UK Cyber Market Update

Q1 2024

Gallagher

Insurance | Risk Management | Consulting

Cyber context

2023 followed several turbulent years for the global cyber market; it is no secret that 2020 and 2021 were severely unprofitable for cyber insurers globally. Carriers were forced to put the brakes on; many paused writing new business or reduced limits and coverage for renewals as everyone grappled to understand what a good risk genuinely looked like.

This period witnessed a transition in underwriting methodology, not only regarding the requirements of rate and retention but also the minimum controls and risk management needed to deem a risk insurable.

Two main factors driving this were COVID-19 (and the global shift to a remote workforce) and the beginning of the ransomware epidemic — combined, they highlighted cybersecurity vulnerabilities across the globe. Consequently, underwriters first had to ascertain what key controls were acceptable for protecting organisations from ransomware and then request that insureds implement these accordingly.

There were indications of a positive shift at the start of 2023, with a broadening appetite and capacity. Insurers who had previously been restricting coverage were keen to grow, and the market saw a number of new entrants. The year started with ambitious growth targets from insurers, and in turn, throughout the year, our insureds were welcomed by rate reductions.

Organisations that demonstrated positive information security controls and sound risk management saw reductions of between 10%–30% as the rating environment eased. The average reduction sat toward the lower end of this spectrum, with the final figure determined by the expiring pricing, underlying risk profile, and placement strategy. Our clients looked to capitalise on the more accessible trading environment, often utilising these savings to reinstate higher programme limits back to a level held prior to 2020.

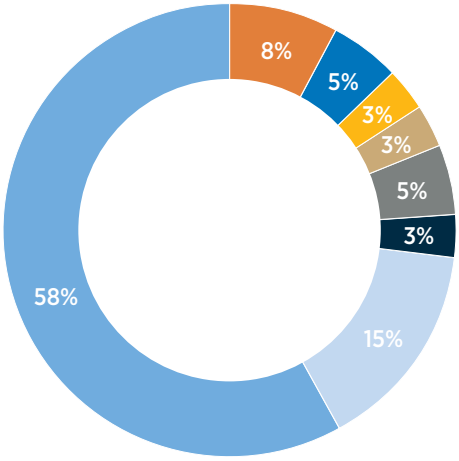
Another theme that developed was the broadening core underwriting appetite concerning the industry sector, geography, and security posture. Markets also started to drop minimum attachment points and deploy increased capacity on individual risks to combat the premium reductions across their portfolios.

Yet the most significant change in 2023 was a softening approach toward the minimum security controls insurers require to offer cover. While mainstay controls such as multifactor authentication (MFA) and endpoint detection and response (EDR) solutions need to be in place throughout the organisation, there has been increased flexibility across areas like privileged access management (PAM) solutions. Without these key controls, insurers would have simply declined the risk outright in the hard market. However, insurers are now willing to write such risks, provided clients can demonstrate a suitable workaround or evidence improvements are in the pipeline.

The claims landscape

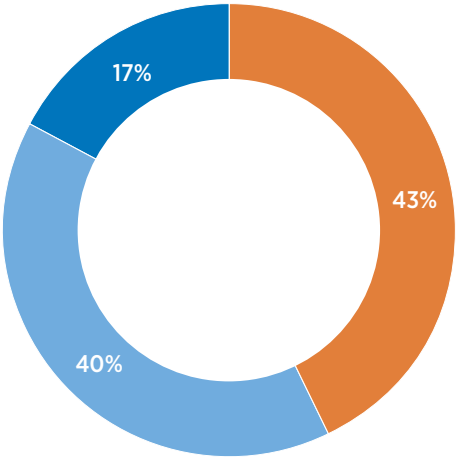
Last year saw an increase in claims compared to 2022, with ransomware notifications remaining at the forefront. According to IBM's Cost of a Data Breach Report 2023, the average cost of a data breach reached an all-time high of USD4.45 million last year (a 2.3% increase compared to 2022),[1] and Pinsent Masons 2024 Annual Cyber Report revealed that 58% of its cases involved some form of ransomware attack.[2]

Incident type



- Third party incident
- Business email compromise
- Credential stuffing
- DDoS
- Invoice Fraud
- Misdirected emails
- Other
- Ransomware

Was data exfiltrated?



- Yes
- No
- Unknown

Source: Pinsent Masons 2024 Annual Cyber Report

The severity of these claims has not seen the same trajectory as previous years, however, due to the increased levels of security controls for our insureds. According to global cyber risk company Arete, the percentage of incidents where a ransom is paid fell to 19% in the first half of 2023.[3]

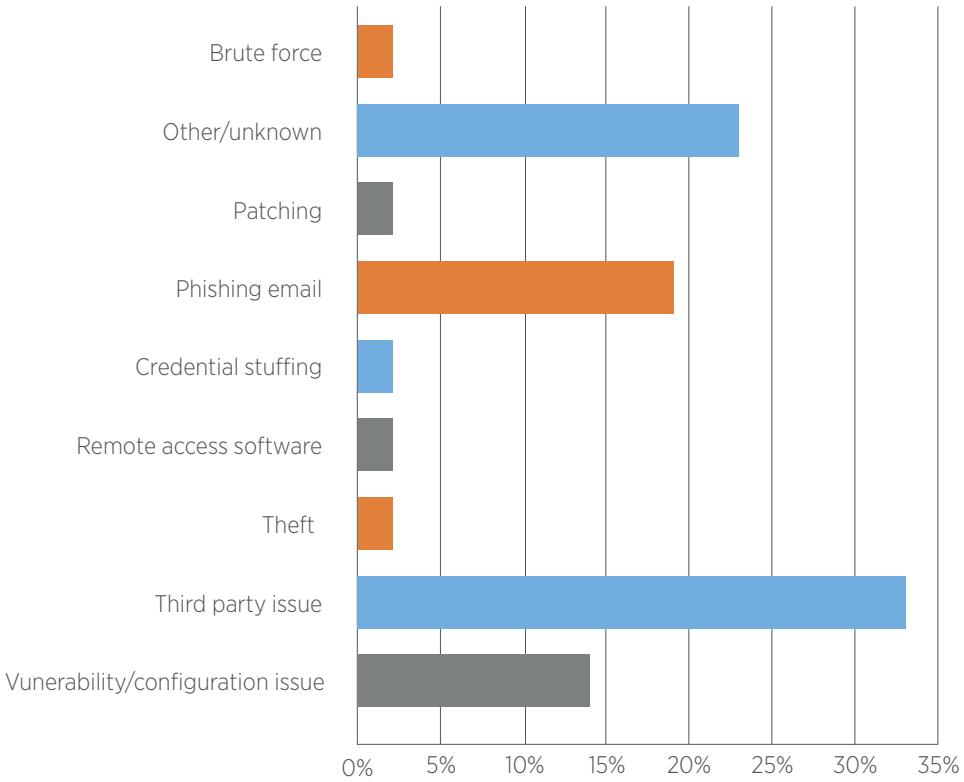
Law enforcement also plays a vital role in combatting criminal ransomware groups. In a first-of-its-kind sting to be led by the UK, in February, the National Crime Agency (NCA), with the support of the FBI and Europol, infiltrated ransomware group Lockbit's systems, stole its data, and took control of its website.[4]

Lockbit offers a ransomware-as-a-service model, leasing out its software to criminals for a share of any proceeds. High-profile targets have included Royal Mail and Industrial & Commercial Bank of China, along with suppliers to the NHS, Allen & Overy, and Boeing.

The NCA works closely with the cyber insurance industry to gain insight into the latest cyber risks. We welcome proactive measures such as this that tangibly reduce cybercriminals' impact. It will be interesting to see if these decisive actions from law enforcement impact cyber premiums in the future.

Pinsent Masons' report also showcases a significant uptick in supply chain breaches, with the root cause for 33% of the cases the law firm received instructions from relating to third-party issues.

Root cause



Source: Pinsent Masons 2024 Annual Cyber Report

The increasingly interconnected nature of our world means an attack can now easily reverberate across industries. An example of this increased vulnerability in action is the attack by threat actor group Cl0p against the file transfer platform MOVEit. As of 3 March 2024, 2,764 organisations and 94,944,183 individuals have been impacted by the attack.[5]

Business process services provider Capita was hit by another significant cyber attack targeting the supply chain in March 2023. After the incident, at least 90 breaches of personal information were reported by connected organisations to the Information Commissioner's Office, illustrating the potential impact of a single attack.[6]

The evolving privacy landscape is also at the forefront of concerns in the UK market. The US is known for being a litigious environment, and data breaches can result in significant damages from class action lawsuits. British Airways settled a class action lawsuit relating to its 2018 data breach in July 2021, and it is unclear whether it will face further privacy litigation in the future.[7] A class action lawsuit is also on the horizon for easyJet in response to the data breach it suffered in 2020. These cases may establish a precedent for privacy in the UK.[8]

Shoosmiths' 2024 Litigation Risk Report found that more than half (51%) of general counsels saw group litigation as the most significant risk over the next three years, with 32% identifying data breach litigation as the specific concern.[9]

Coverage

From a coverage perspective, the main talking point within the cyber market has been war exclusions. This has been the case since Lloyd's introduced its clauses for cyber war and cyber operation exclusions. In 2023, Lloyd's went one step further, and syndicates must now provide clear evidence and rationale behind the war exclusions they are electing to write business on.

Cyber war risk is considered systemic in nature by many, and excluding war perils has been a feature of insurance policies for centuries. Cyber insurance policies were never intended to cover, nor were they priced for, cyber events in conjunction with a physical war with a wide, lateral effect felt by a significant population.

These new exclusions are intended to remove ambiguity and add as much clarity as possible around the scope and intent of the exclusion. However, in reality, there are differing approaches deployed from insurer to insurer and, indeed, across the cyber market more broadly. It's, therefore, more important than ever that clients read the fine print and brokers explain how these unlikely yet devastating events could affect coverage.

Looking ahead

Rate depreciation typically goes in cycles. In the next six months, we believe that competition will continue to drive prices down, which will reverse some of the corrections endured over 2021 and 2022. What happens after that, however, is more difficult to predict. Despite competition and a negative rating environment, claims are still increasing, and the threat of systemic risk looms large. Where the number of ransomware demands being paid has fallen, many hackers have turned their attention to lower-level financial crimes like social engineering.

The cyber market is in a precarious position currently; industry experts are anticipating another market hardening, and 2024 may witness a significant market shift. While minimum security standards have undeniably improved, the downward pressure on rates is not a direct consequence of sufficiently long and sustainable improvements in insurers' claims ratios.

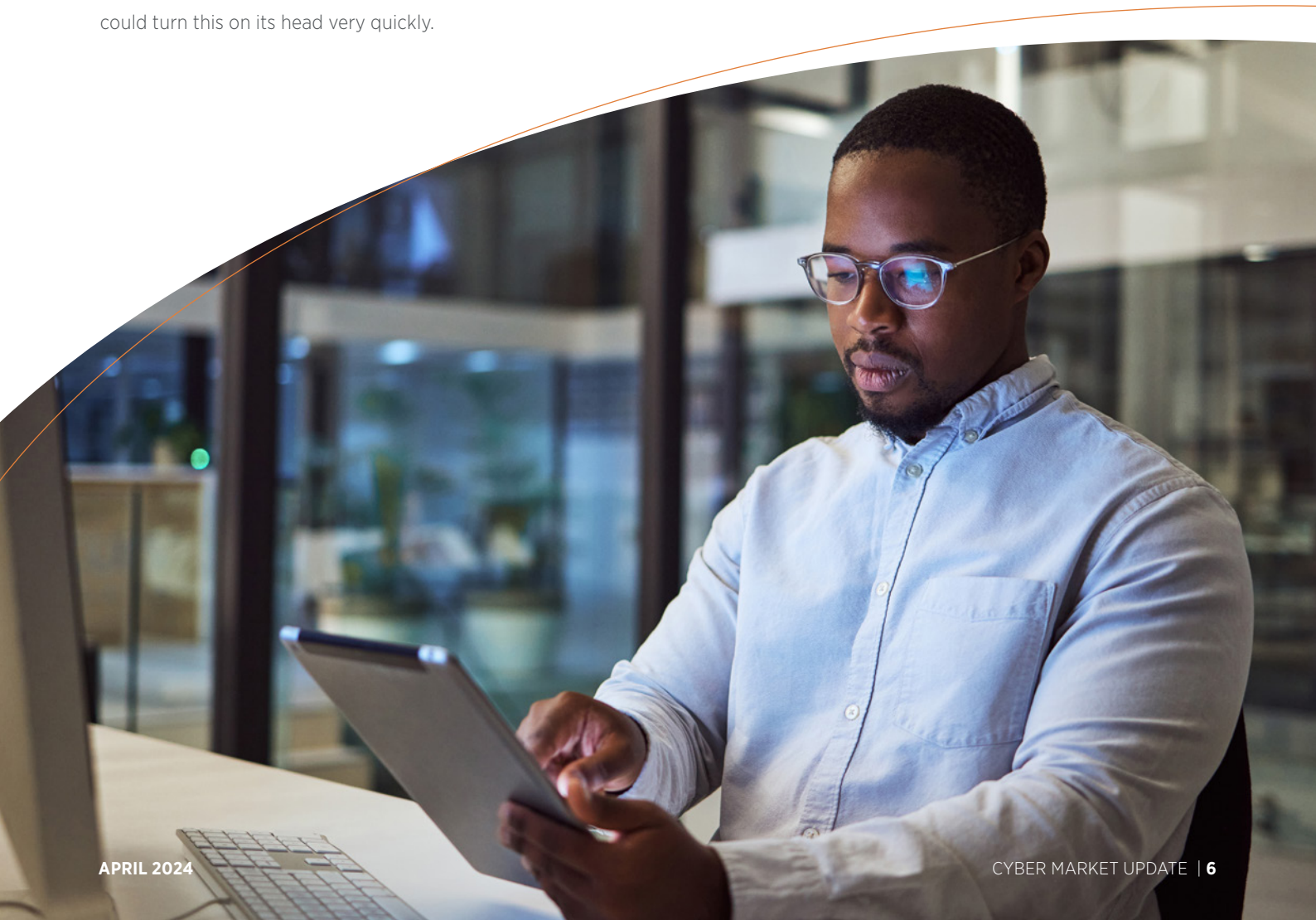
The good news is that cyber reinsurance rates did not dramatically increase in January, which removes one potential catalyst for further rate increases.

Nevertheless, the cyber insurance market remains in a state of flux. While a continuing trend would see further premium reductions through 2024, there are a number of factors that could turn this on its head very quickly.

Given that the risk landscape can develop overnight or we could see a catastrophic loss impact the market, it is impossible to predict the future with any certainty.

Yet the market is currently in an advantageous position for buyers. Now is the time to purchase cyber insurance, and if your firm already does, then now is the time to consider increasing the limit back to where it was before the market hardened. Going forward, cyber risk management and cyber insurance must not be siloed, and one should not be favoured over the other. Risk management and insurance coverage should work in unison to maintain adequate preventative measures while providing protection should the worst occur.

The cyber market has now matured to a level where both applicants and providers of cyber insurance have gained valuable insight into how threats manifest into claims and generally understand minimum security controls, but more needs to be done. Cyber insurance carriers, reinsurance providers, brokers, cybersecurity vendors, the regulators, and, of course, threat actor groups will all play key roles in the development of cyber insurance throughout 2024.



How Gallagher can help?

Engaging with a broker that has access to various insurance markets can have many benefits when trying to source optimal coverage for your business. Gallagher's dedicated cyber insurance and risk management specialists work hand in hand with many organisations, helping them to get the cover they need and embed risk management strategies to defend against cyber threats. If you would like to know more about the comprehensive services we offer, please contact Sam Cheshire, Head of Cyber, UK Retail, using the details below.

Sam Cheshire
Head of Cyber
UK Retail

T: 07714 677 635
E: sam_cheshire@ajg.com

About Gallagher

The Gallagher Way. Since 1927. Gallagher is one of the world's largest insurance brokerage, risk management, and consulting firms. As a community insurance broker and trusted local consultant, we help people and businesses move forward with confidence. With more than 52,000+ people working around the globe, we're connected to the places where we do business and to every community we call home. Managing risk with customised solutions and a full spectrum of services, helping you foster a thriving workforce, and always holding ourselves to the highest standards of ethics to help you face every challenge — that's The Gallagher Way.

Citations

[1]"Cost of a Data Breach Report 2023," *IBM*, July 2023.
[2]"Pinsent Masons Cyber Annual Report 2024," *Pinsent Masons*, February 2024.
[3]"Turning Tides: Navigating the Evolving World of Cybercrime," *Arete*, accessed 01 March 2024.
[4]"The NCA Announces the Disruption of LockBit With Operation Cronos," *National Crime Agency*, 20 February 2024.
[5]Simas, Zach. "Unpacking the MOVEit Breach: Statistics and Analysis," *Emisoft*, 1st published 18 July 2023, last updated 03 March 2024.
[6]ICO Case Reference IC-235406-T7M2, *Information Commissioner's Office*, 01 June 2023.
[7]"British Airways Data Class Action Settles," *Herbert Smith Freehills*, 08 July 2021.
[8]Powley, Tanya, and Kate Beioley. "EasyJet Faces Group Legal Claim Over Cyber Attack Data Breach," *FT.com*, 24 June 2020.
[9]MacLachlan, Matthew. "Class Action Liability Following a Data Breach," *Shoosmiths*, 16 February 2024.

AJG.com/uk **The Gallagher Way.** Since 1927.

Gallagher