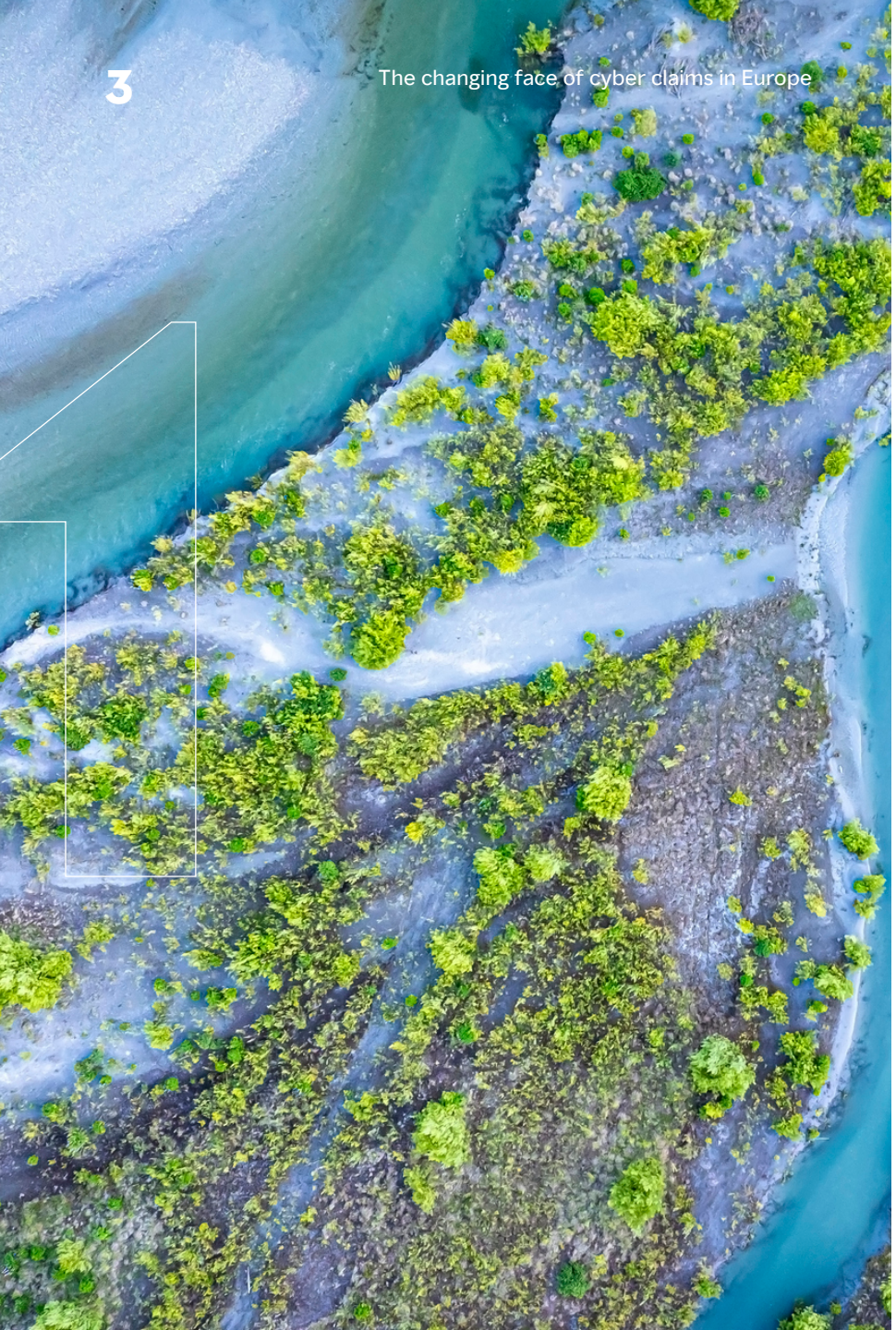
Marsh

The changing face of cyber claims in Europe

Europe cyber claims report

Contents



Key takeaways

Understanding trends in cyber claims helps to inform an effective risk management strategy for what is a signature risk in today's tech-dependent society.

Analysis of the cyber claims submitted to Marsh in Europe in 2023 reveals the following:

- Cyber claims increased 1% in 2023 compared to 2022, continuing a general upward trend that started in 2016.
- Financial institutions accounted for the highest number of cyber claims (21% of the total); followed by communication, media, and technology (17%); professional services (13%); manufacturing (9%); and healthcare (7%).
- The number of claims related to malicious acts continued to far outpace those related to non-malicious acts.
- Claims related to extortion/ransomware accounted for 25% of the total, followed by data breaches (19%), and network interruption (10%).
- In 2023, organisations were less likely to pay a ransom in an extortion incident, amid a general strengthening of their cyber resilience.
- Manufacturers remained a prime target for cybercriminals, although the sector reported fewer claims in the last two years compared with other years.
- Cybercriminals often targeted IT service providers, and the uptake of cyber insurance increased in this group.

Note on 2024:

In the first half of 2024, cyber claims notifications in Europe increased, accounting for approximately 70% of the total claims received in 2023.

The most common incidents included social engineering, phishing, and impersonation, followed by system infiltration, ransomware, and data breaches. Additionally, a major incident involving a CrowdStrike software update caused a global IT outage on 19 July 2024, impacting millions of Microsoft Windows device users worldwide.

A recap of the latest insights and client discussions on CrowdStrike and a recovery resource guide from Marsh can be viewed here.

Introduction

As cyber risk continues to be a key issue for organisations of all sizes and across industries, effective risk transfer remains a central piece of a successful risk management strategy. It's thus important for organisations to understand cyber insurance claims trends and be prepared to effectively manage potential claims.

This report looks at cyber claims reported by Marsh clients in the European region in 2023. Organisations experienced a slight increase (+1%) in the number of claims in 2023, compared to the prior year. However, the total claims in 2022 and in 2023 were both less than in 2021. This can be attributed in part to actions taken by governments and organisations to become more resilient to cyber risk.

Cyber claims trends in 2023 also should be viewed against the backdrop of a rapidly developing cyber insurance market, as well as the EU's new digital strategy.

In this report, we analyse claims by industry and type, with attention to the main triggers and how they have changed in recent years. We also share suggestions on how to manage a cyber insurance claim and explore the challenges of navigating a cyber-related business interruption loss.

Cyber claims in 2023

Cyber claims up slightly in 2023; remain below 2021 level

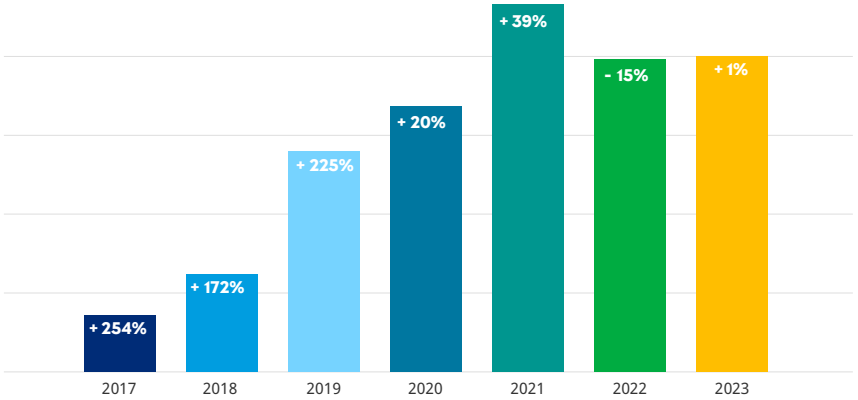
From 2016 to 2021, the number of cyber claims in Europe grew each year, then dropped in 2022 before edging up slightly (1%) in 2023 (see Figure 1). The growth in policies placed in 2023, exceeded the growth of notifications, reversing a recent trend of the growth of notifications surpassing the growth in policies placed.

However, when comparing the number of claims in 2020 to those made in 2023, there was a significant increase over this period. This upward trajectory indicates a continuous growth in cyber claims in the region.

Moreover, the slowing in the number of claims since 2021 should not be attributed to a decrease in cyberattacks, as the European Repository of Cyber Incidents and other sources show incidents increasing over this period.

The drop in the number of claims reported by Marsh clients is likely due to a combination of a better understanding and more precise wording in policies regarding what constitutes a notifiable circumstance, and the adoption by organisations of stronger cyber hygiene practices.

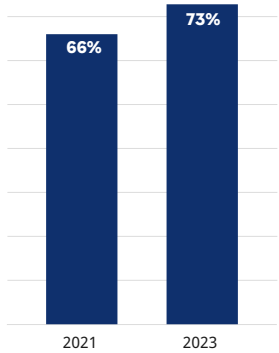
01| European cyber claims up slightly in 2023



Source: Marsh

02| Organisations appear better prepared to face cyber threats

Average IT security maturity score evolution on 10 critical controls



Source: Marsh

03| Marsh key controls with strongest effect related to experiencing a cyber event

Marsh key control category	Description
Hardening techniques	Our system configuration management tools (such as active directory group policy) enforce and redeploy configuration settings to systems.
Privileged access management	The organisation manages desktop/local administrator privileges via endpoint privilege management (EPM).
Endpoint detection and response	The organisation operates advanced endpoint security.
Logging and monitoring	The organisation operates its own security operations centre (SOC) and/or has an outsourced managed security service provider (MSSP) with the following capabilities at a minimum: (a) Established incident alert thresholds (b) Security incident and event management (SIEM) monitoring and alerting for unauthorised access connections, devices, and software
Patched systems	Patching common vulnerability scoring system (CVSS) v3 high severity 7.0-8.9 vulnerabilities across the enterprise within seven calendar days of release.
Cybersecurity training	The organisation conducts internal phishing campaigns at least annually.
Endpoint detection and response	The organisation operates network intrusion detection/prevention systems (IDPS).
Patched systems	Patching common vulnerability scoring system (CVSS) v3 critical severity 9.0-10.0 vulnerabilities across the enterprise within seven calendar days of release.
Email filtering	Email attachments are evaluated in a sandbox to determine if malicious prior to delivery.
Logging and monitoring	In addition to the capabilities above, the SOC/MSSP capabilities include, but are not limited to, the following: (a) 24x7 operations (b) Mix of signature and heuristic-based detection (c) Incident response, containment, and remediation capabilities (d) Active threat intelligence and analytics delivering rapid alerts/notification and/or countermeasures (e) Processes are continuously improved

1| Cybersecurity best practices have evolved since the time period of the cyber incidents, with managed detection and response (MDR) and extended detection and response (XDR) superseding earlier EDR tools such as advanced endpoint security (AES).

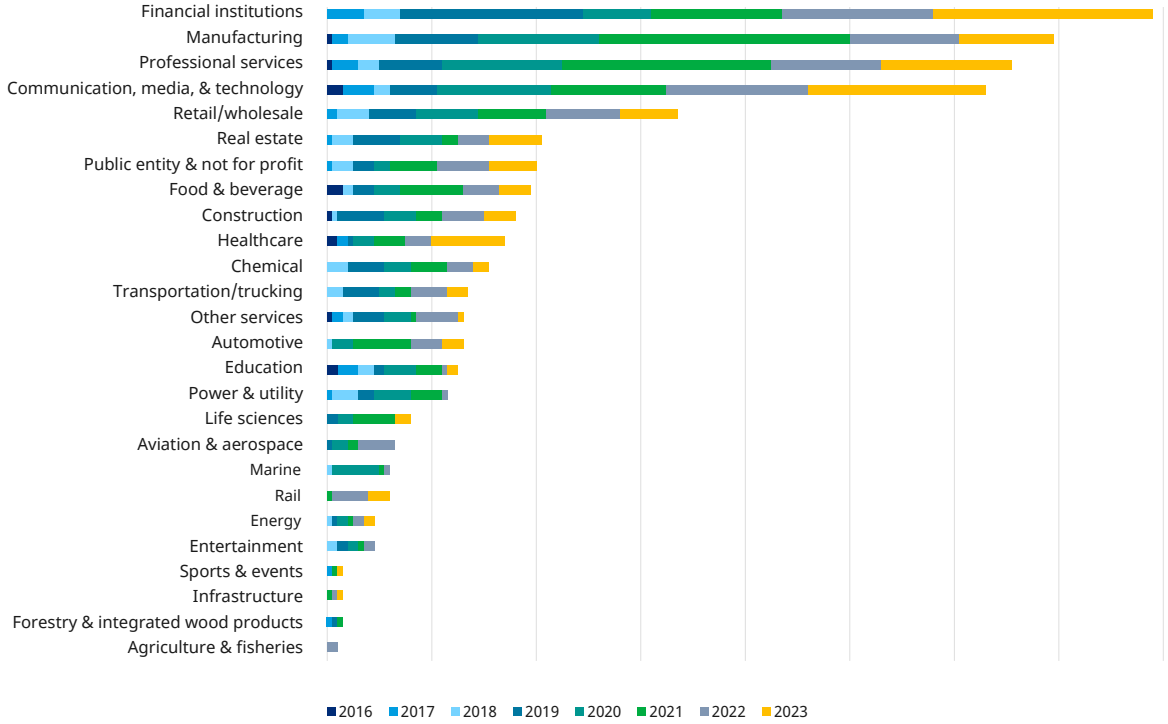
Source: Marsh (Report: Using data to prioritise cybersecurity investments)

There are several factors contributing to the decline in claims in Europe following the large increase in 2021, a trend also seen elsewhere such as in the US and Canada. Cyber security experts, both inside and outside of Marsh, cite factors including a temporary decrease in focus on economically-motivated crime due to the start of the Russia-Ukraine war. In addition, a number of successful law enforcement operations led to the disruption of ransomware-as-a-service (RaaS) operations (where a ransomware group sells its ransomware code or malware to other hackers). Also, organisations' increased cybersecurity maturity and resilience led to a decrease in frequency. Cyber extortion threat actors focused less on encryption and more on data exfiltration, which may have led to fewer business interruption losses and therefore fewer claims exceeding the policy deductible

In addition, we have seen an increase in governmental and regulatory attention, as demonstrated by the EU digital strategy, ensuring that cyber risk management will continue to evolve from an information and communications technology (ICT) subject to include more C-suite discussions. Relevant regulations include the Digital Operational Resilience Act (DORA), which aims to strengthen the IT security of financial entities; NIS2 Directive, aimed at increasing the resilience of organisations' networks and information systems; and the Artificial Intelligence (AI Act), with a goal to increase resilience in organisations' networks and information systems.

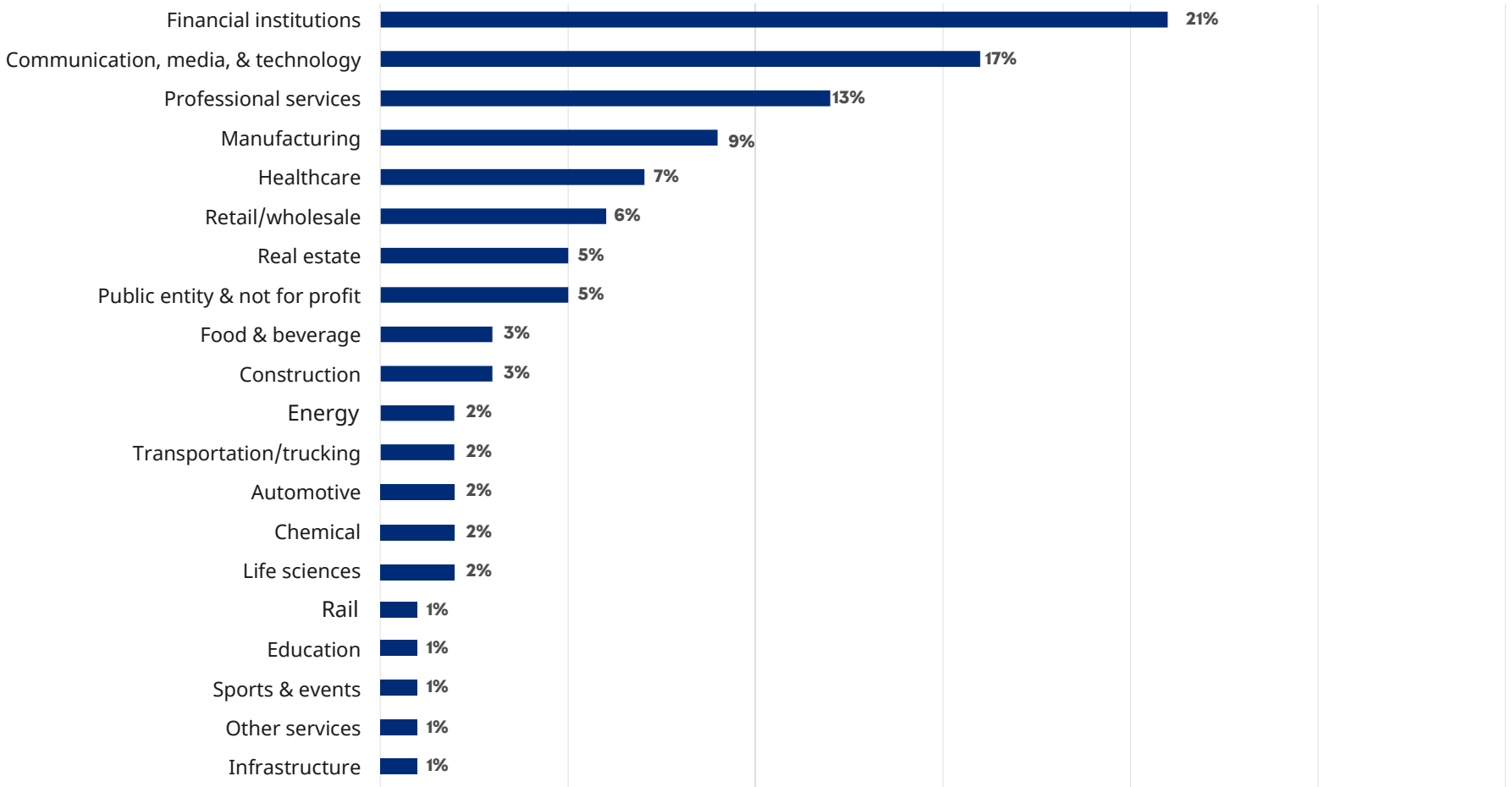
Between 2016 and 2023, the industries experiencing the most cyber claims were financial institutions (15% of the total), manufacturing (13%), professional services (12%), communication, media, and technology (12%), and retail and wholesale (6%) (see Figure 4). However, in the last two years, the manufacturing industry reported fewer cyber claims (see industry focus section below), while the frequency of claims grew considerably in other industries (such as healthcare, CMT, and financial institutions) during this period. In 2023, financial institutions accounted for 21% of total cyber claims, followed by communication, media, and technology (17%), professional services (13%), manufacturing (9%), and healthcare (7%).

04| Financial institutions experience the highest number of cyber claims since 2016

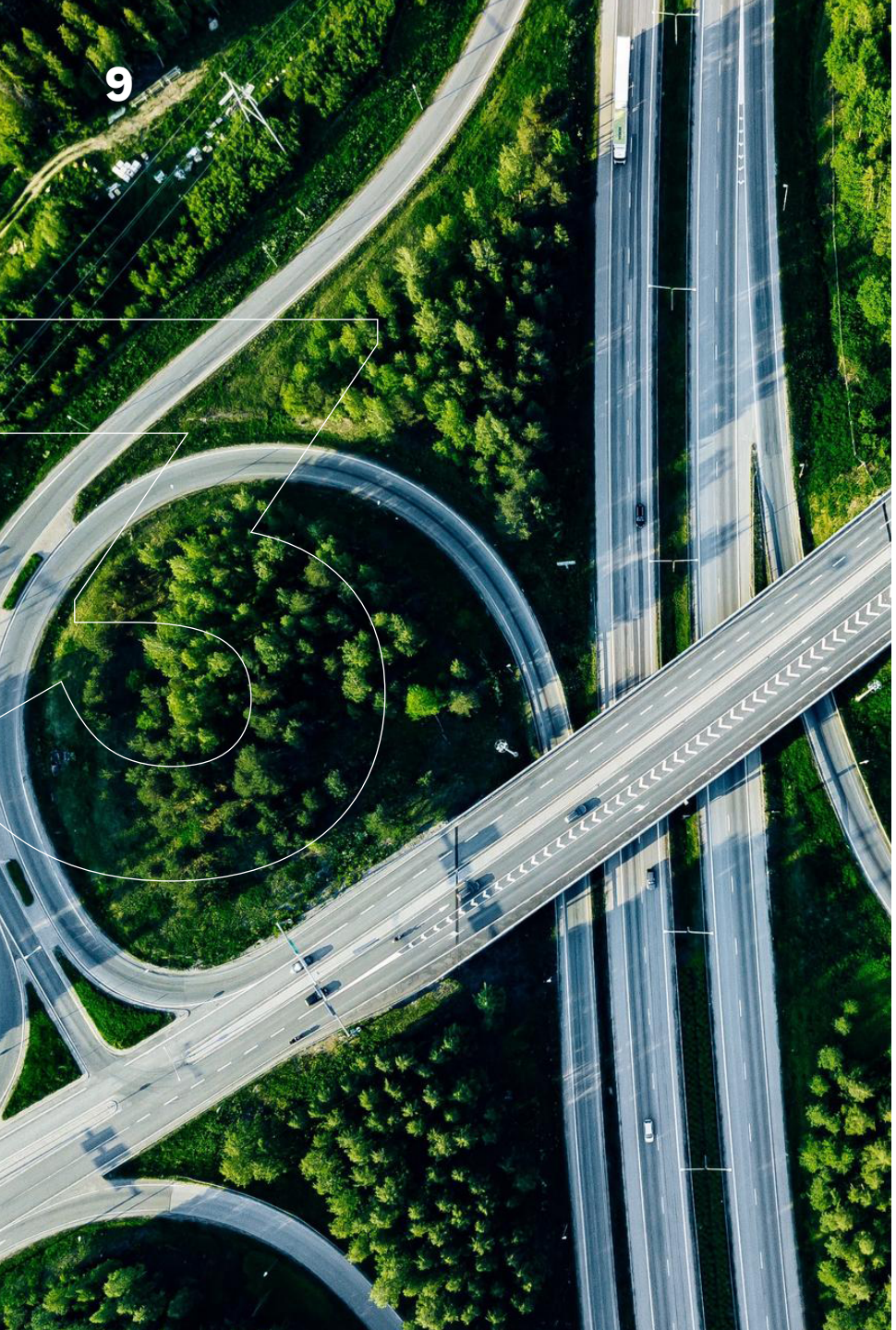


Source: Marsh

05| Financial institutions experienced the highest number of cyber claims in 2023



Source: Marsh



Industry focus

Manufacturers improve their cyber resilience

Manufacturing organisations are often targeted by cybercriminals due to their low tolerance for downtime and relatively low level of cyber maturity compared to other industries. At the same time, their dependence on IT and OT (operational technology) infrastructure may increase the likelihood that they will opt to pay a ransom demand by cybercriminals if they believe the purchase of a decryption key will allow the fastest recovery of systems and resumption of operations.

Additionally, the extended production cycles and the significant investments required to redesign manufacturing lines can lead to a lag in investment in cyber resilience.

Despite these challenges, there is a growing recognition among manufacturing leaders of the need to take action to future-proof their operations. A recent World Economic Forum report, Advanced Manufacturing: A New Narrative, highlighted the necessity of strengthening resilience in the sector, including by improving responsiveness to shocks. Meanwhile, manufacturing leaders are exploring ways to enhance supply chain resilience and prioritise cybersecurity within their organisations.

NIST framework built on six key functions

One valuable tool used by manufacturers and other organisations across Europe is the US-based National Institute of Standards and Technology (NIST) cybersecurity framework. The framework consists of six core functions:

Protect: Implementing safeguards can ensure the confidentiality, integrity, and availability of sensitive information and systems. Measures include controls, encryption, and regular updates to shield systems against unauthorised access by individuals.

Detect: Advanced security controls and mechanisms can swiftly identify cybersecurity events, allowing organisations to respond to potential threats, minimising the impact of security incidents and reducing the risk of prolonged breaches.

Identify: Organisations can gain a clear understanding of their digital landscape by documenting critical assets, systems, and data, and assessing vulnerabilities and potential threats. They can then effectively allocate resources and prioritise security measures to mitigate cyber risk.

Respond: Developing an incident response team and an incident response plan and conducting regular drills and exercises can ensure a swift and coordinated response to cybersecurity incidents. By promptly addressing and containing threats, organisations can minimise damage and efficiently restore normal operations.

Recover: The implementation of strategies to restore normal operations after a cybersecurity incident can minimise downtime and mitigate financial losses. The framework emphasises the importance of conducting post-incident analysis and improving security measures after a cyber event.

Govern: This is the newest function in the framework, introduced in February 2024. The governance aspect highlights the significance of cybersecurity and the importance of organisations considering it at a senior leadership level.

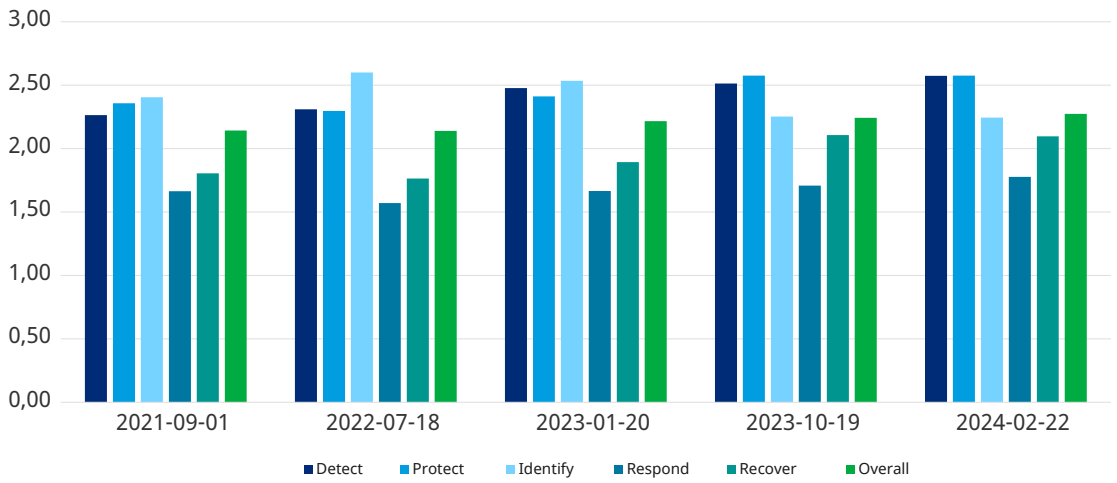
What is NIST cyber risk scoring?

National Institute of Standards and Technology (NIST) scoring measures an organisation's cybersecurity posture benchmarked against the NIST framework. The framework offers high-level cybersecurity outcomes that can be used by any organisation — regardless of its size, sector, or maturity — to better understand, assess, prioritise, and communicate its cybersecurity efforts. The aim of the scoring is to provide guidance to industry, government agencies, and other organisations to manage cybersecurity risks.

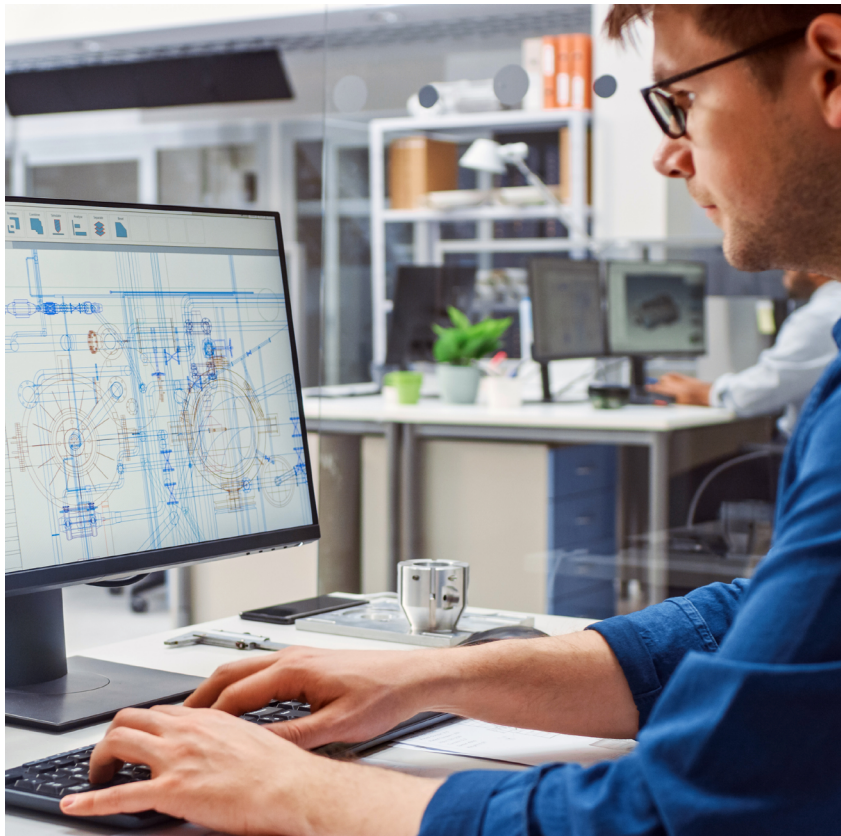
Across Europe, many manufacturers have enhanced their abilities to detect and protect against cyberattacks, as seen in the sector's improved average NIST scores between 2021 and 2023 (see Figure 6). In October 2023, manufacturers' average NIST score for detection exceeded the average for all organisations (see Figure 7).

However, manufacturers generally have been less attentive to what should be done when bad actors infiltrate the ICT network. For example, regarding the NIST "respond" function, we have observed many manufacturers failing to acknowledge severe cyber incidents as a significant business risk that impacts more than IT.

06| Average NIST scores of European manufacturing companies in 2023



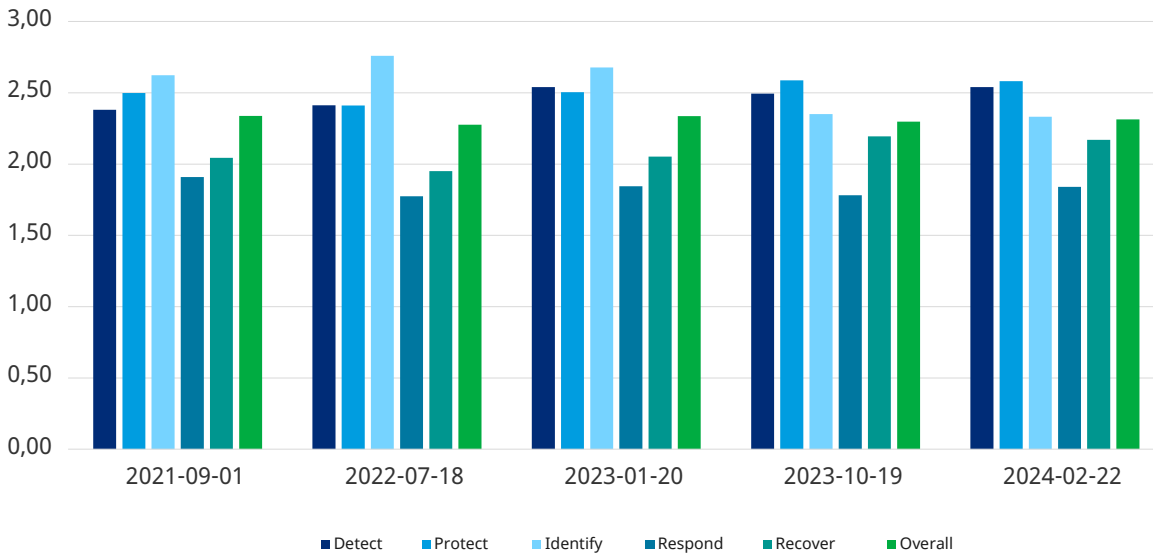
Source: Marsh



Additionally, manufacturers often do not adopt an incident response approach that prioritises mitigating the overall impact of an event across the organisation. In October 2023, manufacturing organisations' average NIST scores for the protect, identify, respond, and recover functions of the framework were below those of organisations in other sectors (see Figures 6 and 7).

An effective strategy during a cyberattack could, for example, involve carefully balancing IT security considerations during the recovery of IT systems, while minimising the duration of business interruption. Such an approach typically results in lower losses resulting from a cyber incident compared to a method that focuses on maximum security but prolongs the interruption period.

07| Average NIST scores of European organisations in 2023



Source: Marsh

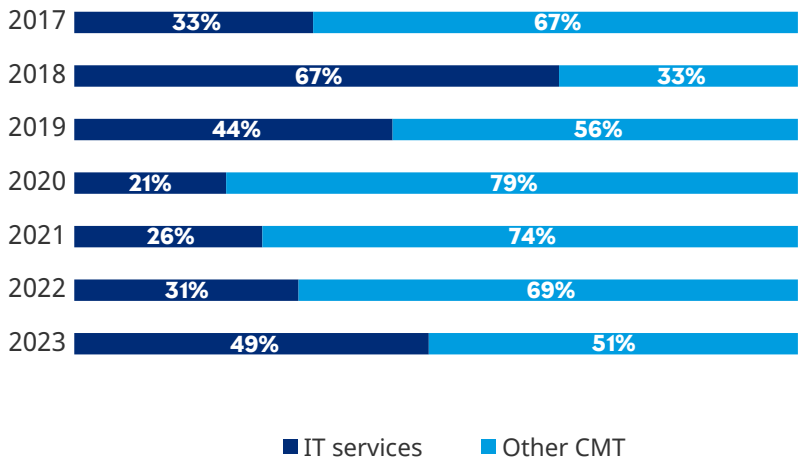
Cybercriminals target IT service providers

While the communication, media, and (CMT) sector, as a whole, experienced increased frequency of cyber claims in 2023, the fastest growth was seen in the subcategory of IT products and services, accounting for 49% of CMT claims in the region, up from 31% in 2022 and 26% in 2021.

Outsourced IT service providers can be attractive targets for cybercriminals due to the sensitive data they hold and the access they often have to their clients' systems. There have been multiple instances — seen in both Marsh's European CMT claims data and in the public domain, globally — where outsourced or technology service providers have specifically been targeted and compromised by cybercriminals. Nevertheless, the increase in the number of cyber claims within the industry (CMT and the subcategory of IT) additionally needs to be seen in the context of the increased uptake of cyber insurance policies within this group.

The purchase of cyber insurance, including standalone policies or blended coverage (with professional indemnity cover, for example) is becoming more common for this group of organisations as they increasingly recognise the value.

08| Cyber claims rise in the communication, media, and technology (CMT) sector



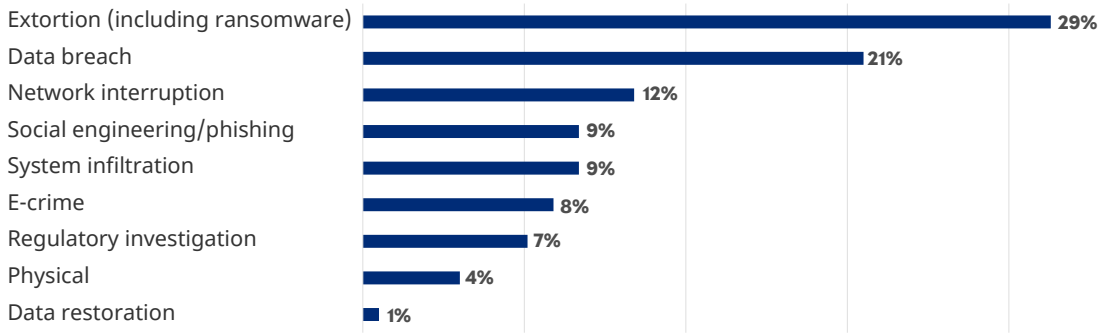
Source: Marsh

Ransomware/extortion remain a top concern

In terms of the types of cyber claims in 2023, the most frequent incidents related to extortion/ ransomware (25% of claims), followed by data breaches (19%), and network interruption (10%) (see Figure 9).

It remains clear that most cyber claims result from malicious cyber events — such as extortion, social engineering, and internal fraud — carried out by threat actors with bad intentions. The claims resulting from non-malicious events — such as IT outages after a faulty software update or patch — are much less frequent. The number of notifications from malicious cyber incidents increased at a slower pace in 2022 and 2023, mirroring the overall trend in cyber claims activity.

09| **Extortion accounted for the highest number of claims in 2023**



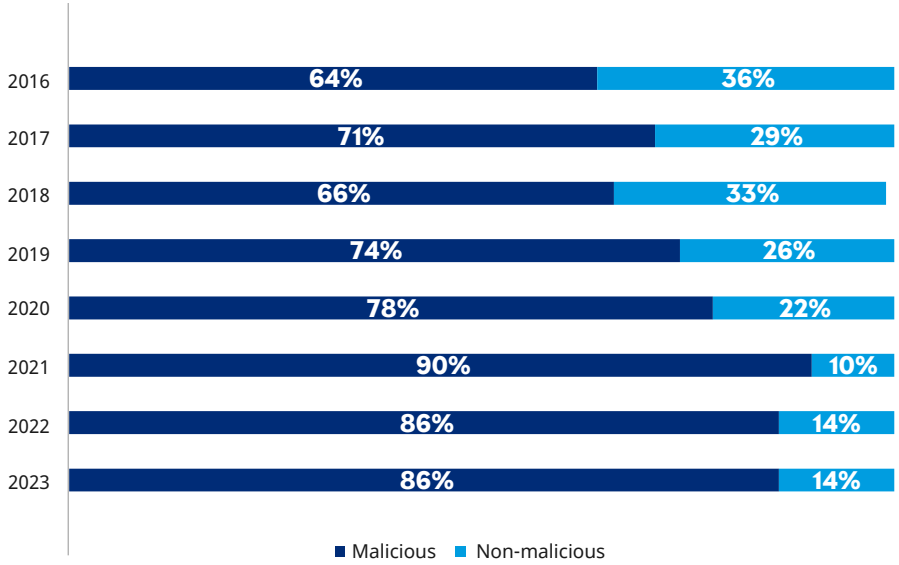
Source: Marsh

Note

There were numerous cases where data was encrypted, but no ransom demand was made.

It's possible that criminals encrypted the data intending to demand a ransom, but the target organisation quickly decrypted its ICT system, or the bad actors were otherwise unable to deploy the ransomware demand.

10 | The majority of cyber claims notifications are from malicious events



Source: Marsh Cyber Self Assessment database

Number of ransom payments declines

Ransom coverage remains an important element of cyber insurance, although the number of companies paying ransoms has decreased over the past few years. This is likely due in large part to organisations opting not to pay ransom demands and the general strengthening of organisations' cyber resilience.

For example, many organisations have implemented secure and isolated system backups that are immune to encryption or deletion by threat actors. Additionally, IT recovery times — the time taken to install a backup — have improved and now increasingly meet established targets.

Number of non-malicious cyber claims remains stable

The number of non-malicious cyber claims remained stable in 2023, making up a small fraction of total notifications. This was due partly to the fact that non-malicious cyber incidents typically have a lower financial and business impact compared to malicious events.

The potential harm from non-malicious events was underscored in the global CrowdStrike incident on 19 July 2024, when a single faulty software update caused outages for millions of users of Microsoft Windows devices worldwide.

Losses arising out of such events can be significant, especially for organisations with a high dependency on the availability of systems and/or a low tolerance for downtime. Across Europe, there were a number of non-malicious incidents in 2023 that led to substantial losses and reimbursements under cyber insurance policies.

Non-malicious cyber incidents observed that had a high impact on the affected organisation included a variety of patterns, such as:

- Poor implementation of enterprise resource planning (ERP) systems used to handle and store data
- General Data Protection Regulation (GDPR) infringements
- Software bugs
- Power outages at data centres
- Faulty updates creating downtime

Five best practices to manage a cyber claim

During a cyber incident, the initial focus will be on containment of the threat and mitigation measures to minimise its impact on the business. At this stage, however, it is important for organisations not to lose sight of any potential claims they may make on their cyber policy. The following actions can help organisations achieve a satisfactory resolution of a cyber insurance claim.

1. Notify insurers and broker

Insurers and brokers should be informed of a cyber incident immediately, so they can triage and provide support and guidance. Organisations should also inform insurers if they become aware of any claim made against them relating to the incident.

2. Seek approval for outside assistance

If organisations are not using preapproved vendors from their insurer's panel, they may be required to obtain consent from their insurer for any external consultants appointed.

3. Gather the facts

Organisations should do all that is reasonably possible to establish the cause and extent of the incident, including what data has been affected.

In order to mitigate business income losses resulting from the attack, they should keep records of sedentary hours of staff, the event's impact on sales and the ability to service customers, overtime required to make up for interruptions, and all other expenses incurred.

4. Collect documentation

Organisations are advised to assemble documents that insurers are likely to request in the event of a claim, such as:

- IT forensic incident report
- Documentation relating to the shutdown of the IT system and network infrastructures in order to contain the spread of the attack
- Reports to regulators and authorities
- Documentation relating to third parties and/or companies involved
- Court documents
- Claims by third parties

5. Undertake due diligence regarding ransom payments

If a ransom was paid, acquire external evidence to show that, to the best of your and your consultants' knowledge, any payment was not made to a terrorist organisation or any persons on recognised sanctions lists. Also, obtain documentation to show why other options to recover data were not deemed possible or financially viable, compared with the extortion payment.

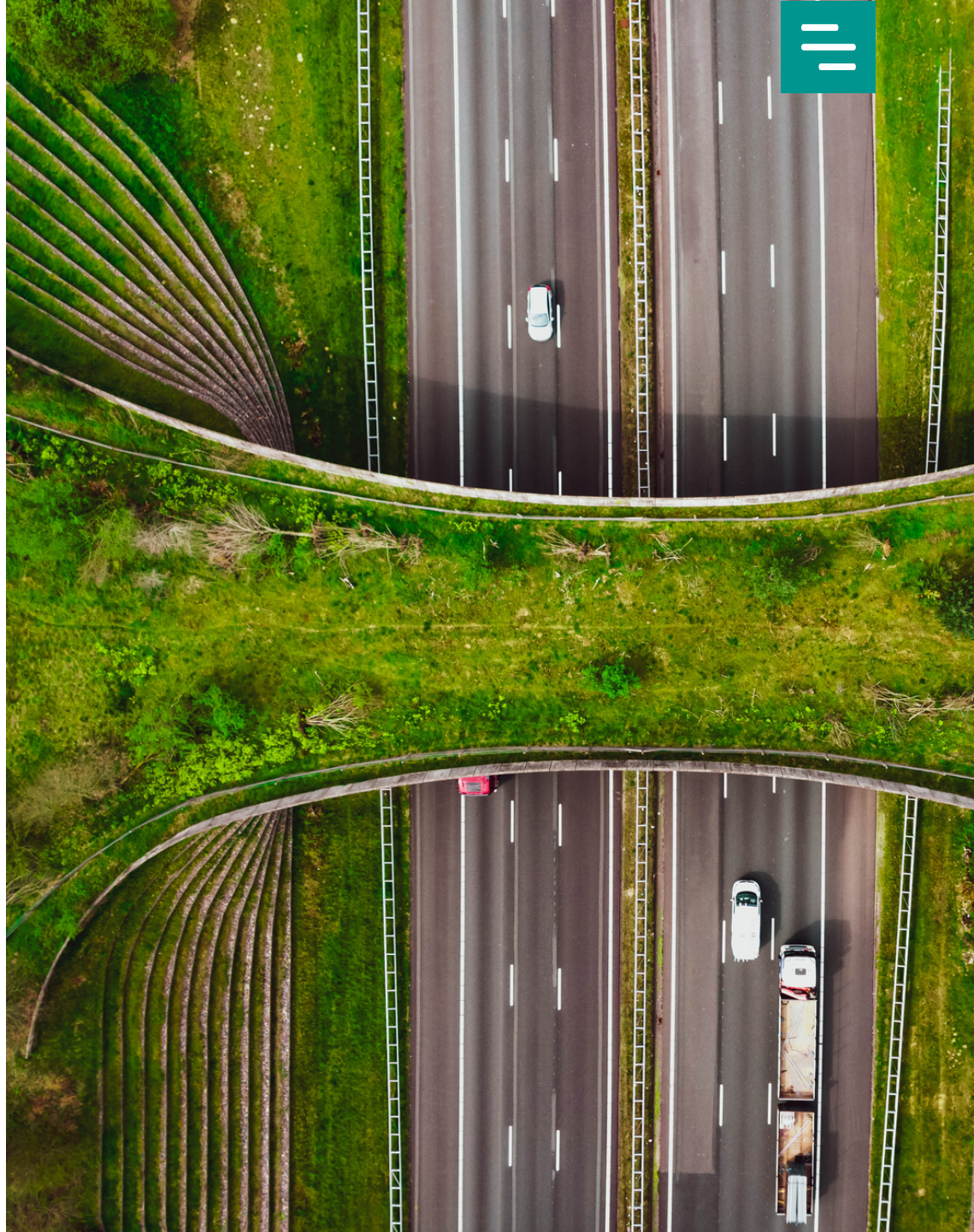
Conclusion

As cyber risk evolves and the cyber insurance market matures, companies should continuously monitor and adjust their cybersecurity controls. When a claim does arise, it is important to engage claims advocates and follow proper steps, such as notifying insurers, brokers, and other stakeholders and maintaining proper documentation.

One of the main cyber claims trends in 2023 was organisations' growing awareness of the importance of cyber insurance to protect against financial loss and improve overall resilience.

This elevated understanding of cyber risk helped lead to a significant rise in the demand for cyber insurance. Brokers and insurers were increasingly called upon to support organisations as they developed risk management strategies, including cybersecurity assessments, employee training programmes, and incident response planning.

As organisations face constantly evolving cyber threats, the demand for comprehensive cyber insurance coverage and efficient claims handling is only expected to grow.



Why Marsh?

Marsh remains committed to helping to quantify your cyber risk exposures with scenario-based loss modeling, benchmarking of potential cyber event losses and costs, consideration of the effectiveness of cybersecurity controls from a financial perspective, assessment of the economic efficiency of multiple cyber insurance programme structures, and help concerning management of your claims, should one arise.

We invest in our brokers and claims handlers and our bespoke Cyber Incident Management (CIM), which provides guidance in navigating cyber incidents. Marsh continuously learns from our clients' needs and questions, as well as from the claims we manage, to support organisations in enhancing their cyber resiliency.

Marsh's Cyber Practice provides organisations with experienced risk advice when managing their exposures.

- In-house legal, technical, and incident response practitioners to help clients before, during, and after cyber events.
- The incident management experience that comes from handling over 1,000 cyber and technology claims annually.
- Digital innovations to augment cyber response programmes.

If you have questions about any of the issues discussed in this report, please reach out to your Marsh representative.

About Marsh

Marsh, a business of Marsh McLennan (NYSE: MMC), is the world's top insurance broker and risk advisor. Marsh McLennan is a global leader in risk, strategy and people, advising clients in 130 countries across four businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. With annual revenue of $23 billion and more than 85,000 colleagues, Marsh McLennan helps build the confidence to thrive through the power of perspective. For more information, visit marsh.com, or follow on LinkedIn and X.

24-351115 - EU