



IBA Formum BsAs

Cyber Liability
Benchmarking and Trending
Discussion

May 2023

- 1. What are the main requirements that companies or law firms need to comply with to obtain cyber insurance? How to calculate the correct amount for the coverage?**



Cyber Key Controls

Marketplace Minimum Expectations



Token Based
Multi-factor Authentication
(MFA)



Vulnerability Scanning &
Patch Management



Endpoint Protection &
Response (EDR)



E-mail Filtering & Security
(DMARC/DKIM)



Social Engineering Exercises
&
Awareness Training



Supply Chain Risk
Management



Identity, Access, and
Privileged Access
Management



Network Segmentation:
Secure RDP, VPN, OT/IT



Disaster Recovery Testing,
BCP, & Backups



Incident Response Plan
(Written & Tested)



M&A Due Diligence
& Integration

Many insurers have been conducting **non-invasive vulnerability scans** on insured's to proactively **flag any vulnerabilities** that are found. These scans will be looking for issues related to RPC (Remote Procedure Call), VNC (Virtual Network Computing), SMB (Server Message Block), and RDP (Remote Desktop).

Key Underwriting Concerns & Best Practices

Critical Controls aligned with Cyber Insurance:	Key Guidance:
MFA / Controlled Access	MFA should be required for all privileged and administrative accounts , remote/VPN/Remote Desktop/cloud access, access to backups.
Endpoint Detection and Response	Effective EDR tools should be installed across all assets and on 7x24x365 basis and monitored by reputable vendors/MSSPs.
Secured and Tested Backups	Backups of critical systems should be in place and tested regularly . Recovery from backup should be tested often and at least annually . Copy of backup should be stored off network or in immutable storage. Full Physical Recovery should be tested as well to ensure Recovery Time Objectives are achievable.
Patched Systems & Applications	A formalized process and policy for patching all endpoints, servers, systems with the ability to document process compliance and patching levels – especially important for critical patches.
Filtered Emails and Web Content	Spam filtering should be deployed on all email systems (MS-Advanced Threat Detection). Secure web access gateways for web filtering need to be implemented.
Protected Privileged Accounts	A Password Asset Management (PAM) solution should be in place in order to manage privileged account passwords and MSLAPs or PAM is used on all endpoints to manage local admin passwords, local admin rights removed.
Logged and Monitored Network	Logging of the entire network, server, cloud and endpoint should be in place with logs managed daily . SOC for monitoring of all log files should be implemented as well.
Encrypted Storage	PCs, server storage and cloud storage are encrypted .
Phishing Aware Workforce	Annual phishing training and phishing simulation campaigns conducted.
Managed Vulnerability and Penetration Testing	At minimum, annual penetration tests and vulnerability scans conducted across the entire network with follow up to close identified issues .
Prepared Incident Response	Formalized IR plan created with identified key internal stakeholders and vendors . Should be coordinated with Cyber Insurance Program.
Other Critical Controls	CISO on staff or on demand, minimize Service Accounts with Domain Privileges.
Business Continuity and Controls of Vendors	Must have in place a reviewed and tested Continuity Plan that includes supply chain vendors and contingencies in place for replacement.
Log4j / Log4Shell	All insurers are releasing their own set of questions to determine exposure and response around this widespread event.

What is the correct / proper amount of Cyber Coverage

- Cyber risk disclosures have become part of **corporate financial reporting**, yet application of **sophisticated risk modeling to evaluate and quantify cybersecurity exposures** has not enjoyed the same sophisticated approach as employed for more traditional business risks.
- The **cyber threat to the balance sheet** is real.
- Better **predictive data**, that determines **commercial consequences** of a cyber event, is needed to provide management clarity on how to either **mitigate, self-fund or transfer** cyber risk to insurance companies.
- Develop **key risk scenarios** that understand your unique **business model, technology profile, industry environment and event history** to deliver a highly tailored view of your cyber exposures. Model losses arising from those scenarios, **as well as an insurance policy response**, delivering a thoughtful analysis with insights to improve investment allocation and balance sheet protection.

Three Key Scenarios:

1. Disclosure of Personally Identifiable Information Data:

Scenario: Scenario 1 overview and details here

Description: Detailed description of scenario 1 here

2. Malware Impacting Corporate Systems:

Scenario: Scenario 2 overview and details here

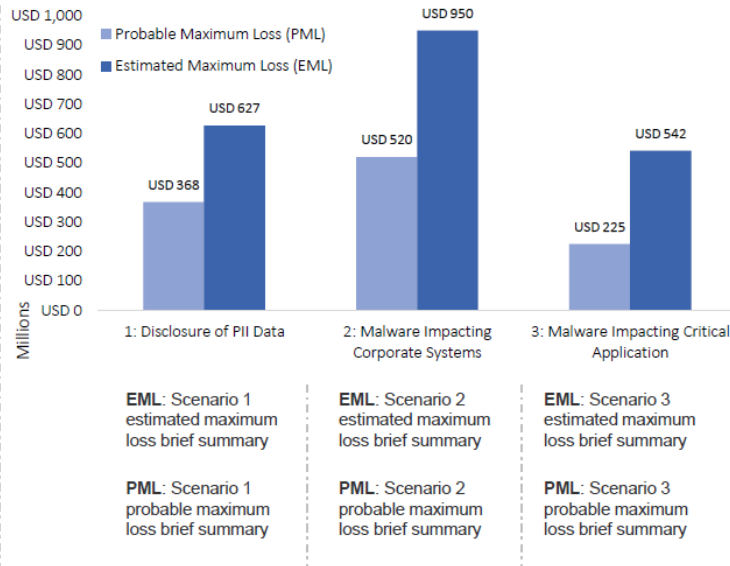
Description: Detailed description of scenario 2 here

3. Malware Impacting Critical Application:

Scenario: Scenario 3 overview and details here

Description: Detailed description of scenario 3 here

Key Results:



Scenario	Business Interruption	Extra Expense	Incident Response	Legal Expense / Public Relations	3 rd Party Liability	Attorney General Settlement*	CCPA*	Estimated Loss Total
Scenario 1: Disclosure of Personally Identifiable Information Data	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M
	BI / System Failure \$z M	Extra Expense \$z M	Privacy Event \$z M	Privacy Event \$z M	Privacy Liability \$z M	Privacy Regulatory \$z M	Privacy Regulatory \$z M	Total Limit \$z M
Scenario 2: Malware Impacting Corporate Systems	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M
	BI / System Failure \$z M	Extra Expense \$z M	Privacy Event \$z M	Privacy Event \$z M	Privacy Liability \$z M	Privacy Regulatory \$z M	Privacy Regulatory \$z M	Total Limit \$z M
Scenario 3: Malware Impacting Critical Application	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M	EML \$x M PML \$x M
	BI / System Failure \$z M	Extra Expense \$z M	Privacy Event \$z M	Privacy Event \$z M	Privacy Liability \$z M	Privacy Regulatory \$z M	Privacy Regulatory \$z M	Total Limit \$z M

Insurability Coverage Key**:

- Insured
- Insufficient Limits
- No Coverage

*Where insurable by State Law / Jurisdiction

**Insurance coverage, wording, limits, sub-limits, terms, conditions, and strategy should be reviewed with insurance broker

2. **What are the do's and don'ts from an insurance perspective when dealing with an attack? What could cause companies to lose their coverage, even when they have one? What are the exclusions or limitations in insurance policies, and how can law firms and companies deal with them?**



Cyber Exposure Law Firms – Professional Services Firms

Law firms and other specialized consultancy firms are a target for cyber criminals with motives of financial gain via theft of confidential information or money. In an increasingly punitive legal and regulatory environment, and with more frequent contractual requirements for cyber liability insurance, forward thinking companies are taking proactive steps to explore and transfer cyber risk.

Cyber risk considerations for Law Firms and professional services organizations:

- ❖ Personally identifiable or corporate confidential information in their care
- ❖ Damage to reputation
- ❖ Interruption to business / prevention from operation
- ❖ Internal technology innovation
- ❖ Privacy regulations
- ❖ High dependency on electronic processes and computer networks
- ❖ Regulatory oversight resulting in fines and penalties
- ❖ Dependence on vendors, independent contractors or additional service providers

Potential cyber incidents for professional services organizations:

- ❖ Theft and potential release of personally identifiable or corporate confidential information in their care
- ❖ Malware preventing access to systems and causing interruption to business
- ❖ Social engineering
- ❖ Network disruption
- ❖ Insider access
- ❖ Cyber incident affecting a crucial outsourced service provider
- ❖ Intentional acts committed by rogue employees
- ❖ Ransomware attacks

AON Cyber Coverages & Exclusions

Third party coverage elements

- **Security and privacy:** defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or wrongful disclosure of confidential information, unauthorized access, denial of service attack or transmission of a computer virus.
- **Regulatory defense and fines:** defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and / or a failure of network security.
- **Media liability:** defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy.
- **PCI fines and assessments:** defense costs for investigations brought by the Payment Card Industry (PCI) in connection with a failure to protect private information and / or network security.

First party coverage elements

- **Breach response costs associated with:** breach notification, including the hiring of outside law firms and public relations consultants, forensic costs, credit monitoring / protection, notification hot-line / call center, identity theft resources.
- **Network business interruption:** loss of income and extra expense due to network security failure.
- **Dependent business interruption:** reimburses the insured for actual lost net income and extra expense incurred when the insured's service provider's computer system is interrupted / suspended due to a failure of network security.
- **System failure business interruption:** coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security.
- **Data restoration:** costs to restore / recreate data / software resulting from network security failure.
- **Cyber extortion:** reimburses the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat.

Standard Exclusions on cyber policies:

- Insured versus Insured
- Competition – Trade Laws - Taxes
- Electronic Communications (Carve back)
- Conduct Exclusion
- Contamination / Pollution
- Bodily Injury / Property Damage
- Errors & Omissions / Product Liability
- War & Terrorism (Carve back for Cyber Terrorism)
- Insolvency
- Money Laundry
- Fines & Penalties (where uninsurable – Carveback)
- Moneys – Cash – Values (sublimited – Crime Policy)
- Intellectual Property
- Contractual Liability (Surety)
- Employment Practice Liability
- Restricted List (OFAC, etc)

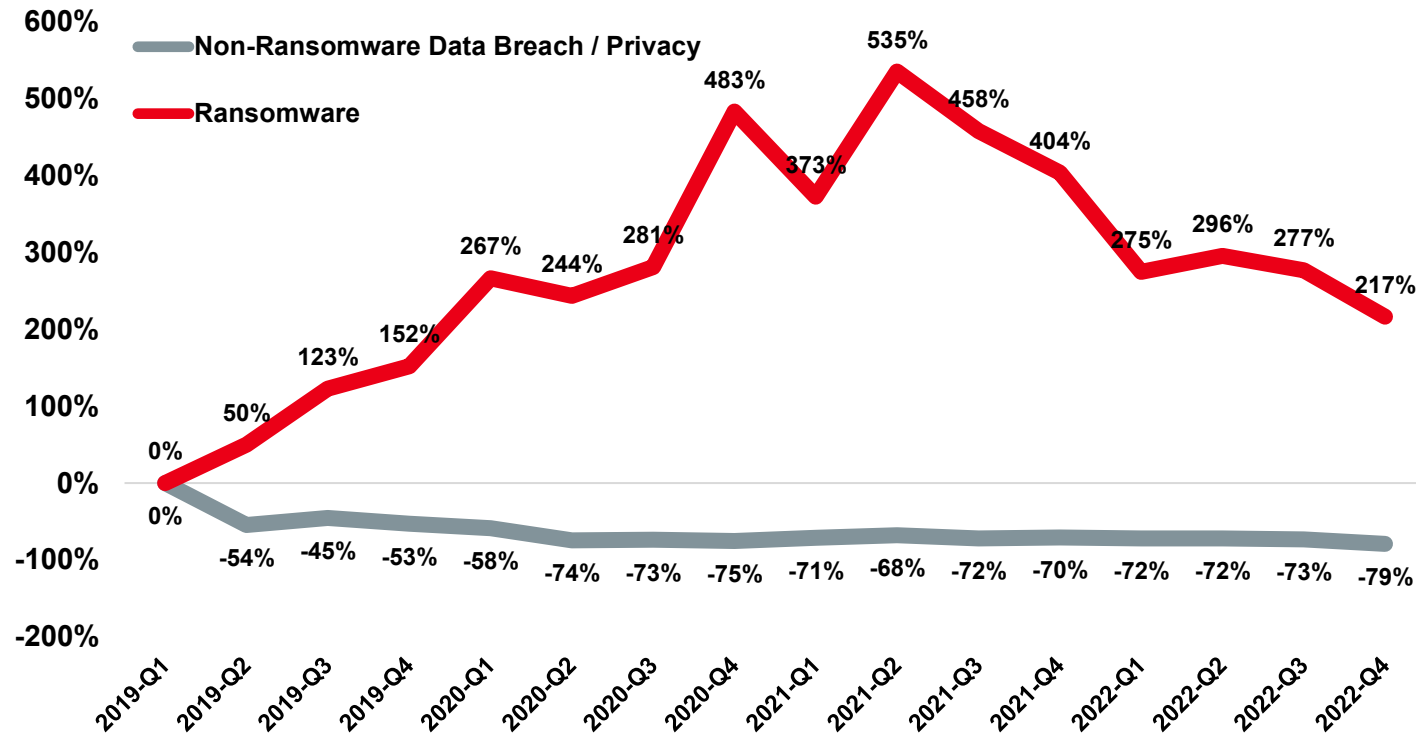


- Do include **Claims Protocol** in your IRP (broker, Panic Button, carrier)
- Do **report / inform to your broker / carrier**, as soon as you have any suspicion of a breach or incident
- Do **follow** Insurer (Vendors) **recommendations** or agree to a plan with Insurer
- Do **NOT** admit liability to any third party without Insurer sign off
- Do **NOT** make / approve any payment without the Insurer sign off (Carve back for Emergency Cost)
- Do **NOT** withhold information that may hinder your coverage.

3. We know that attacks have increased after the pandemic, mainly due to remote work and new ways of working. How have insurance premiums increased in relation to the attacks??



Cyber Incident Rates Indexed to Q1 2019



Key Observations:

- Ransomware activity has continued to **outpace Non-Ransomware Data Breach/Privacy Event activity.**
- **Ransomware up 217%** from Q1 2019 to Q4 2022
- Compared to Q3 2022:
 - **Ransomware down 16%**
 - **Non-Ransomware Data Breach/Privacy down 23%**
 - *Claim count development may mitigate this decrease
- The most commonly impacted industries by Ransomware in Q4 2022 were:
 - Healthcare
 - Public Sector
 - Manufacturing
 - Education

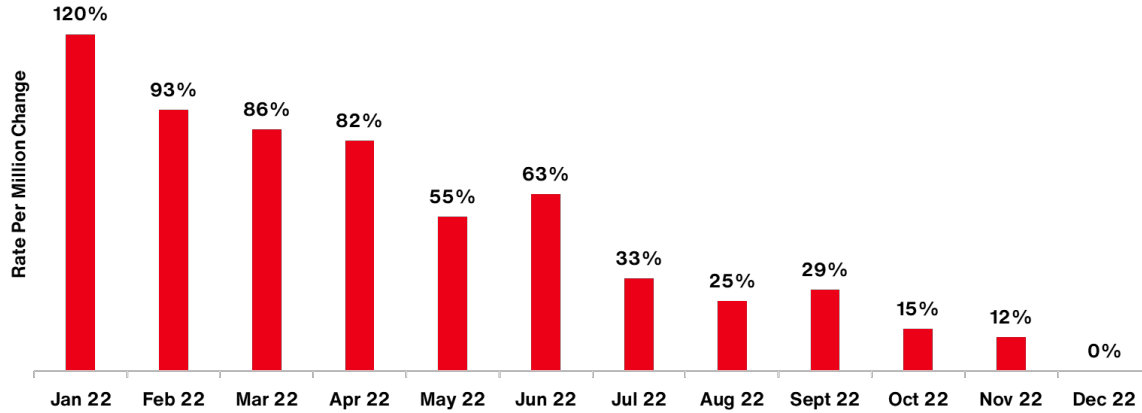
Source: Risk Based Security, analysis by Aon. Data as of 1/3/2023

Proprietary & Confidential: The content, analysis and commentary included herein are understood to be the intellectual property of Aon. Further distribution, photocopying or any form of third-party transmission of this document in part or in whole, is not permitted without the express, written permission of Aon.

Cyber Pricing FY 2022 - 2022

2021-2022 Cyber Monthly Pricing Primary Only

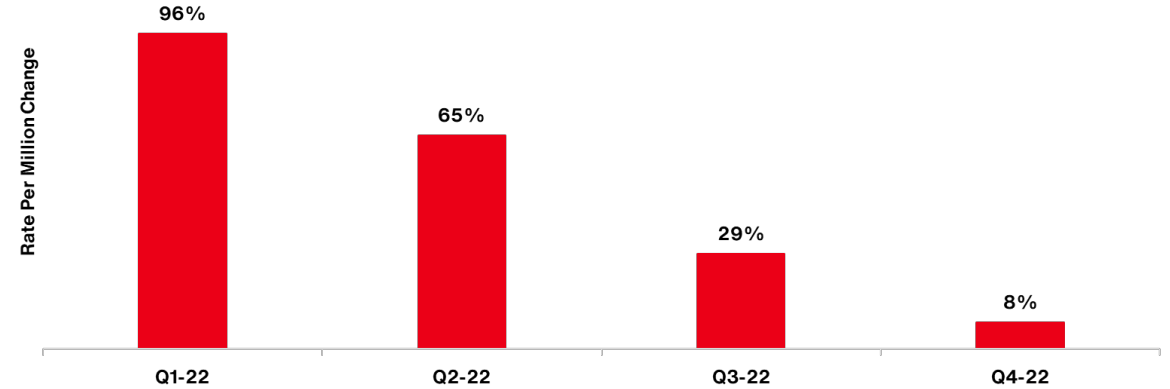
Average Year-over-Year Change (Same Clients)



■ Primary

2021-2022 Cyber Quarterly Pricing Primary Only

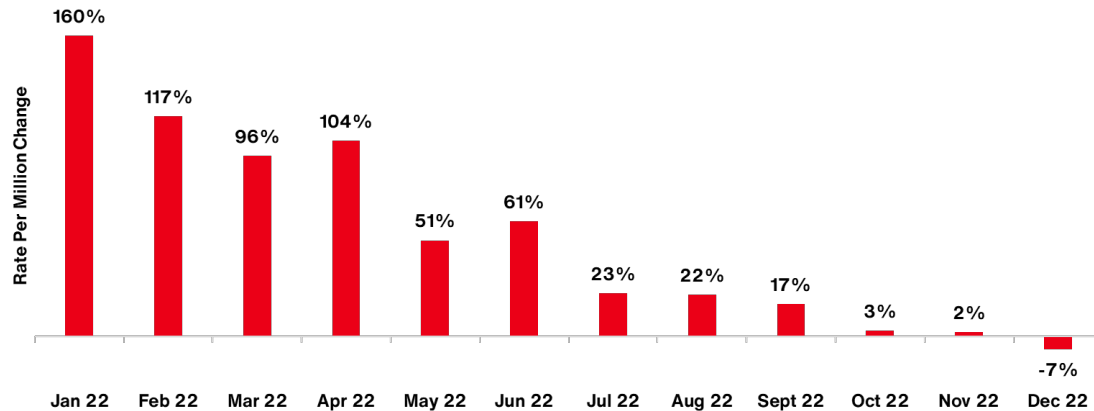
Average Year-over-Year Change (Same Clients)



■ Primary Only

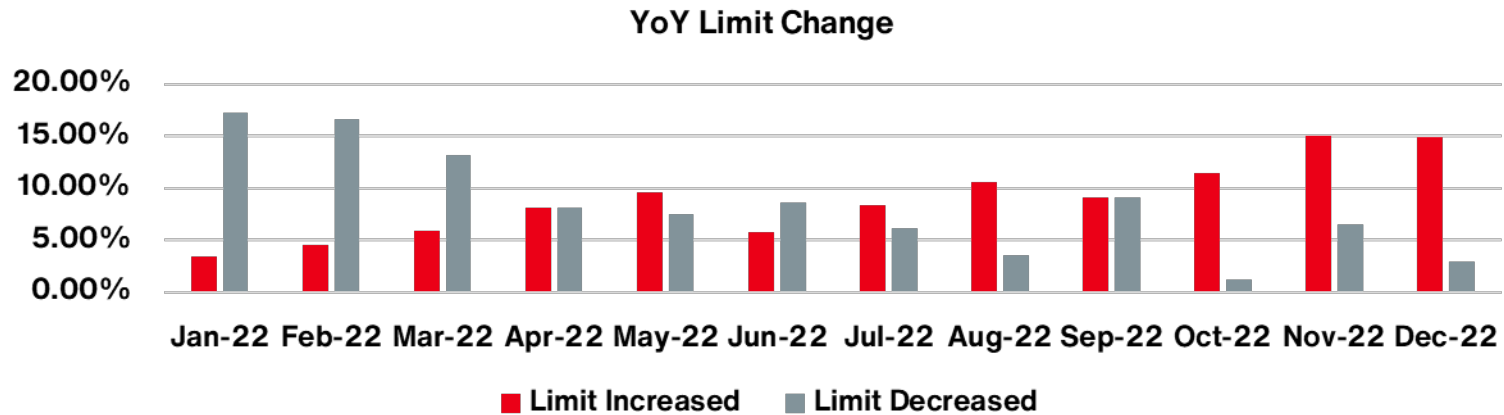
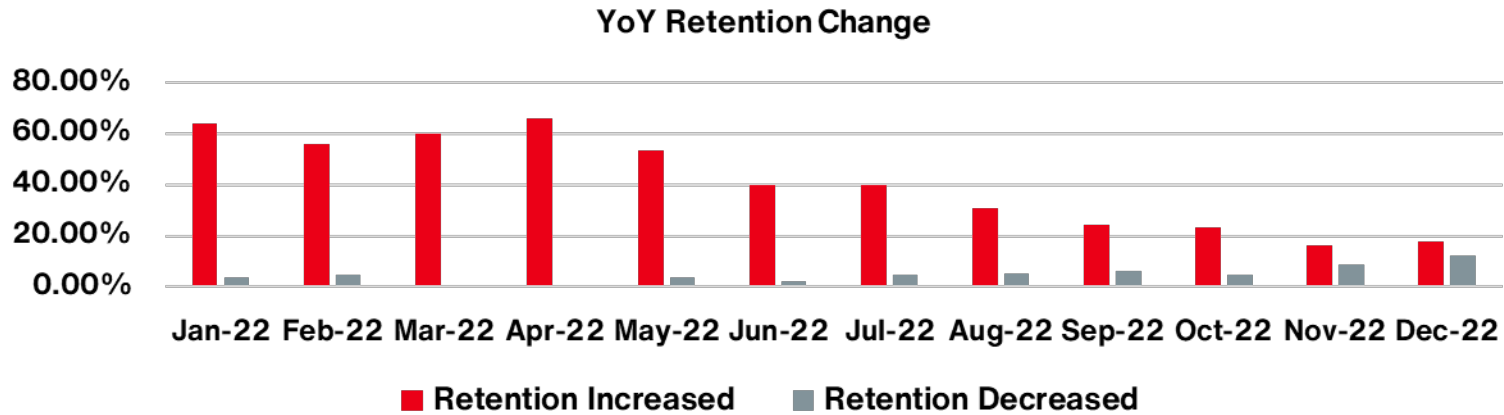
2021-2022 Cyber Monthly Pricing All Layers

Average Year-over-Year Change (Same Clients)









■ All Layers




Retention and Limit Change Year Over Year



- We are starting to see more retention decreases in Q4 and retention increases are leveling off.
- 15% of clients with renewals in November and December increased limits.

Cyber / Technology Professional Liability Q1 2023 Global Market Dynamics

<p>Pricing Primary: (Consistent) Excess: (Consistent to Decreasing)</p>		<p>Overall</p>	<p>Cyber & Tech E&O placements saw significant adjustments (premium, retention, coverage, capacity, etc...) over the past two years. In Q4 of 2022, the marketplace became more buyer friendly as headwinds subsided due to improved insurer loss ratios and the introduction of new capacity. Depending on the class of business, year-over-year improvement of controls, and previous market corrections – Q1 2023 should yield more favorable results compared to Q1 2022.</p>
<p>Capacity/Limit (Improving)</p>			<p>A Look Ahead</p>
<p>Underwriting / Process (Rigorous)</p>			
<p>Retentions (Consistent)</p>			
<p>Coverages (Consistent to Restricting)</p>			
<p>Claims & Loss (Improving)</p>			

-  Exceeds Norms
-  Meets Norms
-  Below Norms

Appendix



Cyber Insurance – Major Market Topics



Aggregation / Systemic Events

- Chubb and Beazley both employ strategies related to addressing aggregated systemic risks across their insurance portfolio.
 - Chubb: [Catastrophic Cyber Risks – A Growing Concern \(chubb.com\)](https://www.chubb.com/insights/cyber/catastrophic-cyber-risks-a-growing-concern)
 - Beazley: [Beazley finalises systemic cyber wordings ahead of phased rollout \(insuranceinsider.com\)](https://www.insuranceinsider.com/news/beazley-finalises-systemic-cyber-wordings-ahead-of-phased-rollout)
- More broadly, many insurers, particularly in London, are no longer offering full limit coverage for supply chain / non-IT suppliers and vendors, instead imposing sub-limits and limiting coverage to scheduled vendors only instead of a blanket all vendor approach. Some markets exclude the coverage entirely as out of appetite.



Pricing and Capacity Volatility Leads to Differing Reactions from Insureds

- Companies Are Ditching Cybersecurity Insurance as Premiums Rise, Coverage Shrinks <https://www.theinformation.com/articles/companies-are-ditching-cybersecurity-insurance-as-premiums-rise-coverage-shrinks>
- Rising cyber insurance premiums haven't scared away most companies <https://www.axios.com/2022/09/09/cyber-insurance-premiums-trend-companies>
- Leading European multinationals create cyber mutual to counter capacity crunch <https://www.miris-insurance.com/>



Markets are reviewing exclusionary language related to war, cyber terrorism, and state-backed attacks

- From March 2023, Lloyd's will require standalone Cyber policies to apply an LMA style exclusion, expressly addressing the cover provided for cyber-attacks carried out by states. [Market bulletin \(lloyds.com\)](https://www.lloyds.com/news/2023/03/01/market-bulletin)
- Other markets continue to revise definitions of cyber terrorism to ensure it does not apply to war or military actions.
- There remains a lack of consistency in the market with this policy provision, and many insurers still negotiate the language on a deal-by-deal basis.



Insurers continue to press for detailed representations as a part of underwriting which has consequences for Insureds.

- Travelers is seeking rescission of a policy in reliance upon an MFA attestation, alleging that the misrepresentation materially affected the acceptance of the risk: [Cyber Insurers Clamp Down on Clients' Self-Attestation of Security Controls \(darkreading.com\)](https://www.darkreading.com/cyber-insurance/cyber-insurers-clamp-down-on-clients-self-attestation-of-security-controls)

Important Notice | Claims Made Policies



Claims Made Policies

E&O / Cyber Liability policies often are claims made, which means that coverage applies to claims made during the policy period or extended reporting period (if applicable).



Reporting Requirements

E&O / Cyber Liability policies generally require reporting of claims during the policy period in which they were made. Failure to do so can result in denial of coverage.



Insurer Approval

E&O / Cyber Liability policies usually require the approval of the insurer(s) prior to selecting breach response vendors or defense counsel, incurring any defense costs, or agreeing to any settlement. Failure to do so can result in denial of coverage.



Note

The above comments are general observations. Please refer to your policy for actual terms and conditions.

This is a summary and is not intended to be an exhaustive analysis of all coverage items, exclusions, terms or conditions relevant to all claims and exposure situations. Please refer to the actual policy(ies) for coverage items

About

Aon plc (NYSE: AON) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

© Aon plc 2023. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

www.aon.com