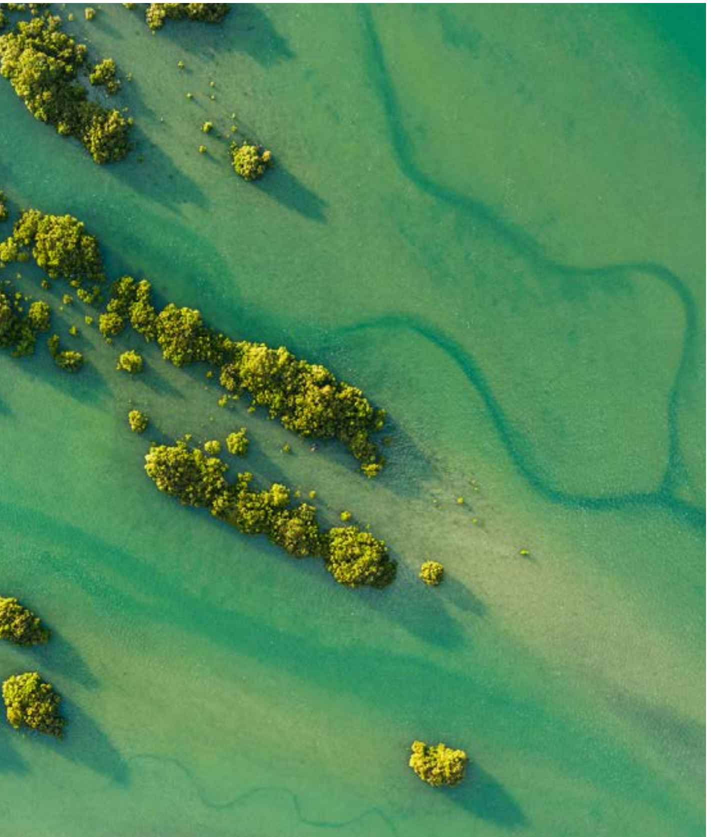
Marsh

The evolution of cyber claims in Europe

Marsh European cyber claims report

Contents



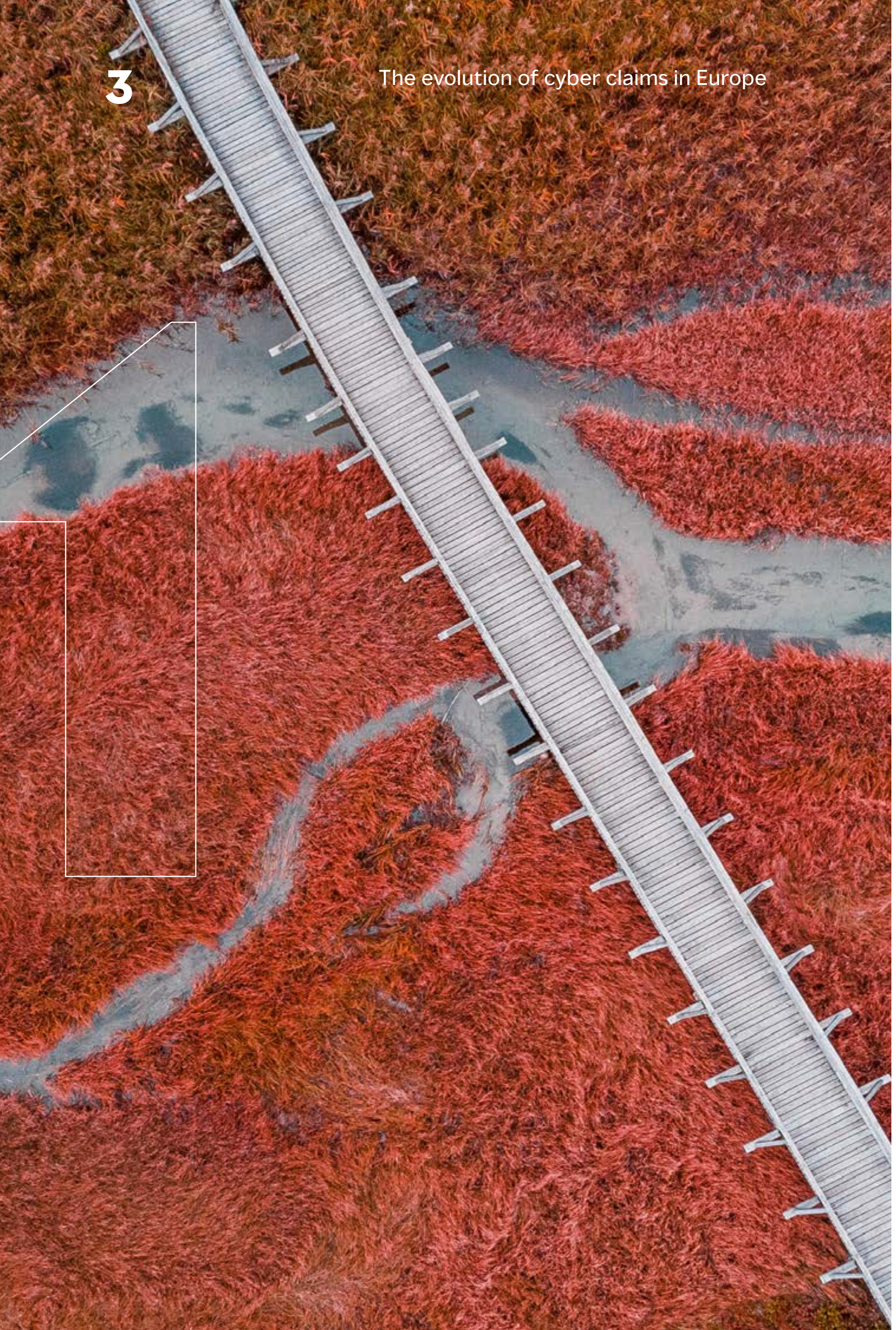
01
03 Key takeaways
04 Introduction

02
05 Cyber claims notifications in 2024
06 CrowdStrike incident raises caution flag
07 Non-malicious incidents increase
08 Threat actors focus on the professional services industry
10 A note on CSA scores
11 Data breaches become more challenging
12 The share of cyber extortion event reports remains stable
13 Ransom payment considerations

03
14 Focus: Claim and incident management insights
15 Navigating a cyber business interruption claim

04
16 Beyond the horizon: New technologies and the cyber incident landscape
17 Quantum computing and implications for cyber and technology risks

05
19 Conclusion



Key takeaways

Understanding cyber claims notification trends helps to inform an effective risk management strategy for one of the signature risks in today's tech-driven society.

Analysis of hundreds of cyber claims notifications submitted to Marsh in Europe in 2024 revealed:

- A significant increase (61%) in cyber claim notifications, compared to 2023.
- Approximately 10% of European clients that purchased a cyber policy reported an event in 2024.
- Claim notifications were driven in part by digital supply chain events, especially the global IT outage on July 19, 2024, that followed a faulty CrowdStrike software update.
- Insured organisations developed more familiarity, trust, and confidence in incident response assistance provided as part of cyber insurance policies. And they generally aligned internal stakeholders — risk management and information security functions — more effectively, contributing to an uptick in notifications and fulfilling insurance policy obligations.
- The share of cyber extortion claims notifications, including for ransomware, stabilised at 18% of all notifications. It remains a top concern given the informational and operational impact these events have on the affected organisations.
- Following claims management best practices, especially reporting potentially impactful incidents early to cyber insurers and to Marsh, was a key initial step enabling long-term claims management and insurance reimbursement success.
- A proactive approach to cyber risk management, including efforts to understand and measure the impact of potential cyber incidents, is key and helps to avoid incidents or to achieve better outcomes when one occurs.

Introduction

In today's digital business environment, technology risk continues to be a critical concern for organisations of all sizes. As a result, the use of cyber risk insurance continues to increase and is a significant strategic component for managing cyber risk. Claims are an essential piece of the insurance framework, fulfilling the promise of protection.

Organisations increasingly use the incident response and claims management benefits that form part of today's cyber insurance policies and help them navigate the complexities of cyber incidents. Given the dynamic nature of losses, it is essential for companies to understand the potential impacts of a cyber incident and the specifics of insurance incident response and claims processes.

In 2024, Marsh's European clients reported a notable increase in incidents, with approximately 10% of our cyber insurance clients notifying Marsh of a potential claim. This was driven by incidents within organisations' digital supply chains, including the global IT outage on July 19, 2024, which stemmed from a faulty CrowdStrike software update.

When assessing organisational risk, it is important to proactively address how future technology risks may amplify existing risk. While cyber extortion incidents have stabilised, they remain a top concern due to their profound impact on affected organisations, encompassing financial, operational, reputational, and potential regulatory consequences.

We hope you find this report useful as your organisation continues to develop and strengthen its cyber risk management strategy.

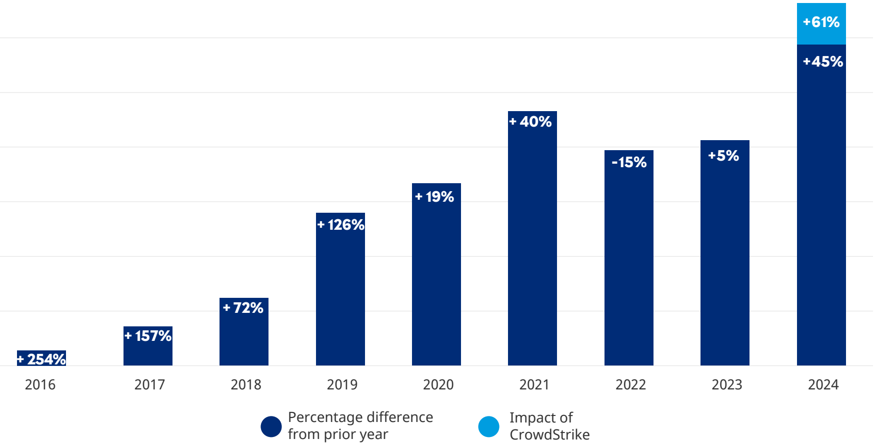
Cyber claims notifications in 2024

Notifications rise sharply

From 2016 to 2021, we observed a steady and significant increase in the number of cyber claim notifications, coinciding with a sharp rise in ransomware threats. In 2022 and 2023, there was a consolidation in the volume of claims notifications, attributed to factors including a more effective cybersecurity posture within many organisations, shifts in the threat actor environment, and geopolitical effects, such as those related to the Russia-Ukraine war.

In 2024, cyber claims notifications to Marsh increased by 61% compared to 2023, as the landscape of cyber threats grew and evolved (see Figure 1). For example, threat actors scaled their efforts, using new technology such as artificial intelligence (AI) to drive efficiency in their criminal activities. Businesses' attack surfaces also increased, given ongoing digitisation and interconnectivity.

01 | Cyber claims notifications in Europe increased sharply in 2024



Source: Marsh

Notifications also increased due to the way that organisations — especially smaller ones (with annual turnovers of up to €250 million) — perceived, valued, and used the additional benefits (and requirements) in most cyber insurance policies, including:

- **Enhanced collaboration:** Improved alignment between information technology, security, and risk management functions has increasingly embedded insurance benefits and placed insurance requirements into incident response plans and procedures.
- **Trust and use of assistance services:** Organisations have become more familiar with and increasingly trust and value assistance services embedded in cyber insurance policies, further encouraging timely reporting.
- **Increased awareness:** Organisations have demonstrated a heightened awareness of the value of cyber assistance and the importance of promptly reporting potential cyber claims to Marsh and their insurers. This is the case even when notifications are precautionary and reported incidents do not lead to an actual loss exceeding the policy retention or deductible.

This proactive approach helps mitigate potential adverse consequences associated with late notifications.

Recent Marsh research has shown that smaller and mid-cap organisations often lag larger ones in cyber incident management maturity.

Cyber insurance is not only an effective way for them to transfer risk, but also to improve their maturity in incident management preparation, testing, and response.

CrowdStrike incident raises caution flag

When looking at the increase in claims notifications in 2024, it’s important to note the effect of the CrowdStrike software update, which caused a global IT outage on July 19, 2024. This non-malicious incident affected millions of Microsoft Windows device users worldwide, including hundreds of Marsh clients.

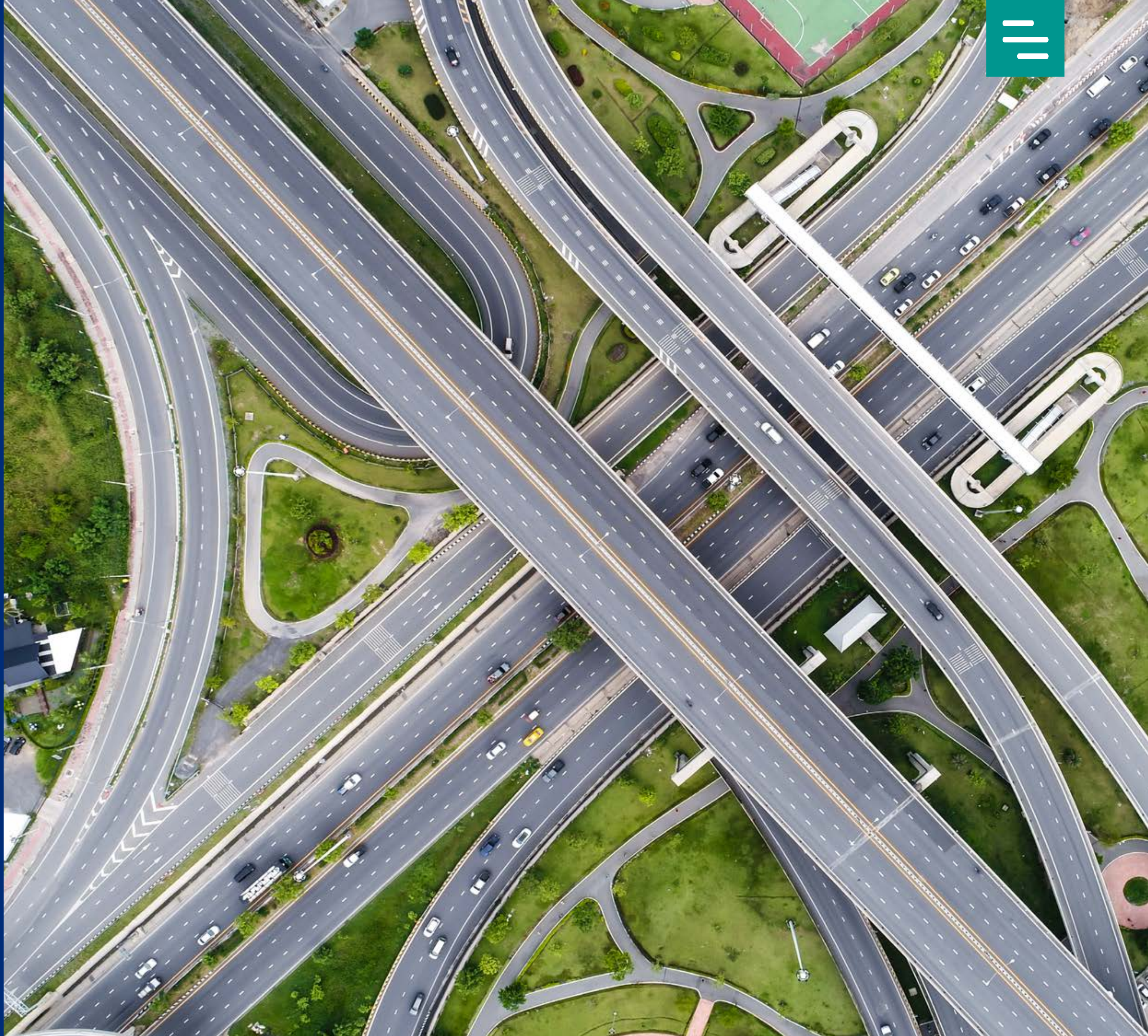
Yet, even when accounting for claims notifications related to this incident, there was still a 43% increase in overall claims volume and frequency compared to the previous year. The overall increase becomes 61% when including notifications related to CrowdStrike.

Given cyber infrastructure’s ongoing innovation, growing sophistication, and critical importance globally, incidents like CrowdStrike are increasingly seen as inevitable. Some view them as more comparable to natural disasters — phenomena we acknowledge, but cannot fully control.

The incident underscored what had already become obvious — it is impossible to completely prevent technology disruptions.

Both malicious and non-malicious events have always existed — for example, the WannaCry ransomware in 2017, the Microsoft Exchange vulnerabilities in 2021, and the MOVEit data breach in 2023 — and will continue to occur. Organisations must learn to accept, anticipate, and effectively manage these disruptions.

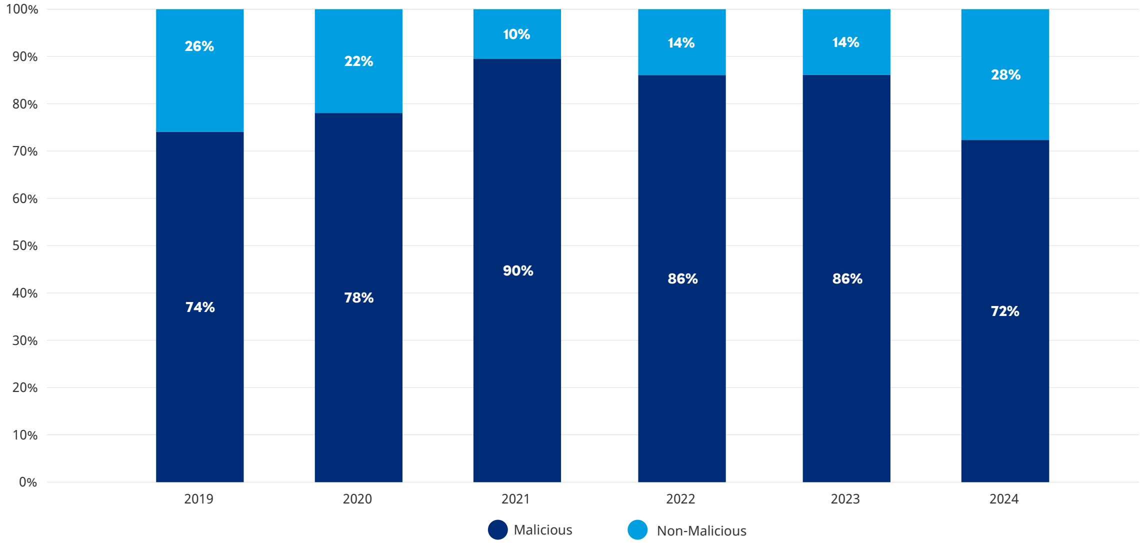
Organisations must recognise that cyber risk is a comprehensive risk management challenge. It requires decision-making during times of uncertainty, often necessitating trade-offs and difficult choices. Embracing this perspective is essential not only for managing insurance claims, but also for navigating the complexities of cyber risk in today’s interconnected world.



Non-malicious incidents increase

The continuing upward trend can be equally observed for non-malicious incidents, which are becoming increasingly significant, making up 28% of the notifications in 2024 (see Figure 2). Operational reliance on technology and the interconnectivity of IT and OT (operational technology) systems are key factors, and non-malicious incidents can be of various natures.

02 | **Percentage of non-malicious events increases**



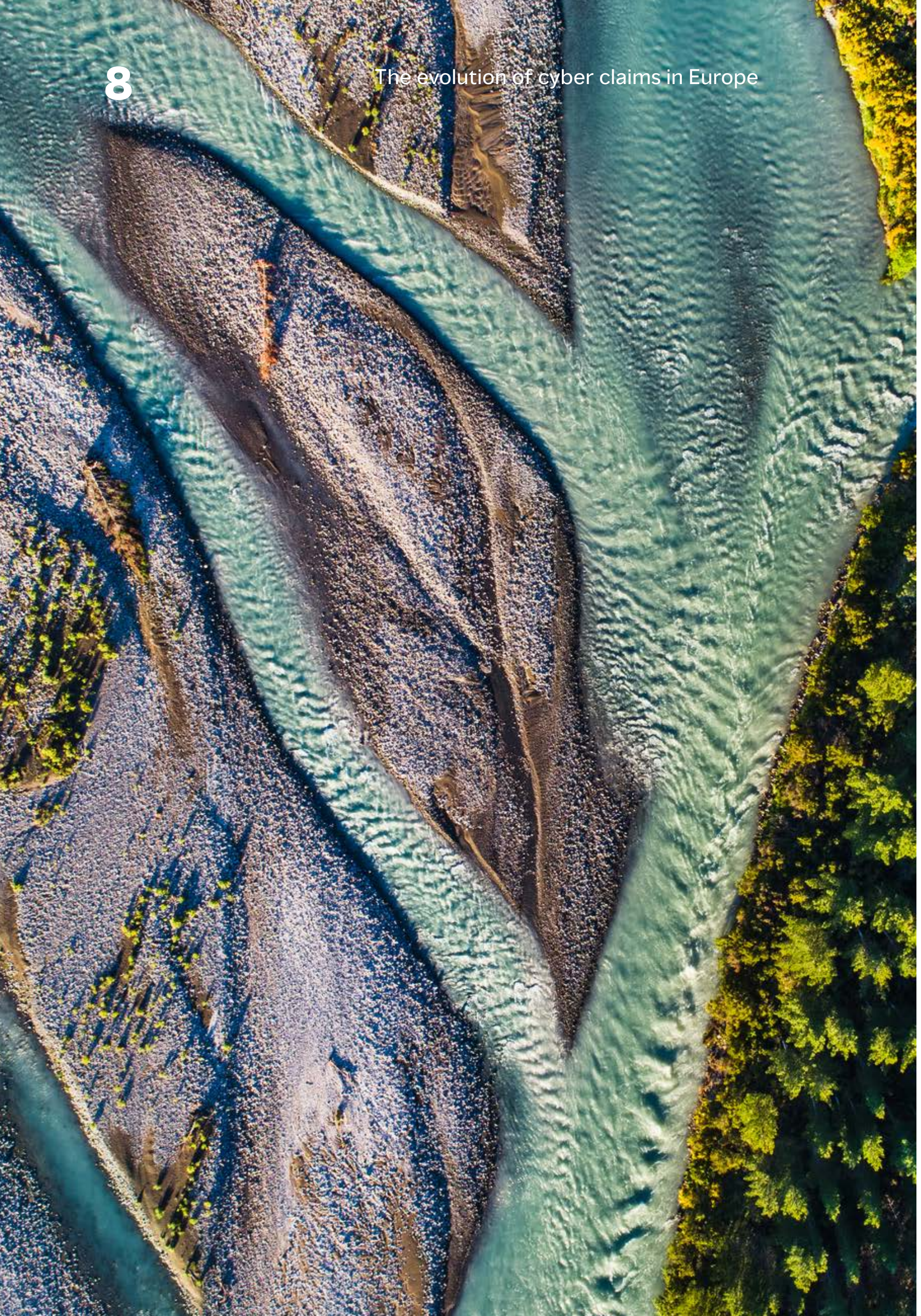
Source: Marsh

Incident origins were both internal and external — including some involving third or fourth parties in the supply chain. The recurrence of such non-malicious scenarios underscores the importance of understanding the broader technological supply chain risks as organisational challenges, not only the cyber risks. Organisations need to review and manage these risks comprehensively, applying a proactive approach to assess them before an incident materialises. Against that background, adopting a comprehensive approach to address the entire digital ecosystem is one of the key new elements in the EU Network and Information Security (NIS 2) Directive.

Non-malicious claim notifications

Incident and claim examples:

- Faulty software updates leading to operational disruptions, as experienced due to the global IT outage caused by the flawed CrowdStrike software update.
- Exposure of personal data of an online platform's business-to consumer due to a software issue that inadvertently displayed customer information.
- Accidental physical damage to a data cable, which led to an outage of key IT servers, affecting the company's business operations.
- Outage of a third-party cloud services/ application provider, which led to operational impacts at the insured company.



Threat actors focus on the professional services industry

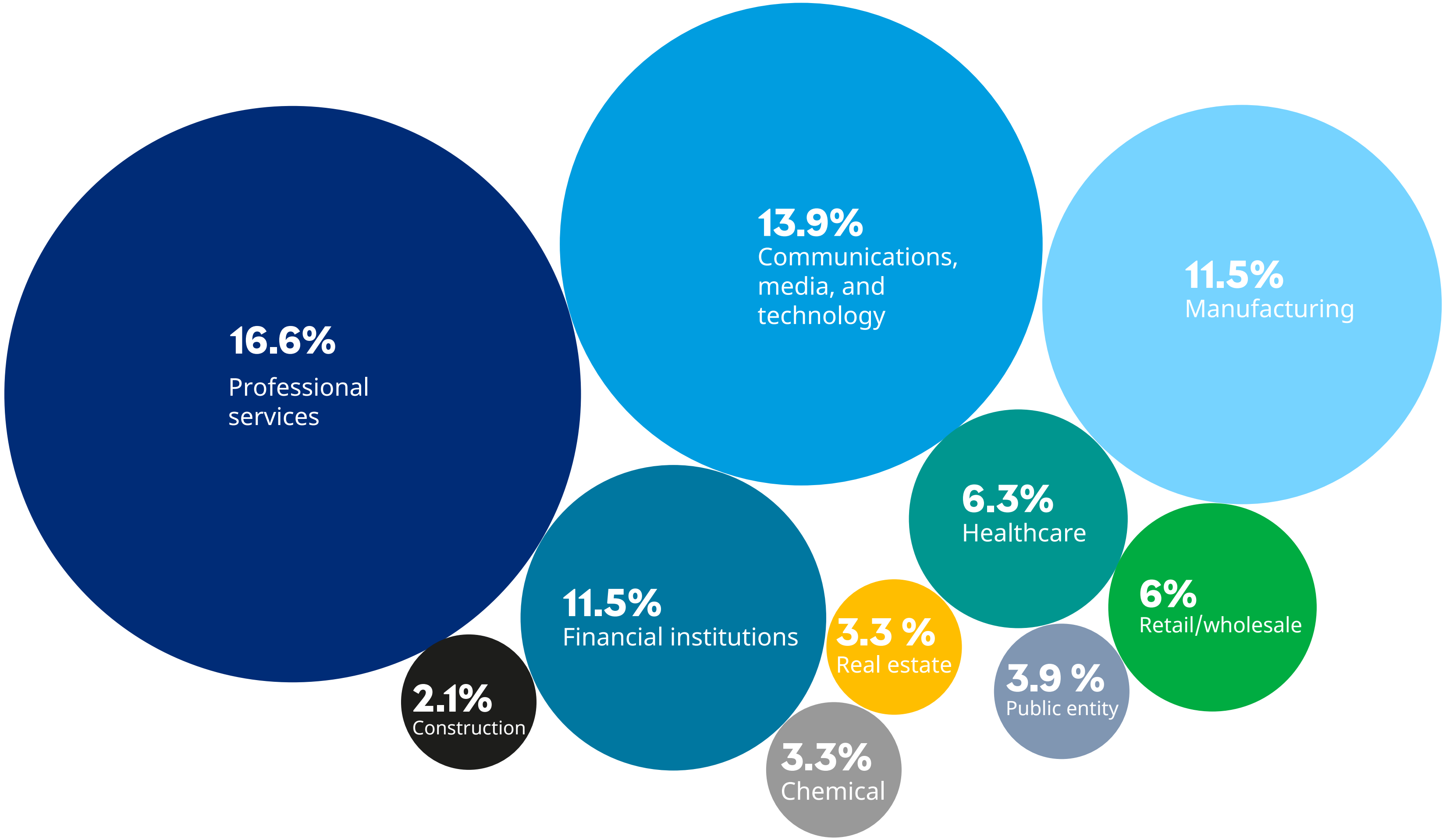
In 2024, professional services clients made the highest number of claims notifications to Marsh, followed closely by the communications, media, and technology (CMT) sector, manufacturing, and financial institutions (FIs) (see Figure 3).

When comparing this distribution year-over-year, both professional services and manufacturing sectors experienced a significant surge in notifications, with numbers approximately doubling compared to 2023. Notably, the chemical industry also experienced a substantial increase in notifications in 2024.

The increase in cyber claims notifications within the professional services, manufacturing, and chemical sectors can be attributed to several interrelated factors, including the rapid pace of digital transformation combined with existing legacy systems. Additionally, the complexity of supply chains in the manufacturing and chemical sectors renders them more vulnerable to cyberattacks.

The rise in cyber extortion incidents has also disproportionately affected these sectors, which, on average, exhibit lower cyber maturity compared to other industries.

03 | The professional service sector generated the most notifications in 2024



Source: Marsh

In contrast, FIs experienced a significant decrease, with claims notifications dropping by approximately one-third. This decline contrasts with the rising claims notifications observed in other sectors. The decrease indicates that FIs have strengthened their defences.

A significant factor in this improvement is the introduction of stricter regulations, including the EU Digital Operational Resilience Act (DORA), which came into force in January 2023, with an implementation deadline of January 17, 2025, which likely compelled FIs to enhance their cybersecurity. According to Marsh Cyber Self-Assessment (CSA) data, the FI industry is more mature than other industries, with a better overall CSA-based cybersecurity maturity score than other industries (see Figure 4).

A note on CSA scores

The Marsh Cyber Self-Assessment (CSA) is a digital tool that examines organisation's cyber risks and streamlines and expedites the process of applying for cyber insurance.

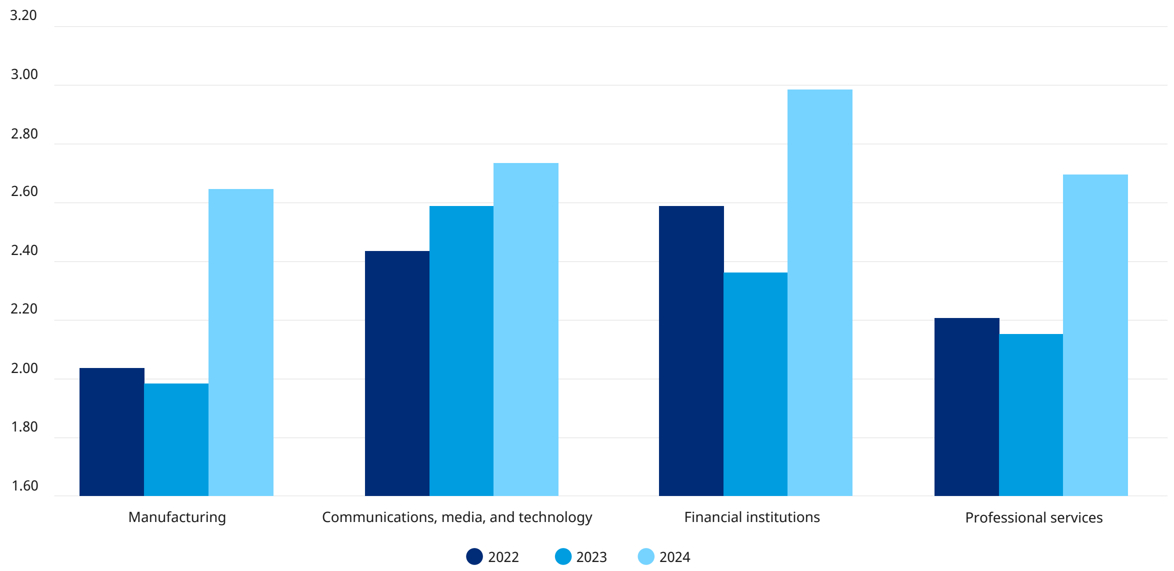
The cybersecurity maturity score is derived from actual organisations' data collected through the CSA. This score ranges from 0.0 to 4.0 and is aligned with the NIST Cybersecurity Framework (CSF).

Cybersecurity maturity scores across all industries demonstrate an overall upward trend; however, fluctuations are evident and can be attributed to several factors.

For example, the apparent decrease in 2023 may not indicate that organisations that previously completed the CSA became less mature, rather it could be that new 2023 CSA entrants with lower maturity levels may have pulled the overall score downward.

These organisations may then have worked to improve their maturity levels in 2024, potentially substantially increasing their scores as depicted in the chart.

04 | Financial institutions show strong cybersecurity in Marsh CSA scoring



Source: Marsh

Moreover, within the notifications from FIs, there is a notable share related to third-party data breaches, typically involving data processors acting on their behalf. This highlights the typical cybersecurity challenges that FIs face, particularly regarding third-party relationships. This underscores the rationale of third-party risk management being one of the cornerstones of DORA.

Both manufacturing and professional services organisations showed substantial increases in cybersecurity maturity levels between 2023 and 2024. Despite this increase, the number of reported incidents continued to rise, likely due to two main factors:

- The cybersecurity maturity of manufacturing/professional services organisations remained lower than that of others, such as financial institutions.
- Manufacturing/professional services organisations increasingly chose to use insurance as part of managing cyber risk, leading to more claim notifications from that industry group.

Data breaches become more challenging

In the past year, the total number of network interruption incident notifications exceeded any other category; however, these were primarily driven by the CrowdStrike incident (see Figure 5). Cyber extortion and data breaches, meanwhile, remain at the forefront of concerns for organisations across Europe.

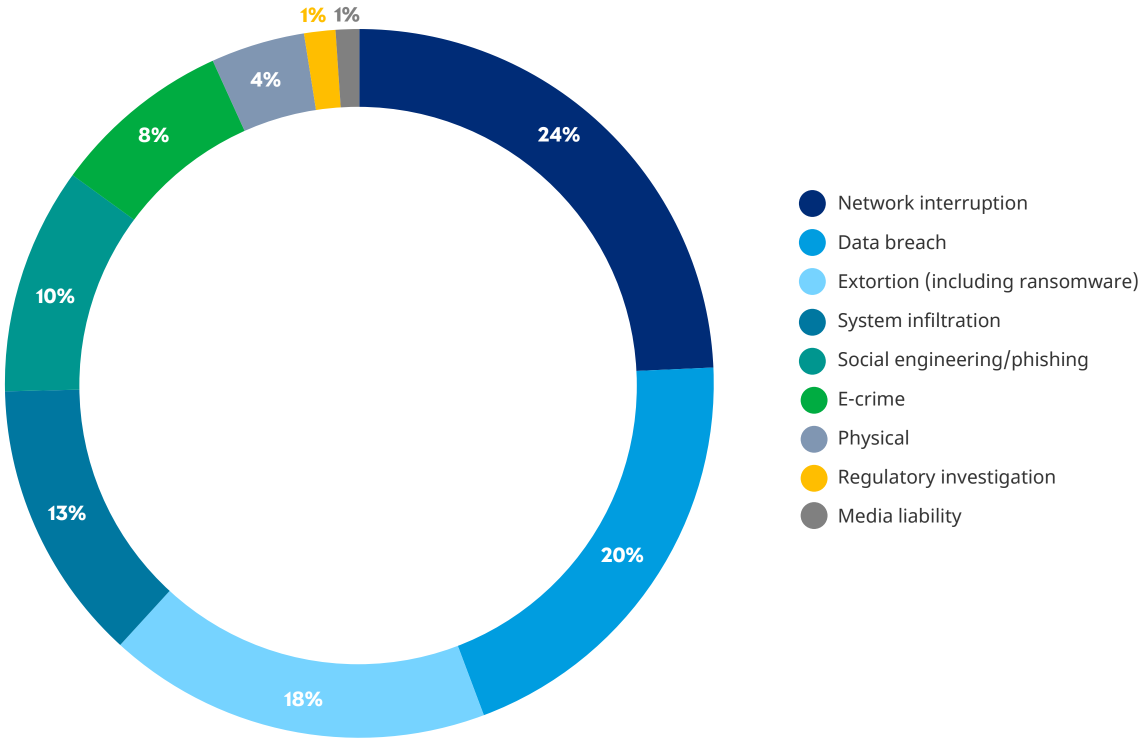
The implications of data breaches are multifaceted, necessitating a comprehensive legal incident response strategy. Many incidents are intertwined with data breach components, including cases of cyber extortion, where threat actors often exfiltrate sensitive information from a company’s network, subsequently threatening to publish this data.

Business-to-consumer (B2C) companies face an elevated risk of large-scale data breaches, which can lead to privacy claims, regulatory investigations, enforcement actions, and ultimately, substantial fines and penalties.

As in previous years, the number of confirmed data breaches remained high. The unique regulatory landscape in Europe, characterised by the General Data Protection Regulation and varying interpretations of its provisions across jurisdictions, underscores the necessity for risk managers to prioritise GDPR compliance both before and during an incident.

As the GDPR evolves, privacy breaches come with additional complexities, especially surrounding the possibility of third parties that have suffered a breach of their personal data to make claims against data owners and processors.

05 | Network interruptions most prevalent incident type in 2024



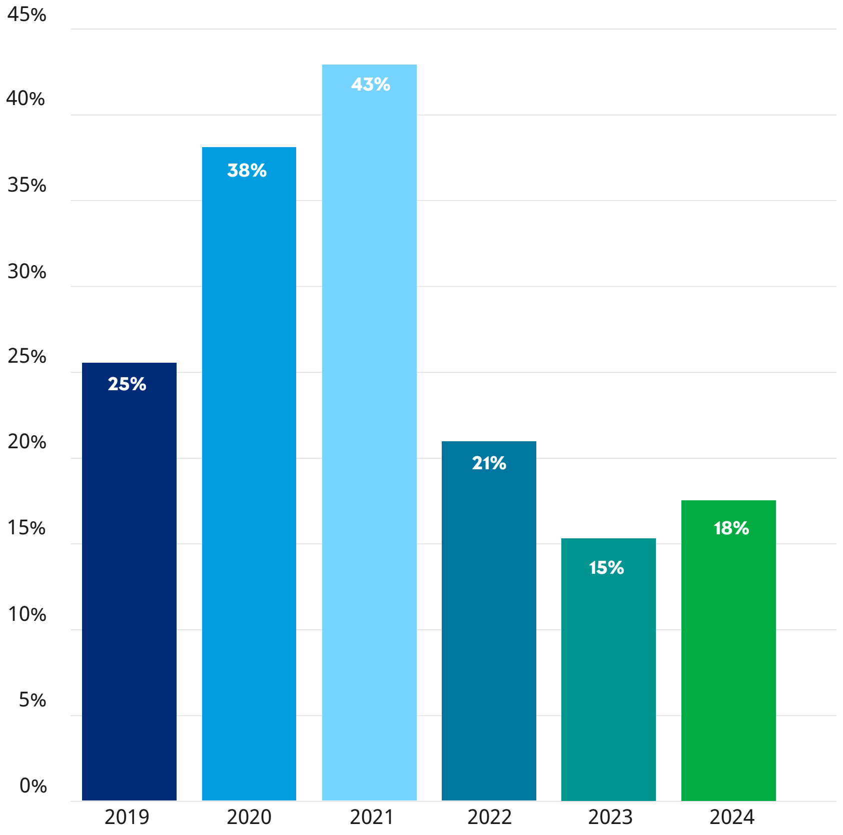
Source: Marsh

The share of cyber extortion event reports remains stable

In total over the past six years, cyber extortion incidents are the most frequently observed incident type. However, for the third consecutive year, they were not the predominant type of incident, maintaining a relative share of approximately 20% of notifications (see Figure 6).

This shift indicates that organisations continue to enhance their cyber maturity, particularly their ability to detect cyberattacks at earlier stages, respond early, and thwart threat actors before they can execute malicious code and encrypt critical systems or exfiltrate sensitive data.

06 | Organisations are more resilient to cyber extortion attacks



Extortion including ransomware as percentage of total incidents

Source: Marsh

Ransom payment considerations

In recent months, as over the past few years, there has been a notable decline in ransom payments among organisations, which can be attributed to several factors.

- **Resilience:** Organisations have enhanced cyber resilience through increasingly robust backup security measures, designed to safeguard against the deletion or encryption of data. Also, organisations are improving backup recovery processes, leading to faster recovery times and less data loss should IT systems be encrypted. This progress enables organisations to lower the operational interruption to the business processes.
- **Threat actor tactics:** There is an ongoing shift in the tactics employed by threat actors. Increasingly, they are focusing on data exfiltration rather than traditional ransomware encryption. This shift contributes to the decline in ransom payment rates, as organisations are more reluctant to engage with, or ultimately pay, threat actors when these have solely stolen and threatened to publish data without a need to recover systems with decryption keys provided.
- **Legal shift:** The legal risk of making ransom payments is increasing. Many governments, such as of Australia and the UK, have openly discussed a partial ransom payment ban. And the French Interior Ministry's Orientation and Programming law (LOPMI) imposes an obligation on companies that are victims of malicious computer attacks to file a complaint to preserve their right to compensation under their insurance policy, including cyber extortion. Making ransom payments to threat actors imposes a legal risk to the payee organisations' directors and officers, since threat actors may be sanctioned entities/persons, which would make a ransom payment an unlawful act.
- **End results:** Cyber extortion consultancy companies have reported a decrease in the reliability of threat actor groups to fulfil their promise after receiving a ransom payment, both regarding the provision of a functioning file decryption key and to not leak or otherwise sell previously exfiltrated data.

Focus: Claim and incident management insights

As the nature of cyber incidents evolves, it is essential for insureds and insurers alike to recognise that the changes directly affect cyber insurance claims. This includes shedding light on the common challenges and unique aspects encountered in cyber claims management, aiming at ensuring a more efficient and effective claims resolution for all parties involved.

Aligning insurers early for effective claims management

When a claim affects multiple layers of an insurance programme, aligning the various stakeholders — including, potentially, multiple insurers — can be a complex undertaking requiring involvement of all relevant parties from the outset.

Ensuring that information is shared in a timely, structured manner enables insurers to collaborate effectively, for example, nominating a single loss adjuster; streamlining communication; and facilitating an efficient claims process. Using harmonised and secure communication streams and platforms enhances the clarity and organisation of information shared among insurers.

Navigating industry-specific loss scenarios

Cyber incidents can lead to losses that are specific to particular industries. For instance, a cyber business interruption incident for a client in the logistics sector led to detention and demurrage costs — charges incurred for the extended use of containers after unloading and delays in cargo pickup.

To navigate industry-specific issues, it is important to substantiate any increased costs from an incident and clearly articulate the causal chain from the incident to the business event and, ultimately, to the financial loss. Expert cyber claims specialists can support organisations by providing best practices and supporting the effort to document and investigate such losses to maximise insurance recovery.

A best practice is to address such issues proactively, planning for them prior to an incident and subsequent loss. By conducting a cyber risk assessment and business impact analysis (BIA), organisations can identify dependencies and ensure insurance programmes effectively cover potential losses.

Understanding the complexity of cyber business interruption claims

Cyber business interruption (BI) claims can be complex, presenting challenges in assessing and “proving” them to insurers. This complexity is heightened when best practices for collecting facts, gathering evidence, and documenting the impact of a BI incident are not implemented in the early stages of an incident. Attempting to reconstruct events after the fact can be daunting, and timely involvement of insurers and specialists is often overlooked. Understanding and substantiating complex issues retrospectively often involves a great deal of effort and frustration — engaging specialists early on can be invaluable. Timely and effective fact-gathering, combined with a structured approach to preparing proof of loss, has proven essential in many high-value claims. Clients that have taken a proactive approach typically experience smoother claims management and successful reimbursement processes.

Navigating a cyber business interruption claim

To successfully navigate a business interruption claim in the wake of a cyber incident, several key factors should be considered:

Choose the indemnity period wisely: When purchasing or renewing cyber insurance, selecting an appropriate indemnity period is essential. And when an incident occurs, businesses must evaluate the duration of the disruption and its economic impact to align their coverage definitions with the actual losses incurred. This strategic choice can significantly influence the recovery amount.

Maintain detailed records and documentation: Keeping accurate records of all costs and related expenses is crucial. Establishing a specific cost centre allows businesses to effectively control and identify the economic impact of the cyber incident. Documentation provides vital evidence during the claims process.

Consider increased costs of working: In some cases, incurring additional costs to minimise disruption can be beneficial. This proactive approach can help reduce the overall period of interruption and mitigate turnover shortfalls. Examples of increased costs of working include staff compensation for overtime work to accelerate the IT recovery, and hiring temporary workers to catch up on lost production capacity.

Account for supply chain disruptions: Cyberattacks can cause ripple effects throughout the supply chain. Assessing potential business interruption losses resulting from these disruptions is crucial, as they can contribute to the overall claim.

Evaluate third-party liabilities: It’s important to understand the potential liabilities associated with third parties affected by a cyber incident. This evaluation helps identify obligations to customers or partners and ensures that all aspects of the incident are considered during recovery.

Addressing multi-jurisdictional claims challenges

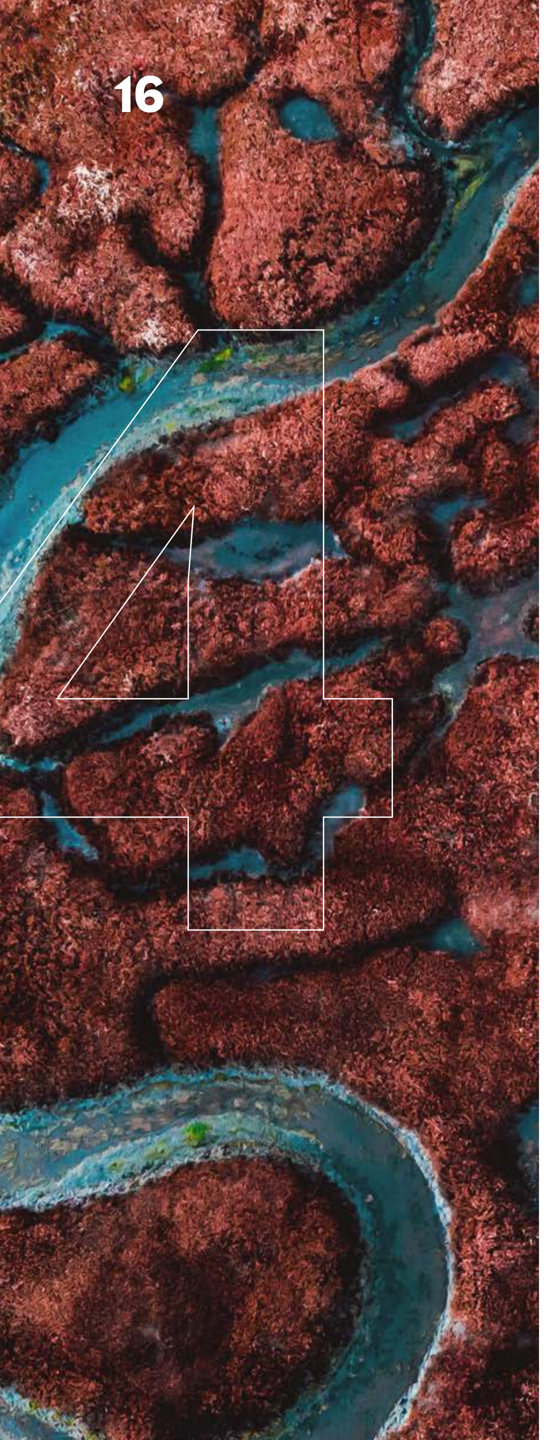
Multi-jurisdictional claims present another layer of complexity. Many European-headquartered organisations operate subsidiaries worldwide, and interconnected IT infrastructures and supply chains can lead to adverse effects.

Claims involving US subsidiaries are particularly intricate due to the legal landscape, especially concerning third-party liability and the application of legal privilege during incident response and claims management. A thoughtful and strategic approach is necessary to navigate these complexities.

Clear communication and established working principles among involved stakeholders are crucial, particularly when a non-headquarters subsidiary is materially affected. In cross-border claims, especially those impacting US sites, Marsh can leverage its extensive network of cyber incident response and claims specialists to provide local expertise and best practices, aiming for the best possible outcome for the insurance claim.

Proactive strategies make for effective claims management

A proactive and informed approach to cyber claims and incident management is essential. By understanding the unique challenges and leveraging the expertise available, organisations can more effectively navigate the complexities of cyber incidents, ensuring that they are well-prepared to manage claims and mitigate potential losses.



Beyond the horizon

How new technologies will impact the cyber incident landscape

The impact of AI on cyber risks: Focus on phishing

As technology advances at a breakneck pace, the implications of artificial intelligence (AI) for cybersecurity become increasingly significant. The World Economic Forum's Global Risks Report 2025 highlights a concerning trend: Cyber risks are escalating, with AI both a tool for protection and a weapon for exploitation. This duality presents a complex challenge for individuals and organisations alike. The Global Risks Report underscores that as our reliance on digital communication grows, so does the sophistication of cyberattacks.

Cyber risks have evolved dramatically in recent years, with phishing attacks emerging as one of the most prevalent attack vectors for a wide range of incidents and claims, encompassing ransomware, espionage, and wire fraud. Phishing involves cybercriminals impersonating legitimate entities to trick individuals into revealing sensitive information, such as passwords or financial details. Also, cybersecurity vendors report a continuous rise in the proportion of incidents attributed to social engineering, now accounting for 30% or more of all reported incidents.

AI plays a pivotal role in this evolution, enabling attackers to create highly personalised and convincing phishing schemes.

According to a recent study, AI-driven phishing attacks have surged dramatically. In the past year alone, there has been a reported increase of over 300% in successful phishing attempts attributed to AI-enhanced tactics. Furthermore, AI-generated phishing emails are 10 times more likely to be opened than traditional phishing attempts, highlighting the urgent need for enhanced cybersecurity measures.

AI technologies can analyse vast amounts of data to craft messages that resonate with specific targets, making it increasingly difficult for individuals to discern between legitimate and malicious communications. For instance, AI can generate emails that mimic the writing style of a trusted colleague or create fake websites that closely resemble real ones.

Cybercriminals can leverage AI to automate attacks, create deepfakes, and develop malware that adapts to security measures in real-time. This amplification of existing risks poses significant challenges for individuals and organisations, as traditional cybersecurity measures struggle to keep pace with the evolving threat landscape.

While AI offers the potential to enhance cybersecurity through improved threat detection and response, it simultaneously amplifies existing risks, particularly in the realm of phishing. The implications highlight the need for a proactive approach to cybersecurity that includes both technological solutions and education and awareness training to empower individuals.

As we look to the future, collaboration between technologists, policymakers, and the public will be essential to navigate the complexities of this new digital frontier and mitigate the risks associated with AI in cybersecurity.

Quantum computing and implications for cyber and technology risks

Quantum computing promises to revolutionise industries, economies, and operations across a wide swath of industries, bringing diverse opportunities such as improving batteries, optimising traffic flow, modelling finances, developing pharmaceuticals, forecasting weather, and further developing technologies from virtual assistants to video games.

While the time horizon for the transition to the quantum-world is unclear, the potential risks are increasingly concerning to cybersecurity experts. For example, quantum computing would override most current encryption methods, threatening today's information, digital infrastructures, and communications.

Another significant threat associated with quantum computing is known as an HNDL (harvest now, decrypt later) attack. In this scenario, malicious actors would intercept and store encrypted data today, confident they will be able to decrypt it once quantum computers advance. This means that sensitive information, such as military secrets, personal data, financial records, and intellectual property, could be at risk for years before it is accessed.

Affected organisations could be incurring multiple types of losses, including, but not limited to:

- Direct financial losses for incident response and breaches of confidential information, such as related to mergers and acquisitions or other strategic initiatives.
- Third-party claims or regulatory enforcement actions resulting from the data breach.
- Intellectual property theft and/or reputational damage leading to loss of business and long-term strategic disadvantages.

The potential for such breaches underscores the urgency for organisations to assess and address the associated risks and operationalise the implementation of quantum-proof encryption.

The roadmap for quantum-proof encryption is a strategic journey, not a race, as it implies different actions to tackle before, during, and after implementation. Developing a structured approach for identifying, measuring, and managing risks and building a technology risk resilience-by-design approach requires organisations to broaden their focus from improving cybersecurity to advancing cyber and technology resilience.

A first step is to conduct a risk assessment to understand the adverse impact that threats associated with quantum computing could have. This would include assessing critical data that may be at risk and identifying current cryptographic methods throughout the company.

A second step is to quantify the risk of emerging and frontier technologies and enhance the ability to evolve in response to emerging threats. Developing advanced cyber and technology risk assessment and quantification will be paramount to maintaining a resilient security posture, and to defining a complete risk treatment strategy roadmap. Data derived from a quantification exercise will enable risk and information security managers to properly balance and align risk mitigation controls and risk transfer options, aiming for the most effective capital allocation while defining and implementing the quantum strategy.

According to recent studies by the World Economic Forum on Quantum Computing, including its implications on the financial sector, additional considerations and keys to eventually managing quantum risks include:

- **Building/upskilling the workforce and raising awareness:** It is crucial for organisations to be prepared to identify the opportunities of quantum applications and to understand their associated risks and potential gaps. The uncertain timeline of a quantum reality, combined with the challenging transition to new security models, may prevent industries from investing in quantum security.
- **Collaborative approach:** Regulators should provide guidance as a catalyst for implementing harmonised quantum-secure systems, in collaboration with private institutions and academia to assure a forward-thinking approach on requirements.
- **Agile cryptography:** There are two different classes of solutions that should be combined, when available, to cope with quantum cyber threats:

  1. Quantum resistant algorithms (also known as post quantum cryptography) that aim to replace existing algorithms vulnerable to quantum threats to new ones. These algorithms are entirely implemented on classical computers and do not involve quantum technology. A few post-quantum algorithms have been standardised by the National Institute of Science and Technology (NIST).
  It is paramount to prioritise parts of the organisation that handle critical data or are integral to operational stability and provision of essential services to define a roadmap to migrate to a post-quantum cryptography.

  2. Quantum cryptography, which includes quantum random number generation for key generation (available for smartphones, computers, and data centres) and quantum key distribution, that requires physical infrastructure and is operated mainly by telecommunication organisations.

While the rise of quantum computing presents significant challenges, it also offers an opportunity for organisations to innovate and strengthen their cybersecurity measures. By understanding and managing the risk implications of quantum technology, we can navigate the complexities of this new era and ensure a secure future for all.

Conclusion

Following a busy 2024, the number of cyber incidents and claim notifications in Europe is expected to continue increasing, adding to the need for organisations to adopt a strategic approach to technology risk. This involves understanding and quantifying risks and making informed decisions based on objective and data-driven insights to enhance risk management.

As the digital landscape evolves, organisations must remain vigilant and informed about new and evolving cyber risks. A proactive stance is needed to navigate the complexities of cyber threats, ensure that they are prepared for potential incidents, and to build an effective risk transfer strategy. A particular emphasis should be placed on digital supply chains, where organisations must develop and implement robust plans and response strategies for cyber incidents.

In the event of a severe cyber incident, the services typically provided by cyber insurers can be a valuable tool. To maximise the benefits of these services, it is important to adhere to best practices in cyber insurance claims management. By doing so, organisations can facilitate a smooth and positive outcome for their claims, ultimately reinforcing their cyber resilience.

Overall, the combination of strategic risk management, continuous awareness of the evolving digital landscape, and effective use of cyber insurance services are key to successfully navigating the future of cyber claims.

Why Marsh?

Marsh remains committed to helping to quantify your cyber risk exposures with scenario-based loss modelling, 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, 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.

This is a marketing communication.

Marsh is a business of Marsh McLennan. This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.