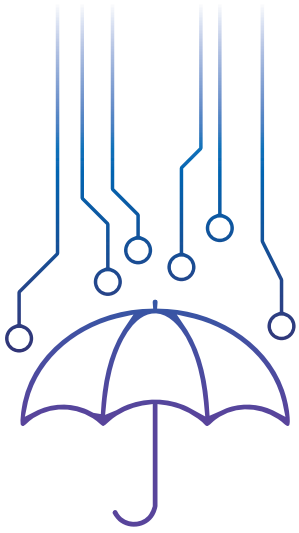
DEMYSTIFYING CYBER INSURANCE

TODAY'S TRENDS & TOMORROW'S CHALLENGES

FERMA
Anticipating changes
Shaping the future

Marsh

HOWDEN



1. INTRODUCTION

1.1. Background

In today's increasingly digital world, **cyber resilience is essential for organisations of all sizes and in all sectors**. Indeed, Risk Managers worldwide have identified cyberattacks as the most critical risk threatening their activities since 2020 (see: FERMA Global Risk Managers Survey 2024[1]). As technological acceleration increases the effectiveness of malicious cyber incidents and companies' overall cyber risk exposure, being unprepared in the digital realm should be considered an existential risk.

Cyber resilience is achieved through the calibrated synthesis of risk management, business continuity and cybersecurity - which is essential to reduce the likelihood and severity of cyber risks. It must be kept in mind that there is no such thing as a 'risk-free' organisation: when an incident does occur, insurance is a critical tool to help companies recover and mitigate any long-lasting impact on their operations. This report focuses on the role of cyber insurance as part of a comprehensive resilience strategy – while reaffirming that risk management and risk transfer must always be seen as complementary.

FERMA, Marsh, Howden and other industry stakeholders in 2023 jointly published a report entitled Cyber Insurance Dialogue: How Europe can lead the way to cyber resilience with the aim of addressing the challenges faced by all participants in the cyber insurance chain. This paper is the continuation of FERMA's longstanding commitment to constructively engage with all stakeholders to build a well-functioning and affordable cyber insurance market contributing to the overall resilience of the EU economy.

1.2. Why this new report?

A pervasive scepticism plagues the risk management community on the topic of cyber insurance. Interviews conducted by FERMA reveal that European Risk Managers harbour concerns regarding:

- Exclusions, notably for war and systemic risks, but also the exclusion of cyber risks from traditional policies (e.g. property, BI) as (re)insurers are perceived to be moving towards broader exclusions.

- Coverage gaps emerging from the interaction of disparate traditional insurance policies and cyber-specific insurance policies.

- Claims management, especially a lack of clarity around triggers and disputes around claims payments.

This perception is undoubtedly a contributory factor to the low cyber insurance penetration rate in Europe: according to Marsh, only 15% of SMEs purchase cyber insurance, despite

1 - FERMA Global Risk Manager Survey Report 2024.

the fact that they represent 99% of all European companies. This low cyber insurance take-up rate is a key driver of the cyber insurance gap, which the Global Federation of Insurance Associations (GFIA) estimated in 2023 to be more than $900 billion per annum globally, with Europe accounting for 23% of that total (i.e. $207 billion per annum[2]).

At the same time, Risk Managers are increasingly concerned about insurance gaps: 53% fear that some of their activities might become uninsurable, with cyberattacks, digitalisation risks and technological threats all considered to be in the top five areas where coverage is believed most likely to be withdrawn[3].

However, we believe that **this scepticism does not fully reflect the current state of the cyber insurance market**. Although challenges undeniably remain, a lack of awareness and understanding about cyber insurance products contribute to underestimating the value that cyber insurance can bring to organisations, limiting the level of resilience that European businesses could achieve.

It is also important to acknowledge that concerns differ depending on the type of organisation. Large corporates often point to market volatility, high deductibles, complex claims processes and insufficient compensation for exclusions in traditional policies. SMEs, on the other hand, frequently face challenges such as lack of product transparency, limited guidance, high entry barriers due to technical requirements and uncertainty about the actual value of coverage relative to cost. These different perspectives must be taken into account when discussing the role of cyber insurance in a resilience strategy.

In some cases, alternative risk financing models or internal preparedness measures may prove more efficient. Nevertheless, it is important to emphasise that, **when used appropriately, cyber insurance can make a valuable contribution to resilience**. It not only provides financial protection, but also access to specialised services such as incident response, forensic analysis and crisis communication. For SMEs, this can be a decisive added value to enable them to remain operational in the event of a cyber incident.

1.3. Aim of this report

This report is directed towards the key stakeholders in the cyber insurance market: (re)insurers, brokers, Risk Managers and corporate insurance buyers more broadly. Its aim is twofold:

1. To provide an overview of current state of the cyber insurance market, as well as the trends that are shaping it, in order to develop clearer understanding of what kind of risks it can cover and how.

2. To address existing challenges, by clarifying misunderstanding and providing recommendations to ensure that all stakeholders can benefit from a well-functioning and affordable cyber insurance market.

In addition, the report includes practical case studies to illustrate typical challenges and solutions.

2 - GFIA (2023). Global protection gaps and recommendations for bridging them, "Report extract: Cyber protection gap"
3 - FERMA Global Risk Manager Survey Report 2024.

2. STATE OF PLAY IN THE EUROPEAN CYBER INSURANCE MARKET

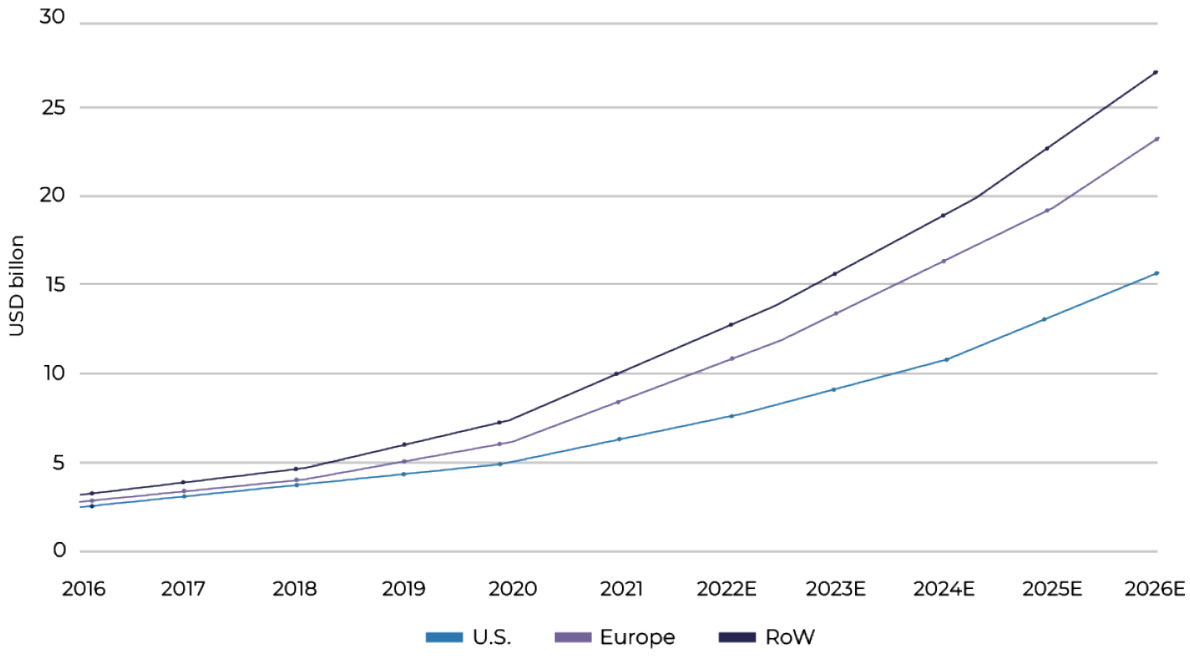
2.1. Key trends and figures

2.1.1. Historical trends

Late 1990s-2020: Market Expansion.

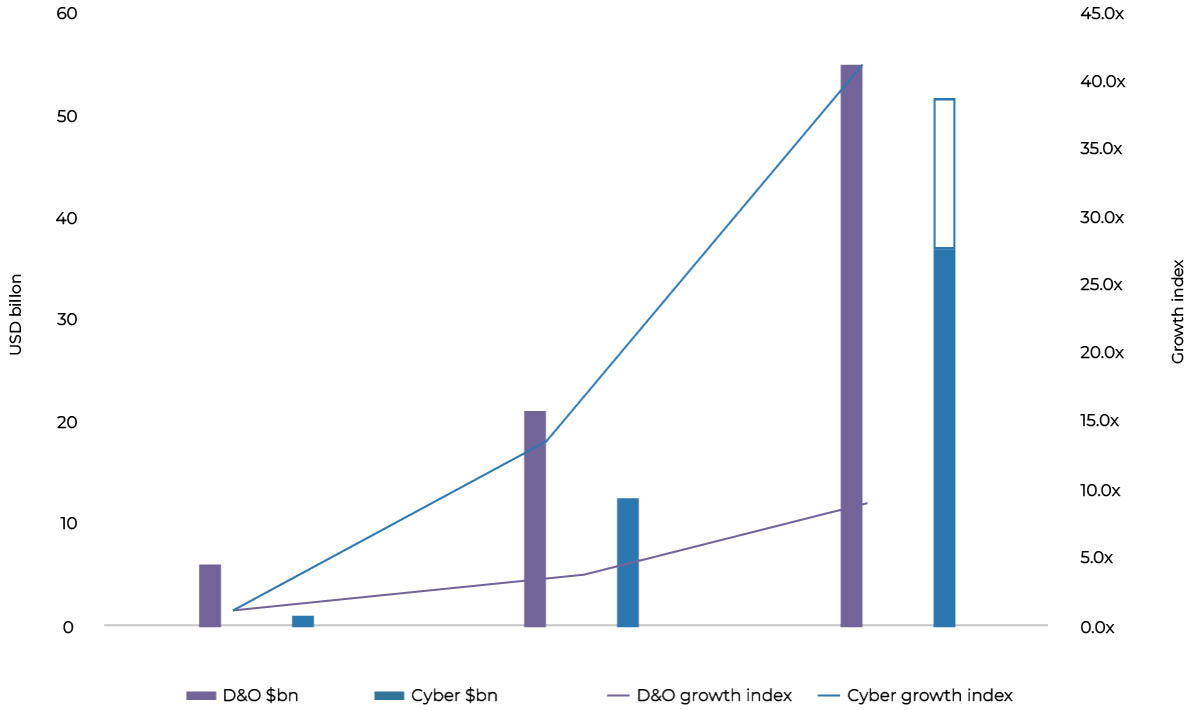
Since its inception, cyber insurance has been both attractive to and feared by insurers. However, since its infancy until 2020 the number of insurers and clients grew rapidly. Despite there being no claims history and limited knowledge of the risk involved, insurers around the world rushed to market this product. (See chart Figure 1 and Figure 2)

Figure 1 - Cyber insurance saw exponential growth in gross written premiums (GWP), especially in the U.S., Europe, and the rest of the world.



Source: Howden

Figure 2 - Compared to others growing lines like Directors & Officers (D&O), cyber insurance grew rapidly from 2015 to projections for 2025.

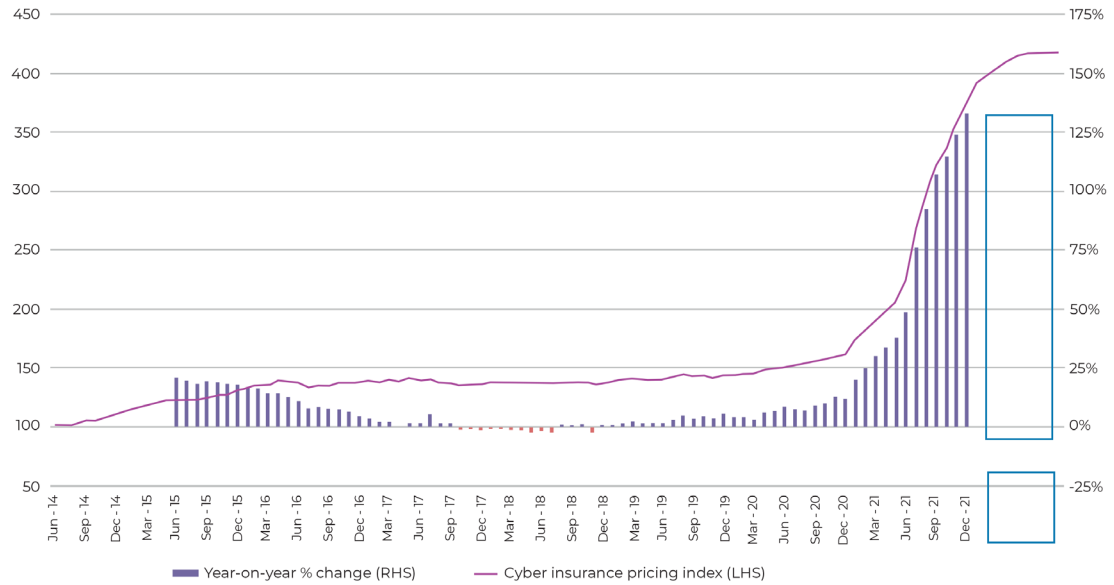


Source: Howden

2020-2023: Turning Point

Cyber Insurance rates skyrocketed due to an increase in the incidence of Ransomware as a Service (RaaS). attacks. This led to a contraction in the market, with notable increases in retention and price together with restrictions in cover, capacity and appetite. During this period, market players learned relevant cyber controls to mitigate ransomware claims and impact. (See chart Figure3)

Figure 3 - The rise of Ransomware as a Service (RaaS) caused a sharp increase in claims ratios, which led to market contraction and also in premiums.



Source: Howden

2024- Today: Back to a buyer-friendly market

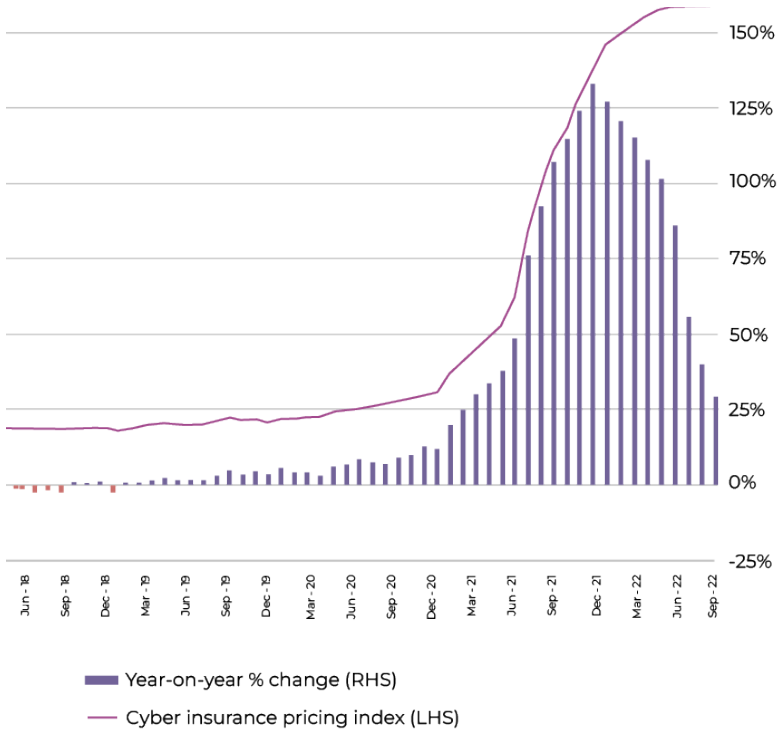
Companies around the world increased their cybersecurity spending, leading to a lower frequency and severity of claims and a return to profitability for insurers. The market is now soft again and clients are experiencing a "return on investment" in their cybersecurity spend in the form of, lower premiums and retentions, and broader terms and conditions. (See chart Figure 4)

In 2024, Europe represented about $3.9 billion in cyber insurance premiums (23,62% of the global cyber insurance market), of which $2.2 billion were collected in continental Europe and the remaining $1.7 billion in the United Kingdom (retail and wholesale).

Across European industries, buyers of cyber insurance products operate in financial services (15% of the market), manufacturing (14%) and services (12%). By contrast, the healthcare sector represents a negligible share of the European market (2%), especially when compared with the United States and Canada (11%).

Europe is one of the fastest growing cyber insurance markets, estimated to account for 25% of the cyber premium growth between 2024 and 2030, with the United Kingdom estimated to account for an additional 9%[4].

Figure 4– Once clients increased cybersecurity investments, resulting in fewer and less severe claims, insurers experienced improved profitability, and the market cycle shifted back to favourable conditions for clients.



Source: Howden

4 - Howden, Cyber insurance: Risk, resilience and relevance

2.1.2. Current market dynamics

Capacity, Retention & Rates

Currently, it appears that existing insurers are offering larger lines per risk. New entrants are causing increased competition for primary business and even more in excess lines - including for SMEs. As a consequence, retention levels have dropped significantly. Many clients have purchased higher limits and have adjusted their programmes and retentions. Rates show double-digit decreases in primary layers and even more aggressive pricing in excess layers. The current soft market reflects improved cyber risk management and stronger security measures, an increase in cyber risk management and security measures among buyers of coverage.

Following the previous hard market, recent advancements in aggregation modeling gave buyers greater confidence in deploying capital through insurance. After several years focused on portfolio remediation, carriers returned to a growth phase. This renewed optimism, combined with the entry of new capacity into the European market, has intensified competition and led to an overall reduction in premiums. Overall, cyber insurance rates decreased for the first half of 2025 with an average reduction of 10% to 15% and in some cases more than 30%. Meanwhile, 63% of clients experienced a discount in their premiums, considerably higher when compared with H1 2024[5].

In Q3 2025, cyber rate reductions accelerated, averaging around 15%, with variations depending on industry, risk quality and client revenue bands. Larger enterprises with enhanced security controls have experienced even greater rate decreases. European companies are capitalising on this softening market by purchasing higher coverage limits and adjusting their retention levels. Coverage restrictions are being lifted as underlying risk quality improves and insurers become more flexible, allowing for broader coverage options. Additionally, the underwriting process has become less complex, with underwriters gaining greater confidence from the more detailed information provided in application forms.

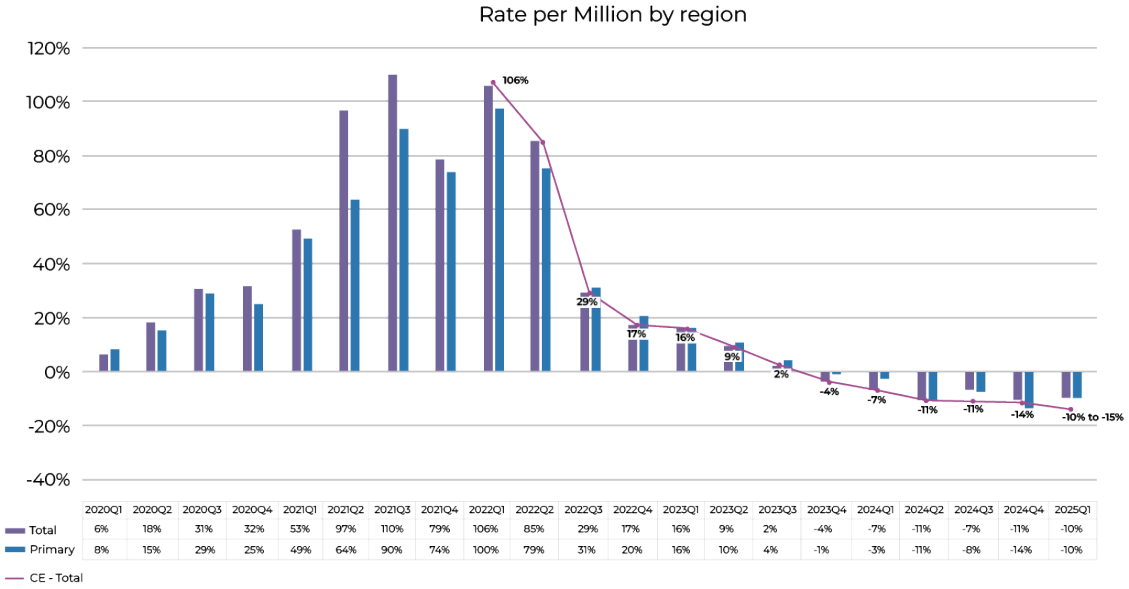
In June 2024, global cyber insurance premium prices were down 15% from their peak in mid-2022. In addition to price decreases (which vary significantly by sector, region and risk profile, with competition highest in remote risk layers), capacity is up and insurers are also willing to increase limits, remove cover restrictions (ransomware-related) and lower retention levels[6].

At the same time, insurance companies are requiring businesses to strengthen their cybersecurity, which can lead to market improvements. The CyberArk Identity Security Landscape Report 2025[7] reveals how widespread this trend has become. The report shows that 88% of organisations worldwide say their insurers now require advanced security controls. In Italy, this trend is even more pronounced, with the study finding that 95% of Italian organisations are responding to their

5 - Marsh, Europe Cyber Market Update (June 2025)
6 - Howden, Cyber insurance: Risk, resilience and relevance
7 - https://techfromthenet.it/2025/09/08/cybersecurity-e-aziende-italiane-il-ruolo-delle-assicurazioni/

insurance companies' requirements for greater security measures. CyberArk's research highlights a major shift in how cybersecurity decisions are made. Insurance companies know how expensive data breaches and cyberattacks can be, so they are no longer just giving advice. The report shows that insurers are now setting strict requirements that companies must follow to obtain or keep their insurance coverage. The report suggests that this outside pressure is driving positive change. Namely: companies now have to think about multiple things at once: keeping their data safe and protecting their reputation, while also making sure they can stay in business and remain financially stable through appropriate insurance coverage. The research frames this insurance pressure as a real opportunity for companies to speed up their cybersecurity improvements. (See chart Figure 5 and 6)

Figure 5 - Rate change for Europe.

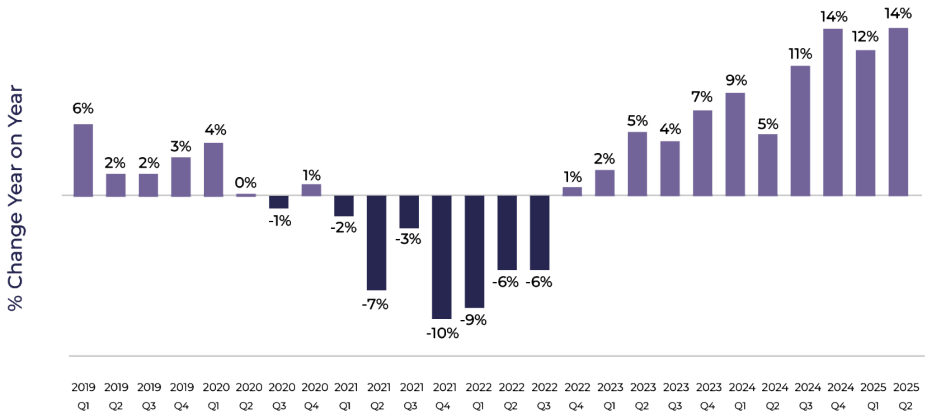


	2020Q1	2020Q2	2020Q3	2020Q4	2021Q1	2021Q2	2021Q3	2021Q4	2022Q1	2022Q2	2022Q3	2022Q4	2023Q1	2023Q2	2023Q3	2023Q4	2024Q1	2024Q2	2024Q3	2024Q4	2025Q1
Total	6%	18%	31%	32%	53%	97%	110%	79%	106%	85%	29%	17%	16%	9%	2%	-4%	-7%	-11%	-7%	-11%	-10%
Primary	8%	15%	29%	25%	49%	64%	90%	74%	100%	79%	31%	20%	16%	10%	4%	-1%	-3%	-11%	-8%	-14%	-10%

CE - Total

Source: Marsh

Figure 6 - Average limit movement.



Source: Marsh

Underwriting Info

- Insurers now ask fewer questions thanks to mature data and technology.

- There is more flexibility regarding key cybersecurity controls.

Coverage

- Insurers typically eliminated restrictions and broadened coverage for accounts with additional industry-specific extensions and solutions.

- Co-insurance for ransomware and systemic risks has ended.

- Long-term agreements (LTAs) and extended coverage options are returning.

- Back to broad wordings, including reinstatement, non-IT Contingent Business Interruption.

- War Exclusions stabilised around variant B clause from Munich Re.

Key figures on market penetration (rough estimates)

- Large organisations account for about 50% of European cyber insurance premiums, followed by small organisations (~20%), medium-sized organisations (~18%) and micro-organisations (~12%)[8].

- This means that large corporates remain disproportionately overrepresented among cyber insurance buyers, since they represent just 0.2% of all EU companies.

- Overall, Marsh estimates that the insurance penetration rate hovers around 15% for SMEs.

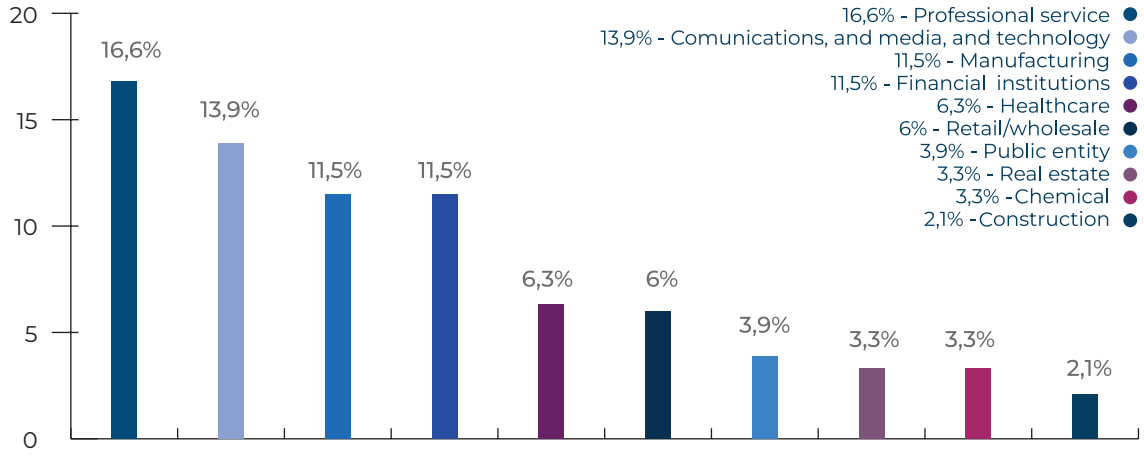
2.1.3. Evolution of Cyber Insurance Claims

The number of cyberattacks, especially ransomware, continues to rise, but these attacks are, on the whole, better mitigated by clients. According to Marsh, cyber claims notifications in Europe rose by 61% in 2024 compared with the previous year, with approximately 10% of cyber policyholders reporting an event. This increase is mainly driven by malicious events (72%), although the share of non-malicious events rose to 28% of all notifications (compared with 14% in 2023). Incident origins were both internal and external — including some involving third or fourth parties in the supply chain.

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). When comparing this distribution year-over-year, both professional services and manufacturing sectors experienced a significant surge in notifications, with numbers approximately doubling compared with 2023. Notably, the chemical industry also experienced a substantial increase in notifications in 2024. In contrast, financial institutions experienced a significant decrease in volume of claims, with claims notifications dropping by approximately one-third. This decline contrasts with the rising claims notifications observed in other sectors and reflects the strengthening of the industry's cyber resilience since the introduction of the EU Digital Operational Resilience Act (DORA)[9]. (See chart Figure 7)

8 - Marsh, Behind the Firewall: 2024 Global Cyber Industry Insights.
9 - Available here : https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng

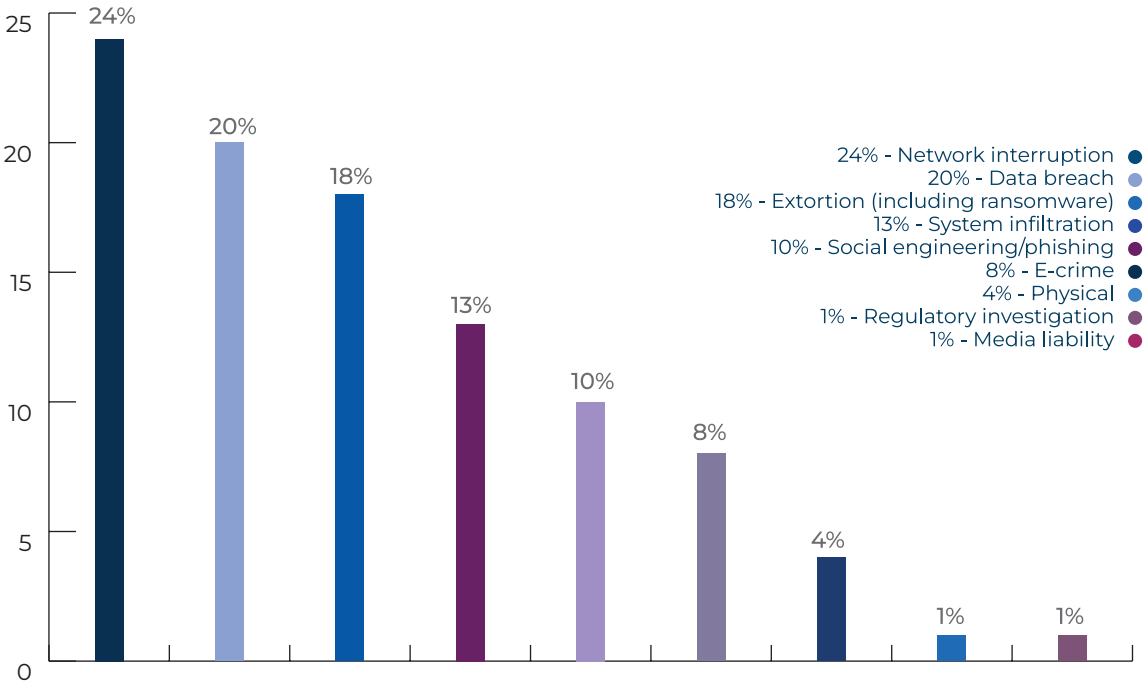
Figure 7 -The professional service sector generated the most notifications in 2024.



Source: Marsh

Regarding the type of incidents leading to notifications, network interruptions exceeded all other categories but were primarily driven by the CrowdStrike incident (see page 10). Cyber extortion and data breaches remain the core concerns for European organisations. 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 (GDPR[10]) and varying interpretations of its provisions across jurisdictions, underscores the necessity for Risk Managers to prioritise GDPR compliance both before and during an incident. (See chart Figure 8)

Figure 8 - Network interruptions most prevalent incident type in 2024.



10 - Available here: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

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

Firstly, organisations have increasingly developed robust security and backup systems to safeguard against the deletion or encryption of data, which has reduced the effectiveness of ransomware attacks.

Secondly, threat actors have shifted their tactics, resorting to data exfiltration rather than traditional ransomware encryption, meaning that organisations have less of an incentive to pay ransoms where their operations are not directly threatened.

Thirdly, the legal risk of making ransom payments is increasing, as many governments (including that of the United Kingdom) are discussing partial ransom payment bans. France, for example, 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 thus creates a legal risk to the payee organisation's directors and officers, since threat actors may be sanctioned entities/persons, which would make a ransom payment an unlawful act.

Lastly, cyber extortion consultancy companies have reported a decrease in the reliability of threat actor groups in fulfilling their promise after receiving a ransom payment, both regarding the provision of a functioning file decryption key and in not leaking or otherwise selling previously exfiltrated data.

Focus: the impact of the CrowdStrike incident on cyber claims

The CrowdStrike incident of 19 July 2024 had an oversized impact on cyber claims notifications in 2024, as it affected millions of users worldwide, as a faulty update to its Falcon Sensor security software caused widespread problems with Microsoft Windows computers running the software.

Yet, even when discounting 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.

It must nevertheless be noted that, despite being far reaching and widely covered in the media, the CrowdStrike incident was ultimately less costly than expected: $ 0.5 billion, versus initial estimates of $ 1 billion).

Focus: Claims and the Risk Manager

- Claims data are useful to draw historical trends and for benchmarking but should only be seen as indicators, since they are by nature aggregated and backwards looking. Corporate insurance buyers should focus primarily on their own risk profile and careful risk evaluation to guide their insurance procurement.
- We recommend that Risk Managers follow the claims protocol outlined in Appendix 2 of the Cyber Insurance Dialogue to improve the quality of the cyber risk and the resilience of their organisation:

1. Prepare before the incident: conduct a risk assessment, develop a cyber incident response plan, train employees, conduct regular stress tests of cybersecurity measures.

2. Contain the incident: quickly isolate and contain the affected systems of devices to prevent further damage or spread of the cyberattack.

3. Notify relevant parties: inform all relevant stakeholders and activate cyber insurance.

4. Activate the Incident Response Plan.

5. Mitigate the Damage: Implement mitigation measures to limit the damage.

6. Report the Incident: Inform law enforcement or regulatory bodies, if required.

7. Restore Normal Operations: Work to restore normal operations as soon as possible and implement measures to prevent a similar incident from occurring in the future.

2.2 Legislative frameworks

In our assessment, the wording of cyber insurance policies is standard across European countries despite differences in legislative frameworks. However, Risk Managers still need to pay attention to several legal considerations, which may impact their cyber insurance programme.

2.2.1. Cyber incident reporting obligations

Across the European Economic Area, United Kingdom and Switzerland, reporting obligations following cyber incidents vary depending on the jurisdiction and type of cyber event.

Several EU laws mandate the reporting of cyber incidents to various authorities on different timelines[11]:

11 - See FERMA's Cyber Reporting Stack: Navigating EU Requirements white paper for more information on the interaction of EU cyber incident reporting requirements and the role of the Risk Manager in cyber incident management and reporting.

- Under the NIS2 Directive[12], relevant organisations must report 'significant incidents' within 24 hours to their national cyber security incident response team followed by an initial assessment of severity, impact, and indicators of compromise within 72 hours.

- GDPR requires that cyber incidents resulting in data breaches be reported within 72 hours of the organisation becoming aware of the breach.

- For cyber incidents that trigger regulatory obligations under DORA, there are a number of stages that organisations must address before triggering the need to report a 'major ICT-related incident'. Once this is triggered, an initial report must be made no later than "than 24 hours from the moment the financial entity has become aware of the ICT-related incident," an intermediate report is required within 72 hours of the initial notification, with a final report required no later than one month after.

As an EU member state, France is subject to the above EU rules; however, Article 5 of the LOPMI[13] (Orientation and Programming Law of the Ministry of the Interior) explicitly adds cyber risks into the French insurance code. It makes it compulsory for any victim of an attack on an automated data processing system to report to the competent authorities (police, gendarmerie, or the public prosecutor) no later than 72 hours after the victim becomes aware of the attack in order to be compensated by any insurance policy.

In the United Kingdom, reporting requirements are dependent on the type of incident. The UK NIS Directive includes mandatory reporting requirements of 72 hours for incidents having a significant impact on the continuity of 'operators of essential services'. Similarly, and analogous to the European Union, cyber incidents resulting in data breaches should be notified to the UK data protection regulator (the ICO) within 72 hours of an organisation becoming aware of the breach. Voluntary reporting of incidents to the UK National Cyber Security Centre is also encouraged. Additionally, the proposed Cyber Security and Resilience Bill is expected to align with the reporting timescales within the NIS2 Directive, requiring an initial report within 24 hours, and a full report in 72 hours. Finally, the proposed ransomware reporting regime for the United Kingdom would require mandatory reporting of a ransomware incident within 72 hours, and a follow-up report within 28 days.

In Switzerland, operators of critical infrastructure are required to report cyberattacks to the Swiss National Cyber Security Centre within 24 hours of discovery, and to complete an initial report within a further 14 days. Reporting is required where the functioning of critical infrastructure is threatened, or there is manipulation or leak of information, or blackmail, threats or coercion. Critical infrastructure operators that fail to report a cyberattack may be fined. Finally, data breaches in Switzerland must be reported to the Swiss Federal Data Protection and Information Commissioner 'as soon as possible' after becoming aware of the breach.

In Italy, the regulatory stratification highlighted above can trigger different notification obligations to different

12 - Available here: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
13 - https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047046768

Authorities. For example, in the case of a ransomware attack:

- the GDPR will apply if personal data is compromised.
- NIS2 will apply where delivery of a critical service is disrupted.
- DORA will apply if the attack has a significant operational impact on a bank.

In such cases, the affected organisation must notify:

- the Privacy Guarantor within 72 hours (GDPR).
- the ACN (National Cybersecurity Agency) within 24/72 hours (NIS2).
- the Bank of Italy within 4/24 hours (DORA).

Furthermore, at the time of this report, Bill no. 1441 of April 3, 2025, is under discussion to establish a comprehensive anti-ransomware strategy that prohibits ransom payments by organisations in the National Cyber Security Perimeter, with administrative penalties for violations and Prime Ministerial exceptions for national security threats. The legislation requires six-hour attack reporting to CSIRT, which coordinates responses with government agencies and intelligence services. The framework foresees institutional support through ACN (the National Cybersecurity Agency) operational plans and a dedicated CSIRT task force offering technical assistance and victim coordination. The bill also considers the creation of a public compensation fund that will partially cover economic losses for compliant organisations. The bill also criminalises Ransomware-as-a-Service platforms and provides legal protection for good-faith vulnerability disclosures, creating a prevention-focused approach that combines prohibition, support, compensation and enhanced enforcement to combat cyber extortion. In addition, the bill provides for the promotion of the underwriting of cyber-insurance, through the provision of additional tax and contribution benefits.

It is worth remembering that cyber insurance is not a substitute for robust cybersecurity measures but a complementary tool to help manage and transfer some of the financial risks associated with cyber incidents. Cyber insurance can accompany businesses in incident management and compliance in several ways:

- By providing financial protection by covering costs associated with cyber incidents (data breaches, ransomware attacks, business interruption).
- By offering support for incident response; cyber insurance often includes access to a network of experts who can assist in responding to cyber incidents (forensic investigators, legal counsel or IT specialists for instance). This is key as some regulations (such as NIS2) focus on specific response processes.
- By giving access to risk assessment and mitigation aimed at helping businesses identify vulnerabilities and implement appropriate security measures.
- By providing coverage for business interruption losses resulting from cyber incidents, therefore allowing for business continuity (through reimbursement for lost income, costs associated with restoring system and data, etc).

- By helping businesses to meet regulatory obligations by providing guidance on compliance and covering the costs associated with regulatory fines and penalties resulting from non-compliance.

2.2.2. Insurability of fines and penalties

In most instances, insurance policies (including cyber policies) provide indemnity for "fines and penalties covered to the extent insurable by law" or similar wording. The insurability of fines and penalties is not standardised across Europe, and is not necessarily ordinarily regulated or legislated upon.

In Germany for instance, there is no concrete view. The German Civil Code states that any legal transaction that is contrary to public policy is void; this may be interpreted as meaning that illegal conduct justifying a fine or penalty cannot be indemnified against, this being inconsistent with public policy.

In the Netherlands, similarly, there is no conclusive position. In line with the Dutch Civil Code, if coverage for fines and penalties is considered incompatible with public policy then the insurance contract may be considered null and void. Determining whether insuring certain fines and penalties aligns with public policy may involve an assessment of whether the policy wording reduces the intention of the fine or penalty, namely to prevent or challenge negligent or wilful conduct.

In the United Kingdom, there are similar public policy questions expressed via the *ex turpi causa* principle – often referred to as the 'illegality defence'. In these circumstances, the principle arguably prohibits the recovery (via insurance) of penalties or fines resulting from deliberate or intentional wrongdoing, as opposed to from conduct that is negligent. The Financial Conduct Authority, for example, explicitly states that regulated firms cannot insure against FCA-imposed financial penalties.

In Switzerland, judicial precedents and the opinions of legal professionals uphold the view that fines and penalties are not insurable. Any policy providing coverage for fines and penalties may be considered unenforceable, but once again, public policy factors are important to these considerations.

In Italy, fines and penalties related to cyber risk are partially insurable through cyber risk policies, but with exclusions and specific limitations provided for by the contractual conditions, such as malicious acts or intentional conduct of the insured. The coverage may include legal fees for civil, criminal and administrative disputes, but not the criminal penalties themselves, while financial penalties can be compensated within certain limits.

It is clear that, across these jurisdictions, the insurability of specific fines and penalties is contingent on the nature of the conduct that gave rise to them.

2.2.3. Insurability of ransoms

Ordinarily, when considering the insurance implications of a ransom payment, the question is not one of insurability but legality. Under a strict legal interpretation, cyber insurance policies are policies of indemnity. A policyholder seeks an indemnity for the sums which it has paid out, which may include a ransom.

It is not the ransom itself which is insured but the policyholder's liability. Insurers will therefore be concerned to ensure that the policyholder has complied

with its legal and regulatory obligations before authorising or making a ransom payment. For example, an insurer will need to establish that any payment has not been made in breach of any domestic or EU sanctions legislation or consider whether links exist to terrorism or certain entities or individuals.

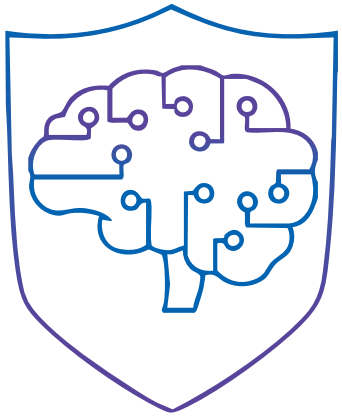
There is no reason in principle why a lawfully made ransom payment should not be insurable. Commercial considerations, such as the risk of encouraging further attacks, do not affect the insurability of ransoms.

Insurers need to be aware of legislative or regulatory developments affecting this issue. In the United Kingdom, for instance, proposals have been advanced to legislate certain issues in respect of ransomware.

- One proposal would formally prohibit all public sector bodies, including local governments, and all owners of critical national infrastructure, from making ransom payments. The efficacy of any proposed ban may lie in the proposed enforcement measures, including possible civil penalties.

- A second proposal would require all proposed ransomware payments (outside of those expressly prohibited) to be reported. The Government would then review proposed payments, blocking those which may breach sanctions designations or which are in violation of terrorism finance legislation. The victim would retain discretion to make a payment where it is not expressly blocked. Again, the efficacy of this proposal will likely lie in any enforcement measures, again including possible civil penalties.

In those instances where ransom payments are made despite being expressly prohibited by legislation or subject to a government block, it is likely that those payments would not be insurable. Similarly, any civil penalties would be subject to those considerations above regarding the insurability of fines and penalties.



3. CHALLENGES

3.1. Coverage of cyber risks through multiple policies

3.1.1. Overview

A cyber event is generally defined as an incident affecting the technology used by a company. Such events can lead to different financial consequences, and depending on the nature of these outcomes, coverage may fall under various insurance policies, as illustrated in chart Figure 9.

1. Financial losses related to bodily injury or physical damage are typically covered under property and casualty policies. However, if these risks are excluded - following the industry-wide "silent cyber" clarification initiative - specific products such as Cyber Physical Damage (Cyber PD or CZ) have been developed to close this gap. For example, a fire caused by a cyber event would fall under this category.

2. Losses impacting directors and officers, such as claims against a CEO following a cyber incident, are usually addressed in D&O policies.

3. Cases involving fund embezzlement, such as fraudulent changes to supplier bank details, are generally covered by crime policies.

4. Losses that do not involve physical damage or financial fraud, such as business interruption or recovery costs following a ransomware attack, are typically covered by standalone cyber insurance policies.

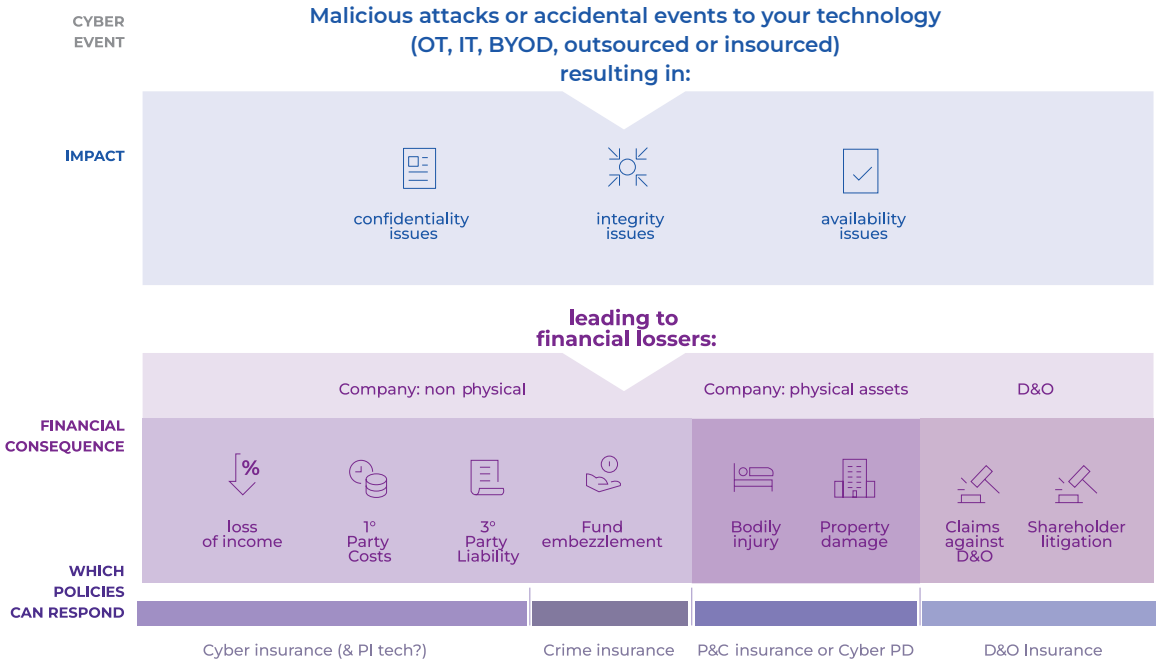
In theory, these policies are complementary, ensuring that clients are not left without coverage for cyber-related risks. However, cyber insurance does not cover all cyber events, it only addresses exposures that are not already included in other policies. For Risk Managers, this underscores the importance of conducting a comprehensive cyber exposure analysis and reviewing the entire suite of policies to identify potential gaps or overlaps. Collaboration with brokers or intermediaries is essential to ensure adequate protection across all major cyber scenarios. (See chart Figure 9)

3.1.2. Focus on: Silent Cyber

The topic of "silent cyber" has gained prominence following increased claims activity and litigation, particularly after the NotPetya ransomware attacks. In response, Lloyd's mandated that, starting in January 2020, all non-cyber insurance policies must explicitly address cyber risk—either by excluding it entirely or by providing specific endorsements to cover the exposure. This requirement was introduced in phases, beginning with first-party property damage policies and later extending to liability and treaty reinsurance. A high-level review of key insurance lines in Europe reveals the following:

- **Property and Casualty:** Most policies now include cyber exclusions, with carve-backs for Cyber PD, often limited to fire, explosion, or machinery breakdown. As a result, coverage gaps are minimal or "manageable".

Figure 9 - Illustration of potential financial consequences and insurance policies triggered by a cyber incident.



- **Aviation**: The AVN 139 clause is widely used to clarify coverage for software-related losses.

- **Energy and Marine:** Cyber PD is generally excluded, but a range of dedicated CZ products is available to address these gaps.

For Risk Managers, the recommended strategy is to adjust Cyber PD coverage to avoid overlaps and, where necessary, consider dedicated products. Broker involvement remains critical to ensure alignment with organisational risk profiles.

3.1.3. Foresight: possible future AI exclusion

Artificial Intelligence (AI) is increasingly embedded in business processes, amplifying both technological capabilities and associated risks. From a cyber perspective, AI is being leveraged by malicious actors to enhance the sophistication of attacks, while simultaneously being deployed by cybersecurity firms to strengthen defenses. Historically, threat evolution tends to outpace defensive measures, creating a persistent challenge for insurers.

For insurers, this dynamic alters the risk landscape: while advancements in cybersecurity may reduce attack frequency, the severity of incidents could increase as adversaries develop more powerful tools. From a client perspective, it is essential to maintain market stability by avoiding restrictive measures that limit cyber coverage in response to AI-driven threats. The fundamental definition of a cyber incident remains unchanged—whether AI is involved or not, a malicious act is still a malicious act, and accidental events remain within the same conceptual framework.

3.1.4 Recommendations:

Organisations should adopt a structured approach to managing cyber risk coverage:

1. Conduct a thorough review of all policies, in collaboration with brokers, to eliminate gaps and overlaps and ensure that all critical scenarios identified by internal stakeholders (CISO, Risk Manager, CFO) are adequately covered.

2. Enhance internal coordination among primary insurers across different lines of coverage through joint scenario reviews based on the CIA triad.

3. Update quantification and modeling of cyber impacts—both physical and non-physical—to adjust policy limits and align cybersecurity investments accordingly.

4. Work closely with brokers to select optimal coverage structures and limits, ensuring an efficient and comprehensive insurance programme.

For their part, insurers should provide clarity regarding AI-related claims, confirming that such risks are covered under existing frameworks. AI does not introduce new categories of risk entirely; rather, it influences the probability and severity of existing threats. Therefore, AI-related exposures can be incorporated into current policy structures without requiring the creation of separate coverage lines.

3.2. Exclusions

Cyber insurance has emerged as a specialised line of coverage designed to address the unique and rapidly evolving risks associated with digital data and information systems. However, its origins can be traced back to long established insurance lines, such as property and liability coverage, which existed long before the creation of the Internet, and never considered the complexities of cyber risks. As the use of digital technology grew and cyber threats increased in sophistication and frequency, insurers recognised that conventional lines of insurance were inadequate for covering losses resulting from data breaches, hacking, or system outages. Consequently, there was a clear need for dedicated, targeted coverage to address these emerging risks.

For example, property insurers carved out damage to data and digital infrastructure caused by malware or cyberattacks from property policies because their forms were designed to cover physical damage from perils — such as fires, theft, or natural disasters — rather than intangible harm to digital assets. Similarly, damages and liabilities arising from data breaches or cyber incidents that could have been covered under Commercial General Liability (CGL) policies are often excluded in cyber insurance policies. CGL policies traditionally cover third-party claims related to bodily injury or property damage, but they were not designed to manage the complexities of cyber risks, such as privacy violations or data loss. As the volume and severity of cyber incidents increased, CGL policies proved insufficient, prompting the development of dedicated cyber coverage.

Because cyber insurance borrowed exclusions from existing lines of coverage, insurance buyers need to understand how this language could result in gaps that organisations must address as the digital landscape expands. Many of the exclusions found in cyber insurance policies are inherited from these foundational lines, reflecting both the limitations of earlier coverage and the necessity to adapt to new and emerging threats. These exclusions serve multiple purposes, including discouraging moral hazards, managing catastrophic risks, and addressing coverage overlaps.

For instance, cyber insurance grants affirmative coverage for regulatory fines and penalties arising from otherwise covered perils, such as privacy breaches, technology errors, or lapses in security. Simultaneously, those policies also mirror other lines and prevent reimbursement of losses arising from fraudulent acts, anticompetitive behaviour, or illegal activities. Insurers use these exclusions to prevent organisations from intentionally engaging in or benefiting from illegal acts, which could otherwise lead to moral hazard—where insured parties might be tempted to take greater risks because they believe they are protected. By explicitly excluding losses resulting from illegal acts, insurers encourage organisations to maintain robust cybersecurity measures and ensure legal compliance.

A second significant category of exclusions pertains to catastrophic risks, which are often difficult to quantify and manage. Two well-publicised examples in this category are the war exclusion and infrastructure exclusions. The war exclusion typically excludes damage resulting from acts of war, including cyber warfare, which could have widespread and unpredictable impacts. Infrastructure exclusions, on the other hand, exclude damages related to failures or disruptions of critical infrastructure, such as energy production, financial markets, or telecommunications. Insurers design these exclusions to avoid potentially unlimited losses from large-scale or systemic events.

In recent years, the application of war and infrastructure exclusions has garnered increased attention due to heightened geopolitical tensions and the rise of nation-state cyber operations. The ability of threat actors—often sponsored or aligned with nation-states—to conduct cyberattacks remotely has blurred the lines between traditional warfare and cyber conflict. The undefined parameters of cyber warfare, including what constitutes an act of war in cyberspace, complicate the application of these exclusions.

However, although many hundreds of nation-state-related attacks have resulted in insurance claims[14], insurers have routinely refrained from invoking these exclusions, and their language has never been litigated in the context of a cyber insurance policy. Instead, the insurance industry continues to recognise that such exclusions should apply only to extremely rare instances that result in catastrophic loss.

14 - The Digital and Cyberspace Policy for the Council on Foreign Relations tracked more than 900 cyber operations conducted by threat actors known to be affiliated with a nation state occurring between 2005 and 2024. See CFR Cyber Operations Tracker. This research collected open-source data and does not account for operations that remained classified, went undetected, or failed to receive confirmed attribution.

Examples of cyber-attacks related to nation state actors where insurers paid claims include:

- The WannaCry malware campaign, carried out by North Korea in 2014, that encrypted data and interrupted operations affecting hundreds of thousands of computers across multiple industries worldwide.

- The 2017 NotPetya operation, attributed to Russia, in which a bogus software update released malware causing widespread destruction of networks leading to disruption of operations and more than $10 billion in costs.

- A destructive malware campaign carried out by North Korea in 2014 that leaked sensitive data from and caused significant operational disruption to a US company.

In addition, thousands more cyber operations linked to nation states have involved cyber extortion, theft of cryptocurrency, and espionage. In these instances, insurers recognised that the typical motives and tactics of nation state-backed operations lie outside of the scope of cyber warfare, making coverage is not applicable.

Nonetheless, insurers apply war and infrastructure exclusions similarly to other lines of coverage, viewing them as mechanisms to limit exposure to 'black swan' events—rare but high-impact incidents that could cause widespread economic damage.

Lastly, insurers use exclusions to prevent the stacking or overlapping of recoveries across multiple lines of insurance. As technology becomes increasingly embedded in physical processes — such as manufacturing, transportation, and energy production — the potential for coverage gaps has grown. For example, a cyberattack that disrupts a physical infrastructure component might trigger multiple policies, but insurers embed exclusions to prevent double recovery for the same event. This has led clients to expand their cyber insurance coverage to fill these gaps, especially as the integration of digital and physical systems continues to deepen.

Finally, the rapid pace of technological innovation introduces new risks that challenge existing insurance frameworks. Emerging technologies — such as generative AI and quantum computing — bring both opportunities and vulnerabilities. Cyber insurers have yet to use exclusions to limit their exposure to the complex and fast-evolving landscape of cyber risks associated with these innovations. As technology continues to evolve, insurers will need to understand how to underwrite these new exposures effectively[15].

3.3. Low SME penetration

All companies, regardless of their size or industry, rely on technology to some extent. Consequently, every organisation faces cyber risks, including small and medium-sized enterprises (SMEs). These businesses typically have less mature cybersecurity measures, making them more vulnerable to attacks.

15 - Rather than creating novel technology risks, generative AI tends to amplify existing, familiar risks like data privacy and security, dissemination of misinformation, infringement of intellectual property rights and technology errors. See Debunking Generative AI myth #3: GenAI insurance issues | Marsh

Figure 10 - Distribution of ransomware attacks by companies annual revenue in 2023/24.

There are two primary motivations for targeting SMEs: generating modest financial gains on a scale and exploiting them as an entry point to compromise larger organisations. The latter scenario represents a significant supply-chain risk for major corporations, as illustrated in the graph above. (See chart Figure 10)

When a cyber incident occurs, the consequences can be devastating for organisations. According to Google's Current Cybersecurity Landscape in Spain report (2023), 60% of European SMEs cease operations within six months of suffering a cyberattack, primarily because they cannot absorb the financial losses associated with the incident. These losses often include direct costs such as ransom payments, system restoration, and legal fees, as well as indirect impacts like reputational damage, customer attrition and operational downtime. This data highlights the critical importance of implementing robust cybersecurity measures, even for smaller organisations that may perceive themselves as less attractive targets.

Cyber insurance plays a critical role in enhancing financial stability for organisations; however, its penetration among small and medium-sized enterprises (SMEs) remains notably low. Current estimates indicate that adoption rates are below 40% in the United States and under 10% across the United Kingdom, the European Union, Latin America, the Middle East, Africa, and the Asia-Pacific region.

From the insurers' perspective, developing a strong SME portfolio is essential to balance the concentration of large accounts and ensure risk diversification and greater portfolio stability.

Furthermore, SMEs are now explicitly included within the regulatory scope of the NIS2 Directive and the Digital Operational Resilience Act (DORA), both of which impose stringent cybersecurity and operational resilience obligations across the European Union. Under NIS2, SMEs operating in sectors deemed essential or important must implement comprehensive measures such as incident detection and

reporting, regular risk assessments, robust access control mechanisms, and documented security policies. The directive also mandates corporate accountability, requiring management to oversee and approve cybersecurity strategies, with potential liability for non-compliance.

Similarly, DORA applies to financial entities and their ICT service providers, including SMEs, and focuses on ensuring digital operational resilience. It introduces requirements for ICT risk management, incident classification and reporting, resilience testing and third-party risk oversight. These frameworks collectively aim to strengthen the security posture of SMEs, recognising their critical role in supply chains and financial ecosystems, and underscore the need for proactive investment in cybersecurity governance and controls.

These dynamics raise a critical question for the industry: how can the market's full potential be unlocked?

The emergence of exponential technologies has brought endless opportunities but also opened the door to new threats such as cyberattacks. In this regard, consequences can be very negative notably regarding European SMEs, 60% of which disappear within six months of falling victim to such an attack because they cannot afford the losses,according to Google[16].

Italy, cybersecurity and credit access

In Italy, financial institutions are increasingly imposing cybersecurity as a **requirement for credit access**. This trend reflects concerns outlined by the Bank of Italy in its late-2023 document "Cyber sicurezza: Una continua sfida per l'economia e per la società", which emphasised that inadequate cyber resilience could compromise a company's ability to obtain financing. Financial institutions are no longer limiting their role to evaluating economic stability; they now require proof of digital security, with initiatives such as Intesa Sanpaolo's "D-Loan" directly linking financing to cybersecurity and digitalisation efforts[17]. Therefore, the fact of having insurance cover may be interpreted as further confirmation of their cyber resilience (i.e. cyber cover is not compulsory).

16 - 60% of European SMEs that are cyber-attacked have to close after six months | Startups Magazine available here: https://startupsmagazine.co.uk/article-60-european-smes-are-cyber-attacked-have-close-after-six-months

17 - Source https://www.cybersecurity360.it/legal/niente-cyber-niente-prestito-le-banche-imporranno-la-sicurezza-come-requisito-di-credito/

Recommendations

To foster the growth of cyber insurance adoption and strengthen overall resilience, coordinated efforts are required across all stakeholders in the value chain.

For insurers, the priority should be to simplify the customer experience. This includes streamlining the underwriting process and designing bundled products that are easy to understand and purchase. Digitalisation is another key enabler, allowing for more efficient policy management and claims handling. Additionally, insurers should invest in specialised training programmes—such as those offered by the Cyber Insurance Academy—to enhance internal expertise and ensure that teams are equipped to address the evolving cyber risk landscape.

For brokers and agents, embracing innovative cyber insurance products is essential. They must also commit to continuous education, leveraging training initiatives like the Cyber Insurance Academy to build confidence in advising clients on complex cyber risk issues.

For clients, awareness and preparation are critical. Organisations should prioritise cybersecurity training for their teams, collaborate closely with their supply-chain partners to mitigate systemic risks and maintain ongoing investments in security measures.

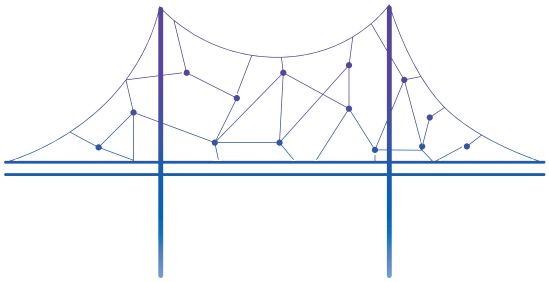
Finally, policyholders and cybersecurity associations should recognise cyber insurance as a complementary tool within a broader risk management strategy. It is not a substitute for robust cybersecurity practices but rather an additional layer of protection that can enhance resilience.

Ultimately, achieving a more stable and resilient economy requires a collaborative approach—insurers, brokers, and clients working together to address cyber risk in a comprehensive and sustainable manner.

Targeted recommendations by FERMA Member GVNW[18]

- **Assistance Services (Preventive & Reactive)**: Offer 24/7 hotlines, IT forensics, legal support, and crisis communication—services that add tangible value and improve incident handling, even before claims are formally reported.
- **Cybersecurity Awareness & Training**: Embed training (e.g., e-learnings, phishing simulations) into policies to boost resilience. Potentially reward participation through premium incentives.
- **Simplified Digital Underwriting**: Streamline underwriting for SMEs via digital risk assessments and AI-supported tools to enable faster "click-and-bind" solutions.
- **Integration into Supply Chain Qualification**: Cyber insurance could serve as an indicator of risk maturity, helping SMEs meet increasing resilience requirements from larger supply chain partners.
- **Segmented, Industry-Specific Coverage Models**: Tailor offerings to the unique risk profiles and regulatory needs of SME sectors like healthcare, retail, manufacturing, or trades.

18 - https://www.gvnw.de/



4. CONCLUSION

Based on this report's findings, it appears that the perceived cyber insurance gap does not always reflect the state of play of the market and, when it does, those gaps are not insurmountable. On the contrary, many options are available to overcome the lack of awareness and understanding about cyber insurance products that contribute to underestimating the value that cyber insurance can bring to organisations.

Clients often hesitate to buy cyber insurance for a range of interconnected reasons:

1. Brokers and other intermediaries are frequently **not adequately trained** to address the full range of inquiries related to cyber risks. This underscores the urgent need for continuous education and capability-building across the industry.

2. There is still widespread **confusion between cyber insurance and crime coverage**. In line with FERMA's recommendations, these risks should be assessed holistically, and in many cases, a blended solution may offer greater clarity and value.

3. Large clients often perceive **cyber insurance products as overly standardised** and not tailored to their specific needs. This calls for greater innovation in product design.

4. The **underwriting process is still seen as too complex** and opaque, although this perception is changing given the current soft market.

5. A further challenge is the **reluctance to share underwriting information,** which is often viewed as too risky—limiting transparency and trust in the process.

6. **Cost** is another frequently mentioned barrier. Many clients consider cyber insurance too expensive; however, the current soft market presents more favourable pricing conditions.

7. Some clients mistakenly believe that if they are not operating in the **cloud**, they are not exposed to cyber risks. This is a **misconception**, as demonstrated by cases such as Marks & Spencer[19], where non-cloud-related exposures were still covered under the policy.

8. There is also a lack of understanding regarding the **distinction between cybersecurity controls and cyber insurance**. These should not be seen as substitutes for each other but rather as complementary tools—much as sprinklers and fire insurance work together to mitigate fire risk.

9. Finally, many clients either do not fully understand the solution or fail to **recognise its added value**. This is particularly concerning given that 60% of SMEs go bankrupt following a

19 - More information is available here: https://www.bbc.com/news/articles/c0el31nqnpvo

major cyber incident without adequate coverage, and large corporations may face significant financial consequences, including profit warnings.

Ultimately, the solution lies in the insurance industry's ability to listen more closely to client needs and to challenge itself to evolve—offering more relevant, transparent, and value-driven solutions in a rapidly changing risk landscape.

With this report, FERMA, Howden and Marsh reiterate their longstanding commitment to constructively engage with all stakeholders to build a well-functioning and affordable cyber insurance market contributing to the overall resilience of the EU economy.

NOTES

NOTES

NOTES

Special acknowledgment for their contribution to the report to:

Federica Maria Rita Livelli, Business Continuity & Risk Management Consultant, (CLUSIT Direttivo)

Gamze Konyar, Managing Director, Head of Cyber, (Marsh Europe)

Hanneke van Oss, Department Head Insurance (Bluewater) – member of FERMA digital committee

Jean Bayon de la Tour, Head of Cyber, International (Howden)

Manuel Pérez Head of Cyber, Southern Europe and Latin America (Howden)

Mathew McCabe, US & Canada Cyber Coverage Leader (Marsh)

Patrick Hill, Partner (DAC Beachcroft LLP)

Stuart Hunt, Senior Associate (DAC Beachcroft LLP)

Tobias Bunz, Senior Insurance Expert (EON) - member of FERMA digital committee

Marsh

HOWDEN

FERMA
Anticipating changes
Shaping the future

Federation of European Risk Management Associations
Avenue de Tervuren 273 B12 - 1150 Brussels (BELGIUM)
Tel: +32 2 761 94 32 - Email: enquiries@ferma.eu

@FERMARISK