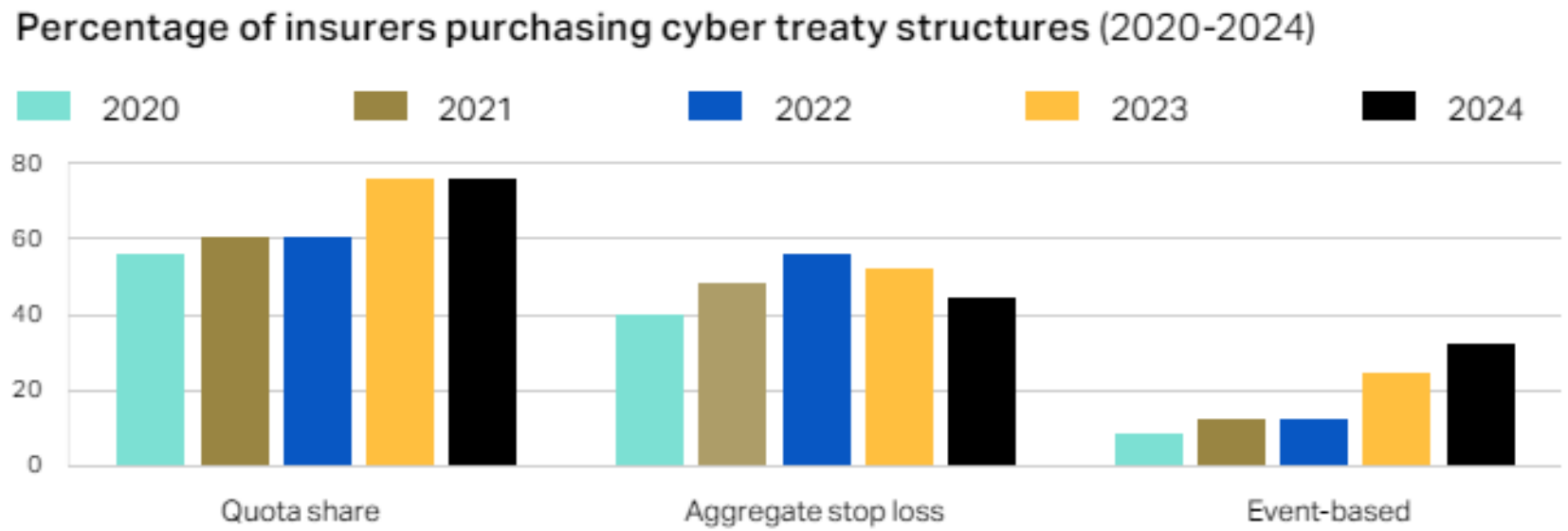
Cyber Market—Supporting Future Growth

- Growth highlighted on previous slides will not be based solely on price
- Increase in exposures will require additional capital
- Additional capital expected to be a mix of traditional (re)insurance, ILS capacity, public-private partnerships



https://insights.cybcube.com/projecting-cyber-insurance-growth-report

Cyber Market—Reinsurance



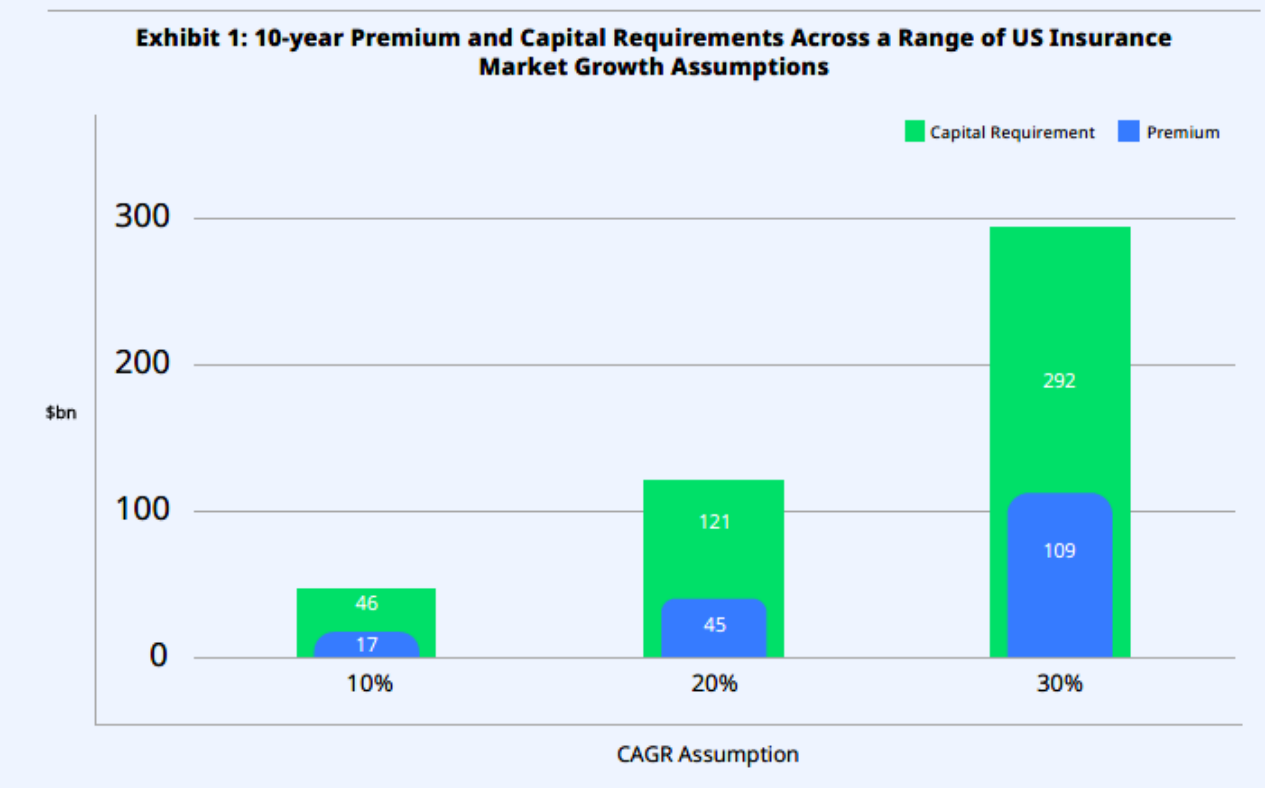
- Cessions are decreasing as primary carriers become more comfortable with their exposure
- Est. 35% premium ceded today, with less mature markets/geographies ceding a higher %
- Shift away from ASL structures to event-based cover expected to continue into 2025
- Estimated that carriers are ceding 56% of their CAT AAL while retaining 65% of their premiums

Source: Howden Re, https://howdenre.com/wp-content/uploads/2024/05/10503-Cyber-report-2024_v9_digital-FINAL.pdf

Cyber Market—Retro, Alternative Risk Transfer

- Retrocession capacity will be important to future market growth
- Limited retrocession capacity to date driven by accumulation and information-sharing concerns (same key players)
- In 2023, cat bonds benefitting Beazley, Chubb, AXIS Capital and Swiss Re were issued
- In 2024, Swiss Re purchased the market's first cyber retrocession industry loss warranty (ILW)
- Chance that private sector will not assume all tail risk, requiring public-private partnerships to develop

Sources:
https://www.artemis.bm/news/cyber-reinsurance-retro-ils-all-critical-to-market-expansion-sp/
https://www.artemis.bm/deal-directory/?_sft_perils=cyber-risks
https://www.reinsurancene.ws/swiss-re-purchases-cyber-markets-first-retrocession-ilw-brokered-by-gallagher-re/



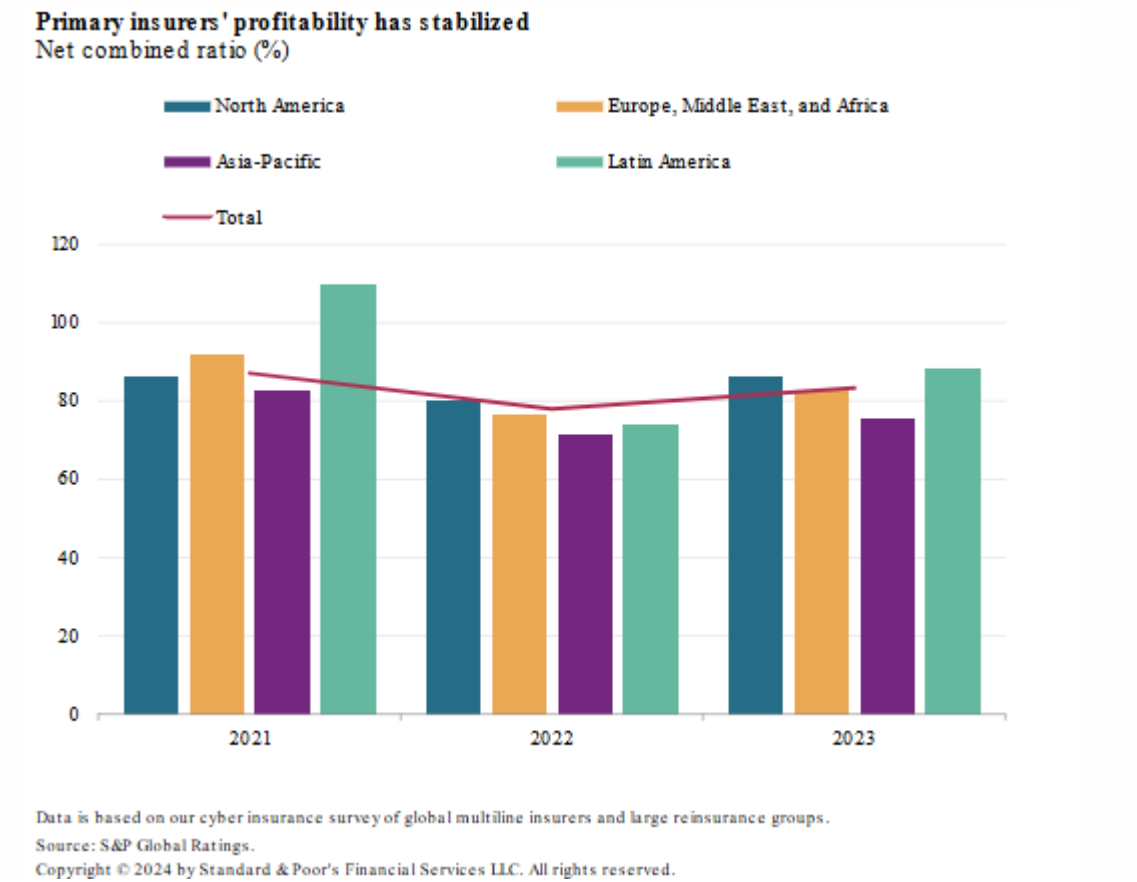
https://insights.cybcube.com/projecting-cyber-insurance-growth-report

Cyber Market—CAT Bonds

Issuer	Cedent	Risks / Perils covered	Size	Date
PoleStar Re Ltd. (Series 2024-3)	Beazley	Cyber risks	$210m	Sep 2024
PoleStar Re Ltd. (Series 2024-2)	Beazley	Cyber risks	$160m	May 2024
Cumulus Re (Series 2024-1)	Hannover Re	Cloud outage	$13.75m	Apr 2024
East Lane Re VII Ltd. (Series 2024-1)	Chubb	Cyber risks	$150m	Dec 2023
Matterhorn Re Ltd. (Series 2023-1)	Swiss Re	Cyber risks	$50m	Dec 2023
PoleStar Re Ltd. (Series 2024-1)	Beazley	Cyber risks	$140m	Dec 2023
Long Walk Reinsurance Ltd. (Series 2024-1)	AXIS Capital	Cyber risks	$75m	Nov 2023
Beazley cyber cat bond (Cairney III)	Beazley	Cyber risks	$16.5m	Sep 2023
Beazley cyber cat bond (Cairney II)	Beazley	Cyber risks	$20m	May 2023
Beazley cyber cat bond (Cairney)	Beazley	Cyber risks	$45m	Jan 2023

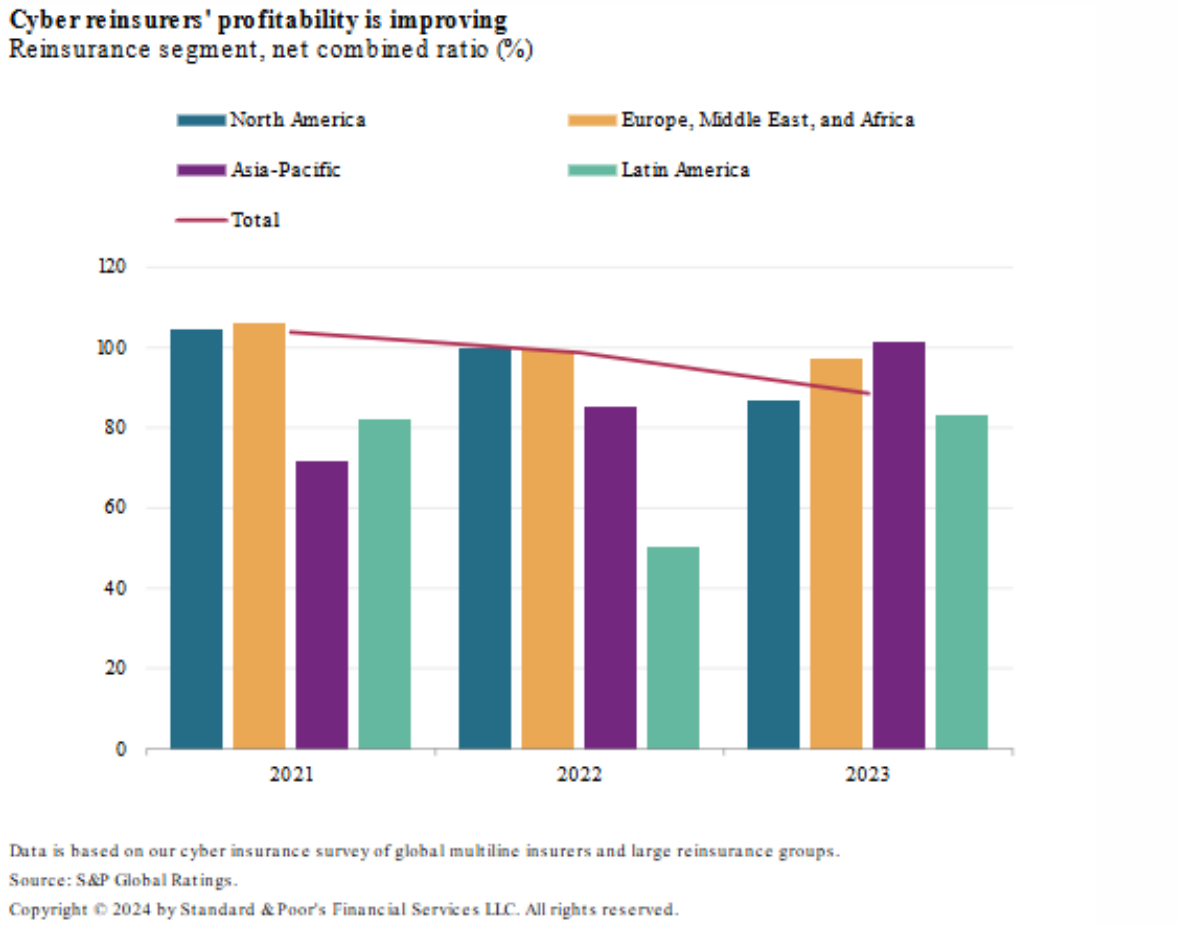
Source: https://www.artemis.bm/deal-directory/?_sft_perils=cyber-risks

Cyber Market—Insurance Profitability



- Stabilizing profitability in the primary space, though market conditions are soft currently
- Underwriting actions contributing to improved loss ratios:
  - Enhanced risk-selection and claims management
  - Tightening of terms and conditions in 2021-2022

Cyber Market—Reinsurance Profitability



- Results over this time worse than primary insurance segment
- Reinsurance results improved over 2021-2023 due to strict underwriting and higher rate adjustments
- Increased demand for excess-of-loss treaties, event-based structures
- Softer market conditions at 1/1/2025 renewals:
  - Proportional ceding commissions up more than 1 pt on average from 1/1/2024
  - Rate reductions up to 20% (risk-adjusted) in the non-proportional market
  - Entrance of nine new reinsurers, adding around $250m in capacity
  - 2024 events (Change Healthcare, Crowdstrike) had little impact on renewal terms

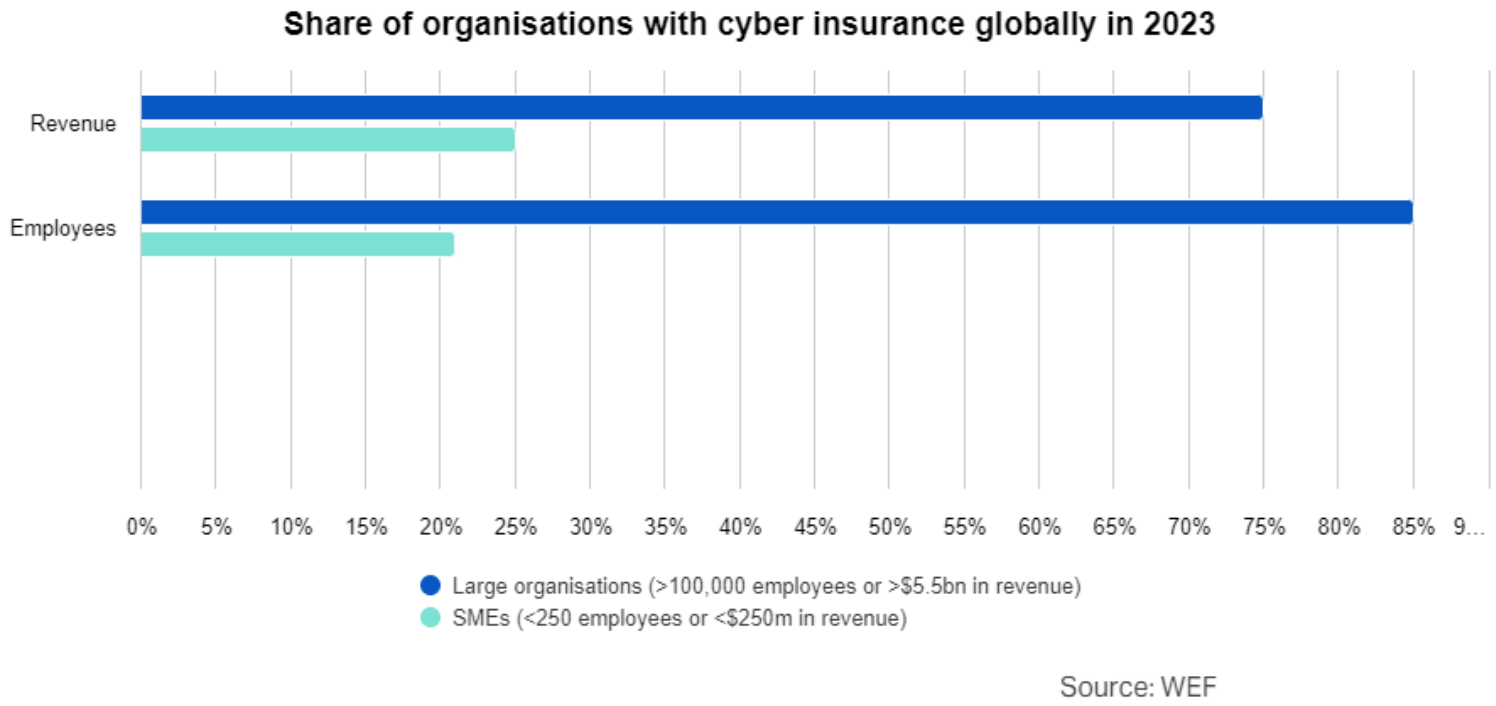
Cyber reinsurance market increasingly mature and efficient: Howden - Reinsurance News

Cyber Market—Products, Coverages

- Coverages are becoming standardized but still differ by geography
- Major coverage differences re: ransomware payments, business interruption coverage/sublimits
- For example, some geographies have regulations prohibiting insuring the payment of ransoms
- Some regions have more add-on cyber (endorsements on BOP, PL, etc.) v. standalone. Add-on/bolt-on business may be lighter in coverage, limit

Cyber Market—Adoption Rates

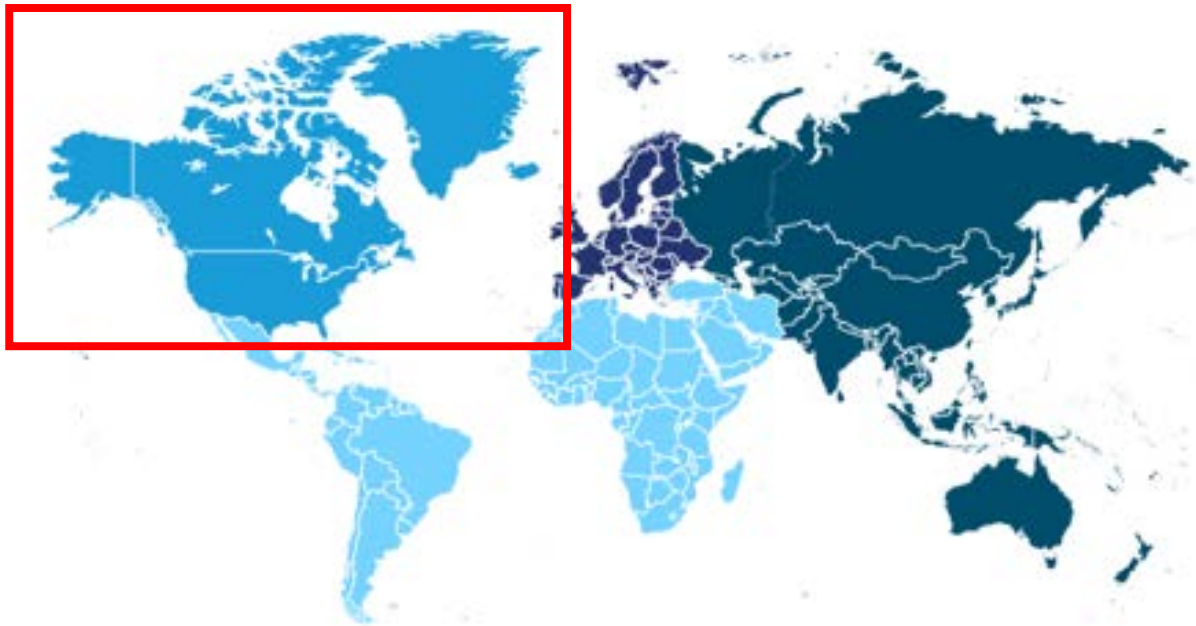
- Adoption rates in education, government entities, financial services and energy industry sectors are the highest across the world
- Small business adoption rates are consistently lower than large corporat rates.
- Approx. 1 in 4 small businesses carried cyber insurance v. 3 in 4 large businesses in 2023



Source: https://www.howdengroupholdings.com/reports/2024-cyber-report

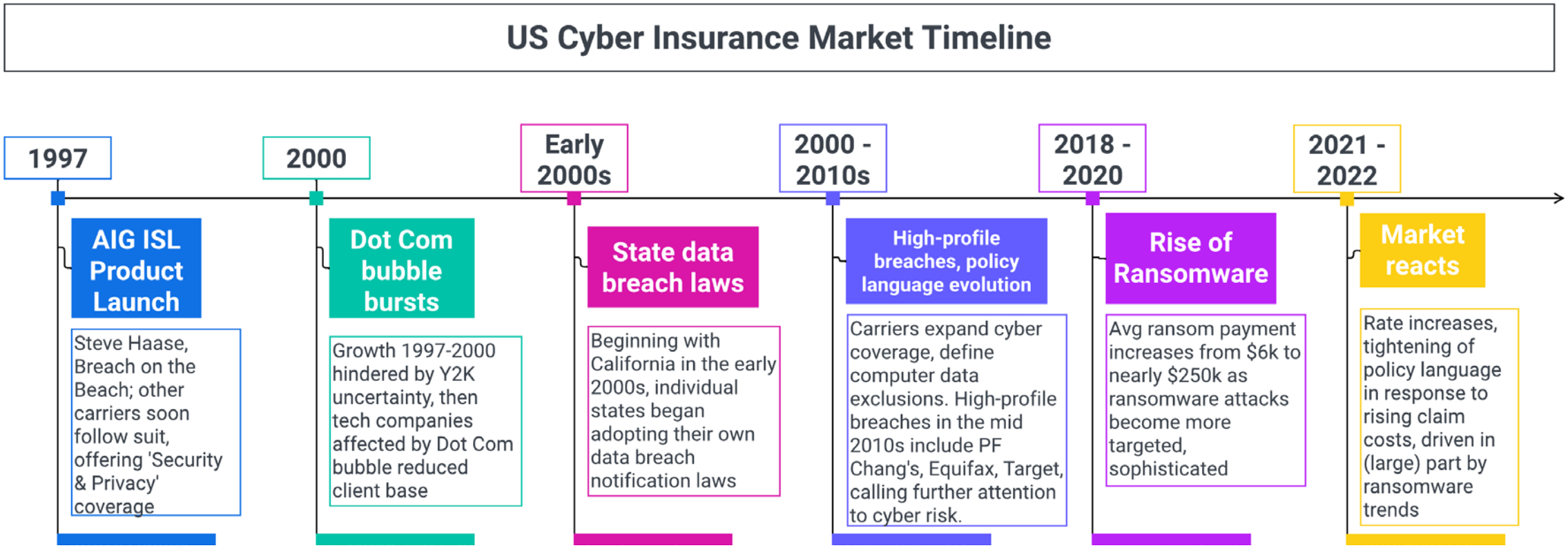
Global Market—Regional Insights

Cyber Market—North America (U.S. & Canada)



- Leading market with more than 50% of the global GWP
- US market has existed since Security & Privacy coverage was introduced in the mid 1990s
- Just under half of the growth through 2030 is expected to come from North America

Cyber Market – US History



https://slate.com/technology/2022/08/cyberinsurance-history-regulation.html
https://www.itgovernanceusa.com/data-breach-notification-laws
https://prowritersins.com/cyber-insurance-blog/history-cyber-insurance/#:~:text=In%20the%20early%202000s%2C%20online,Wild%20Viruses
https://www.korurm.com/blog/an-abbreviated-history-of-cyber-insurance---the-first-25-years
https://www.aon.com/inpoint/bin/pdfs/white-papers/Cyber.pdf
https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/behind-the-rise-of-ransomware/

Cyber Market—U.S. Today

- GWP estimates nearly $10bn USD
- Approx. 70% of GWP from standalone policies
- Almost $3bn in GWP is from admitted business
- Competitive market conditions
  - Rates decreased in the mid-single digits in 2023 and 2024
  - Package business more concentrated than standalone
  - Remains to be seen if large 2024 events impact 2025 rates

Cyber Market—Canada

- Fast-growing market: $500m CAD GWP in 2023, up from under $25m CAD in 2015
- Increase in ransomware frequency and severity mirrored the US experience
- Subsequent rate increases, tightening of underwriting standards in 2021 – 2022 similar to the US
- Data breach notification laws that are currently in place were not passed until 2018
- Lloyd's continues to dominate the Canadian cyber insurance market, with more than 75% of the market share in 2022

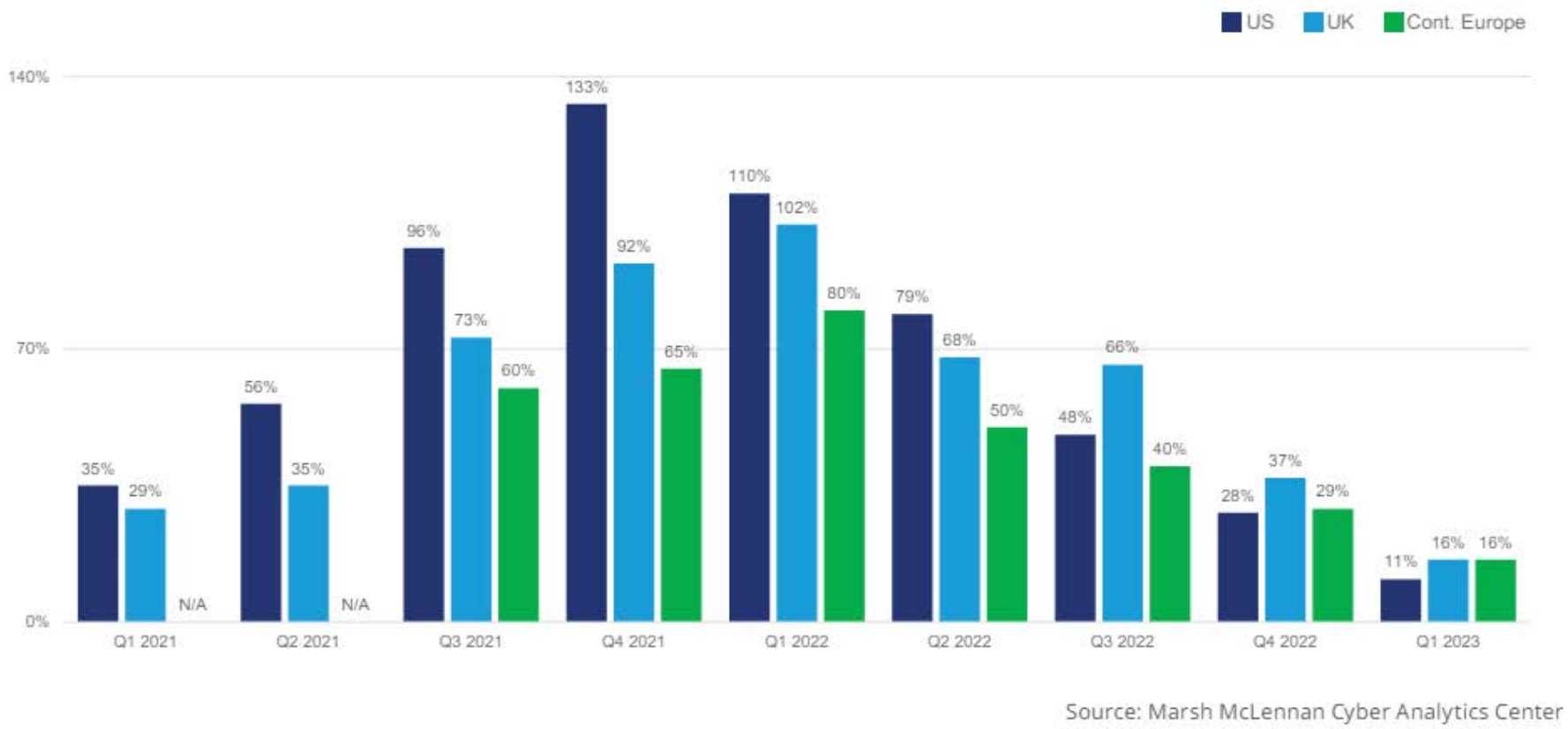
- https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Guy_Carpenter_Cyber_(Re)insurance_Market_Report_Publish_rev%20.pdf
- https://businessinsurancehelp.ca/wp-content/uploads/2023/10/The-Canadian-Cyber-Insurance-Market-Report-Sept-2023.pdf
- https://www.westlandinsurance.ca/news/the-growing-challenges-trends-in-the-cyber-liability-insurance-market/
- https://www.nortonrosefulbright.com/en/knowledge/publications/ac3ee5c4/mandatory-privacy-breach-reporting-requirements-coming-into-force-in-canada-november-1

Cyber Market—The UK & Continental Europe

- First cyber policy issued through Lloyd's was written in 1999, providing both first- and third-party coverage
- Today Lloyd's is a world-leading provider of cyber insurance
- The Lloyd's Market Association (LMA) war exclusions were market-leading
- Growth rates in the UK and other European markets have escalated in recent years, outpacing the US
- Germany and France are the two largest markets within continental Europe, comprising more than 8% of the global GWP between them
- Coverages in continental Europe are less standardized, targeted towards local industries than in North America or the UK

https://www.guycarp.com/insights/2014/10/historical-development-of-cyber-reinsurance.html
https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Guy_Carpenter_Cyber_(Re)insurance_Market_Report_Publish_rev%20.pdf
https://onlinelibrary.wiley.com/doi/full/10.1111/rmir.12261

Cyber Market—The UK & Continental Europe



Source: Marsh McLennan Cyber Analytics Center

Rate changes in the UK and Continental Europe have lagged those in the U.S. in recent years

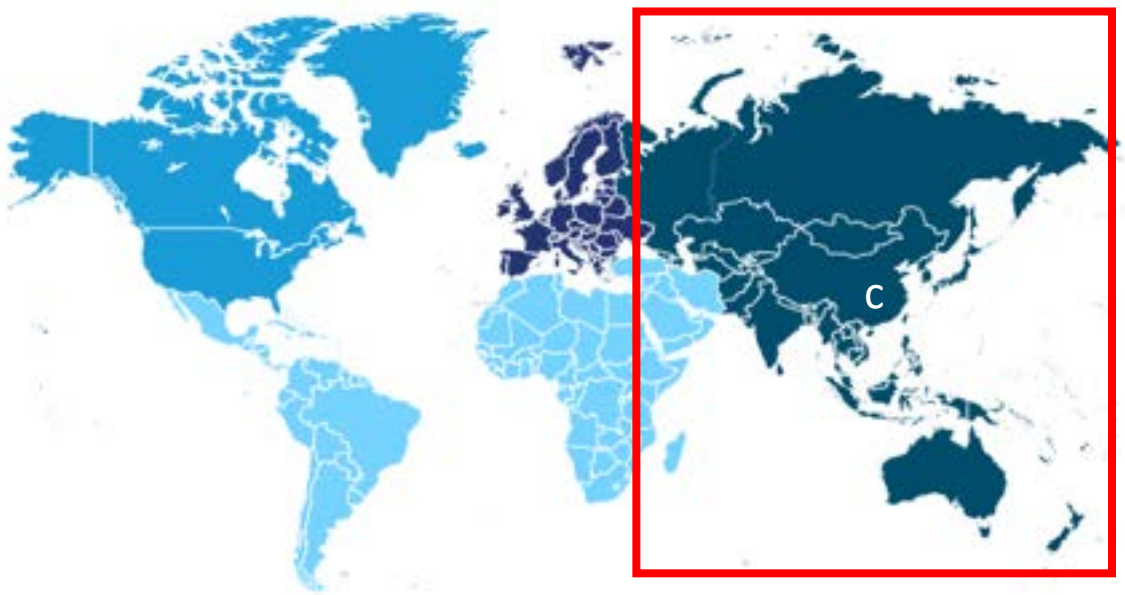
https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Guy_Carpenter_Cyber_(Re)insurance_Market_Report_Publish_rev%20.pdf

Cyber Market—The Middle East & Africa

- 2024 market size: approx. $283m USD
- Less than 2% of the global market
- New capacity in the market, but overall still limited
- Limited information available
- Security maturity in the region has historically been less advanced than the rest of the world, but geo-political tensions and a rise in cyber incidents drove an uptick in security maturity around 2022

https://www.cognitivemarketresearch.com/regional-analysis/middle-east-and-africa-cyber-insurance-market-report
https://www.marsh.com/ua/en/services/international-placement-services/insights/imea-insurance-rates-q1-2024.html
https://www.aon.com/2023-cyber-resilience-report//region/emea-building-resilience-to-navigate-rising-cyber-risk/

Cyber Market—APAC Overview



Overall, the APAC region is expected to have one of the highest rates of growth over the next 5 years, driven by increased regulation and recent cyber attacks.

Three main drivers of cyber risk in the region are geopolitical tensions, digital supply chain vulnerabilities and exfiltration of IP.

- https://www.peak-re.com/insights/a-primer-on-cyber-insurance-and-the-use-of-models/
- https://www.insurancebusinessmag.com/asia/news/cyber/cyber-insurance-market-set-to-surge-456802.aspx
- https://www.aon.com/2023-cyber-resilience-report//region/apac-regulators-and-companies-respond-as-ransomware-and-reputation-risks-intensify/

Cyber Market—APAC—Australia

- 2013: Emergence of cyber insurance in Australia, only a few policies written
- 2018: market has grown to about $40m USD GWP
- 2022: approx. $200m USD GWP
- Similar to other regions, the Australian cyber insurance market is becoming more competitive as new capacity enters the market & profitability improves. Rate change in 2023 was still positive, but down from 2022.
- Anticipated that Australia may follow the US's lead on a federal backstop for cyber CAT

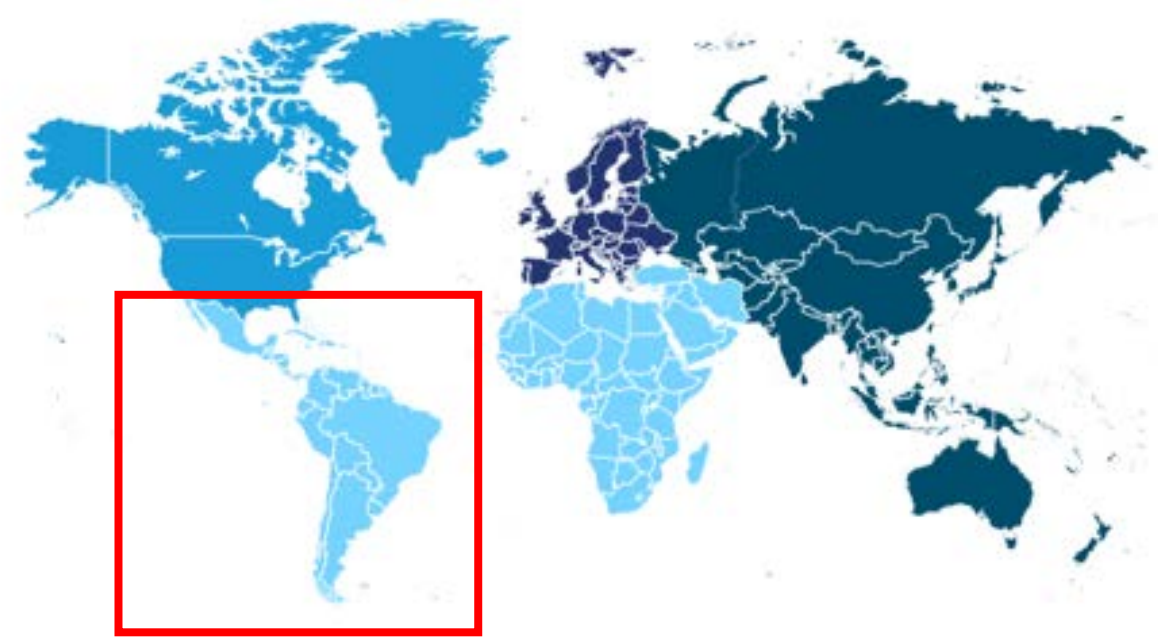
- https://aoninsights.com.au/cyber-insurance-market-insights-q3-2018/
- https://www.aicd.com.au/risk-management/framework/cyber-security/new-research-finds-gaps-in-australian-cyber-insurance.html
- https://insurancecouncil.com.au/issues-in-focus/cyber-risk/
- https://info.marsh.com/au-2023-mid-year-insurance-market-update

Cyber Market—APAC—Other

- Japan - larger market in the region, approx. $200m USD GWP in 2022. Low adoption rates compared to North America, Europe. Business interruption and ransom payments not commonly covered.
- China – Est. $30m USD GWP in 2022. Recent increase in standalone cyber coverage interest thought to be driven by uptick in ransomware, regulators encouraging the purchase of cyber insurance through industry associations.
- India – market size similar to China. Adoption rates thought to be increasing following high-profile breaches.
- Other – Southeast Asian market is still young, premium volume believed to be very low as of 2022. Coverage mostly offered as add-ons, though some businesses with US operations have purchased stand-alone coverage.

https://www.peak-re.com/en/knowledge-hub-insights/a-primer-on-cyber-insurance-and-the-use-of-models/

Cyber Market—LATAM



- One of the fastest growing cyber insurance markets globally
- General investment in cybersecurity on the rise, mirroring the growth in cyber insurance market
- Increased focus recently: NetDiligence
- Security maturity varies by country
- Example: Argentina, Brazil have active data protection regulation in place, while Chile has regulation only for some industries, like financial institutions

https://netdiligence.com/conferences/cyber-risk-summit-miami-2024/agenda
https://www.lexology.com/library/detail.aspx?g=a43e4f2a-0b9c-410d-9238-e9c70d28bc0b
https://www.aon.com/2023-cyber-resilience-report//region/latin-america-three-crucial-at-risk-control-areas/

Cyber Modeling Use Cases

Katie Koch, MAAA, FCAS
Member, Committee on Cyber Risk

Predictive Modeling in P&C Insurance

- Techniques Used
  - Generalized Linear Models (GLMs)
  - Machine Learning Algorithms
  - Catastrophe Modeling
- Advantages in Underwriting and Ratemaking
  - Ranking Risks
  - Developing Risk Classification Relativities
- Limitations in Underwriting and Ratemaking
  - Data Quality / Reliance on 3rd Party Data Vendors
  - Regulatory Compliance

Cyber Modeling Techniques

- Techniques Used
  - Frequency-Severity Models
  - Scenario Analysis
  - Causal Modeling
- Advantages in Underwriting
  - Strengths in Identifying Blind Spots
- Limitations in Underwriting and Ratemaking
  - Accuracy
  - Assumptions

Comparison and Contrast (Traditional P&C vs. Cyber Models)

Similarities	Differences
Statistical and Mathematical Models	Use Cases
Catastrophic Events Modeled Separately	Data Sources and Data Availability
Aim to Predict and Mitigate Risk	Regulatory Environment

Cyber Risk Committee Cyber Model Paper

Key Insights

- Overview of eight Cyber Risk model vendor approach and use cases
- Limitations of traditional frequency-severity models
- Data source exploration activity
- A snapshot in time of cyber risk modeling (≈ 2022)
- Appreciation for the progress and complexities

Questions and Answers

Thank You

For more information, please contact

Rob Fischer, Policy Project Manager, Casualty

fischer@actuary.org