Commentary

Cyber Insurance: A Tool to Mitigate Increasing Cyber Threats to Corporates, SMEs, and Banks

Morningstar DBRS
2 July 2025

Key Highlights

- As corporates and SMEs continue to digitise their operations and expand their reliance on third-party vendors and cloud services, their exposure to sophisticated cyberattacks has escalated sharply.
- Cyber risks constitute one of the largest emerging threats to banks and a potential source of financial instability.
- Cyber insurance could be an effective tool for large corporates, SMEs, and financial institutions to manage cyber risk.

Mario De Cicco
Vice President
Global Insurance & Pension Ratings
+34 919 036 512
mario.decicco@morningstar.com

Marvin Pokies
Assistant Vice President
European Corporate Ratings, Diversified Industries & Energy
+49 69 2713 77010
marvin.pokies@morningstar.com

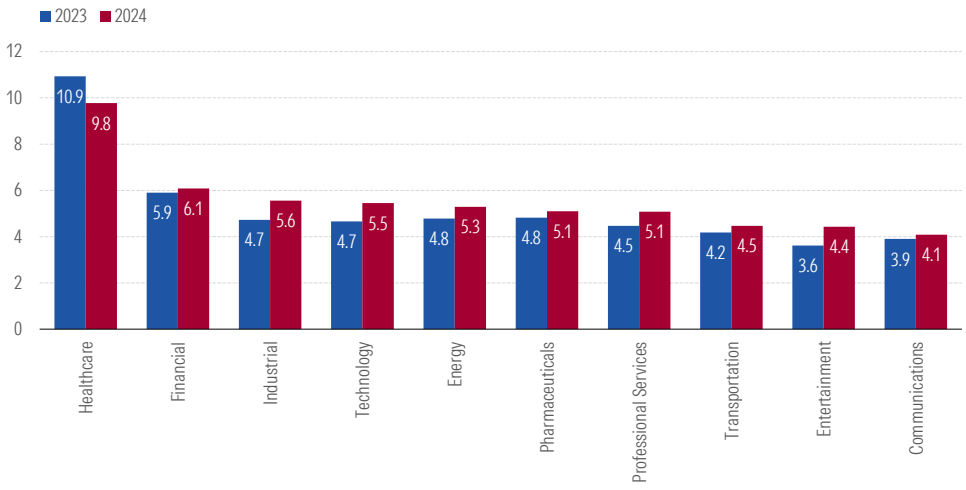
Nicola De Caro
Senior Vice President, Sector Lead
European Financial Institution Ratings
+49 69 8088 3505
nicola.decaro@morningstar.com

Marcos Alvarez
Managing Director
Global Financial Institution Ratings
+34 919 036 529
marcos.alvarez@morningstar.com

Overview

Wide adoption of new digital technologies, including artificial intelligence; the global interconnectivity of operating systems and platforms; a high reliance on third-party service providers; and rising geopolitical tensions are among the main threats making corporates, small and medium-size enterprises (SMEs), and banks increasingly vulnerable to cyber attacks and operational incidents. Cyber attacks are usually intended to destroy, steal, or alter confidential information, including customer data, or cause operational disruptions such as service interruptions or delays. These could lead to severe financial losses and reputational damage. In April 2025, for instance, a combined cyber attack hit the large British retailers Marks & Spencer and Co-op causing losses estimated at GBP 270 million to GBP 440 million, according to the Cyber Monitoring Centre. In this landscape, we see an increasing demand for cyber protection, which could likely fuel the already fast-growing cyber insurance market. Cyber insurance can help mitigate financial losses generated by malicious and non-malicious cyber threats, especially for entities with limited defences in place. However, because of the dynamic nature of these risks, the fast-changing operating environment, and the potentially high financial impact of cyber events, (re)insurance companies need to prove their capability to effectively assess and price cyber risks.

Exhibit 1 Average Cost of Data Breach Incidents by Industry (EUR millions)



Sources: IBM, Morningstar DBRS.

Cyber Risk Exposure in European Corporates: Sectoral Disparities and Operational Impact

Corporates across Europe, ranging from SMEs to large public companies, face an increasingly hostile cyber threat landscape. As firms continue to digitise their operations and expand their reliance on third-party vendors and cloud services, their exposure to sophisticated cyber attacks

has escalated sharply. While no sector is immune, evidence reveals distinct disparities in attack frequency and impact across industries. As reported by IBM,[1] the global average cost of a data breach reached USD 4.88 million, marking a 10% increase over the previous year. The average cost in Europe ranged between USD 4.0 million and USD 5.9 million, with the Benelux countries and Germany being in the upper bracket. Notably, attacks in the healthcare sector remained the costliest globally, with the cost of the average breach at USD 9.77 million, down from EUR 10.9 million in 2023 (Exhibit 1).

The European Union Agency of Cybersecurity (ENISA) reported that, in terms of threat frequency and distribution across European sectors, public administration (19%), healthcare (8%), manufacturing (6%), finance (6%), and transport (6%) were the most targeted sectors by volume of observed cyber incidents from July 2022 to June 2023. Ransomware (a type of malicious software designed to restrict access to a system or data until a ransom is paid) continues to dominate the attack landscape, with manufacturing (14%), healthcare (13%), public administration (11%), and services including consulting and legal (9%) representing the largest shares of ransomware incidents. These figures suggest a layered exposure structure. Healthcare and manufacturing not only face high attack frequency but also disproportionately suffer ransomware-driven disruptions. Public sector organizations, while often targeted for ideological or geopolitical reasons, also carry extensive data security burdens. In contrast, sectors such as construction or logistics appear less frequently among top targets, though indirect exposure through supply chains remains a critical concern.

The operational consequences of cyberattacks can be severe. Advanced phishing (a fraudulent technique used to acquire users' sensitive data) and credential theft, often coupled with lateral movement and ransomware deployment, were the most prevalent techniques leading to system-wide compromise. Consequences are often even more severe for SMEs, which are more likely to be targeted by malicious cyber threats and less able to defend themselves. SMEs tend to be more likely to pay ransoms when they do not have any other alternative to restore data, making them more vulnerable to cybercriminals. Moreover, private companies have limited budgets allocated to cybersecurity and some of them do not have a specific IT department to manage cyber-related risks. A successful attack by ransomware or phishing can even result in a business closure for SMEs.

To address these weaknesses, the NIS2 Directive[2] enacted in 2023 expands the cybersecurity governance obligations for medium and large organisations across critical sectors such as healthcare, energy, finance, and digital infrastructure. ENISA notes that, while policy architecture is improving, the implementation of cybersecurity measures remains uneven, particularly among midsize corporates and those operating with tight margins.

1 IBM. Cost of a Data Breach Report 2024. July 2024.

2 European Commission. NIS2 Directive: new rules on cybersecurity of network and information systems. 14 December 2022.

A Potential Threat to Financial Stability

Cyber risk constitutes one of the largest emerging threats for banks and a potential source of financial instability. According to a survey by the Bank of England, 80% of financial institutions view cyber risk as a source of risk to financial stability and 31% believe that it is the main risk facing the financial system. Cyber attacks and IT outages could lead to significant financial losses and cause severe reputational damages. Given the extensive interconnections among financial systems, such attacks could have ripple effects on financial stability.

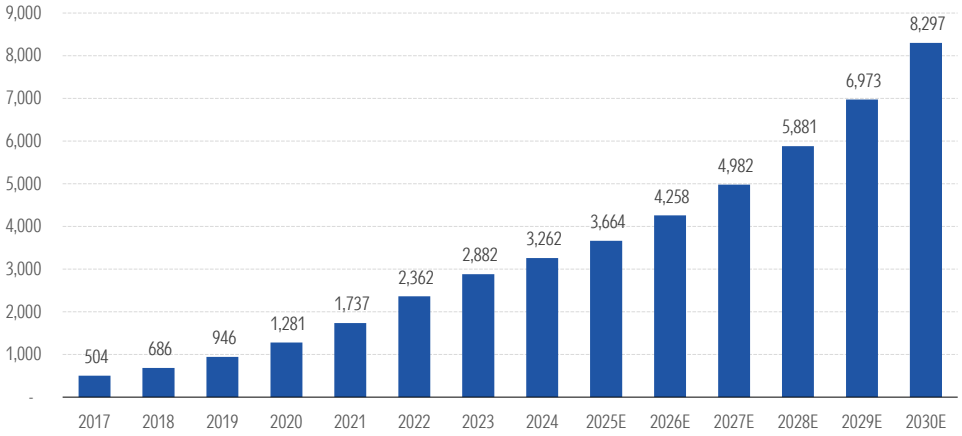
The total number of cyber attacks, successful and unsuccessful, remains unknown; however, public data show an increase in the volume of attacks targeting financial institutions and third-party service providers used by banks. According to data from the European Central Bank, the number of significant cyber incidents in 2024 increased to 153 (+12% year over year). Ransomware, Distributed Denial-of-Service (DDoS; designed to interrupt the availability of a server or website), and phishing (a fraudulent technique used to acquire users' sensitive data) appear to be the most frequent cyber attacks targeting European banks. There has been also an increase in politically motivated cyber attacks after Russia's invasion of Ukraine in 2022 and a similar trend might be expected given the ongoing conflicts in the Middle East.

For the time being, attacks have resulted in limited financial losses and manageable reputational impacts. However, as technology advances, cyber attacks are increasingly sophisticated, and their impact could prove far more material. Against this backdrop, banks will need to strengthen their cybersecurity systems. Increasing their investments in cyber protection and tightening their cybersecurity to comply with the regulations in the EU's Digital Operational Resilience Act (DORA) will likely help the banks strengthen their ability to withstand, respond to, and recover from IT failures.

Cyber Protection Demand Is Booming

As a result of the above, more and more large corporates, SMEs, and financial institutions, as well as individuals, are pushed to seek cyber protection.

Exhibit 2 Cyber Insurance Gross Written Premiums (EUR millions)



Sources: Munich Re, Morningstar DBRS.

Cyber insurance is a relatively new specialty product with a small and overall underpenetrated market in Europe. Cyber insurance gross written premiums (GWP) accounted for less than 1% of total property and casualty (P&C) insurance GWP in Europe in 2024. Nevertheless, cyber insurance can be considered one of the fastest-growing segments in the P&C business globally as its GWP increased at a compound annual growth rate (CAGR) of 16% in the last five years. According to Munich RE,[3] global cyber insurance GWP reached EUR 15.3 billion in 2024 (EUR 14.3 billion in 2023), more than double the amount five years ago. Around two thirds of the total premiums were related to North America with the U.S. being a significantly larger and more developed cyber insurance market. Premiums generated in Europe were EUR 3.3 billion in 2024 compared with EUR 2.9 billion in 2023 and more than double the amount generated in 2020 (Exhibit 2). Rising demand for cyber insurance protection is expected to drive cyber insurance GWP growth even further, with GWP expected to increase at 14% CAGR, reaching EUR 8.3 billion in 2030.

The fast-growing cyber insurance market represents an opportunity for insurance companies to increase revenue generation and diversify their business. However, because of the complexity of this product, we expect the market to continue to be dominated by large global players such as Beazley, Chubb, Munich Re, AXA, and Fairfax, which currently represent the top five insurers by GWP in the cyber insurance business worldwide, generating around 30% of total GWP.[4]

Fast-Developing Landscape Creates Challenges for (Re)Insurance Companies

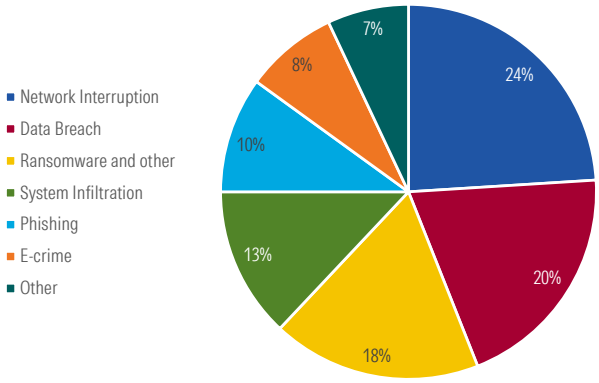
On the other hand, cyber insurance risks develop in a fast-changing landscape characterised by the quick spread of emerging digital technologies, a changing/developing regulatory environment, and increasing geopolitical tensions. This supports the proliferation of existing and new, malicious and non-malicious cyber threats that can ultimately lead to an increase of cyber claims. As reported by Marsh,[5] cyber claims submitted by clients in Europe increased by 61% in 2024 and overall have been on an increasing trend for the last nine years. Over this time period, claims were generally affected by higher ransomware threats, geopolitical issues, and the use of new digital technologies that cybercriminals can use cause damages whose effects could be amplified by widespread systems interconnectivity. Looking at the types of incidents, most notifications were related to network interruption (24% in 2024) followed by data breaches (20%) and extortion, including ransomware (18%) (Exhibit 3).

3 Munich Re. Cyber Insurance: Risks and Trends 2025. 3 April 2025.

4 Insuramore Insurance Insight. Gross Direct Premiums Written for Cyber Insurance, 2023: Top 5 Insurer Groups Worldwide.

5 Marsh. The Evolution of Cyber Claims in Europe. 23 April 2025.

Exhibit 3 Cyber Claims Notifications by Type of Incident in 2024



Sources: Marsh, Morningstar DBRS.

In addition, cyber risks can be catastrophic risks for (re)insurers, with one single event potentially leading to severe insured losses and/or sharp increases in claims worldwide. For instance, in July 2024, a CrowdStrike cybersecurity software update led to a severe IT outage causing Microsoft Windows systems to crash globally. Marsh reported that the CrowdStrike incident alone was responsible for a 16% increase in cyber claims in 2024 compared with the prior year. These challenges can potentially create significant vulnerabilities for (re)insurers in terms of adequate risk assessment and pricing.

The fast-growing cyber insurance market represents an opportunity for insurance companies to increase revenue generation and diversify their business. However, because of the complexity of this product, we expect the market will continue to be dominated by large global players such as Beazley, Chubb, Munich Re, AXA, and Fairfax, which currently represent the top five insurers by GWP in the cyber insurance business worldwide, generating around 30% of total GWP.[4]

Related Research

- *Middle East Tensions Add Underwriting and Investment Risks for Global Insurers and Reinsurers,* 24 June 2025
- *Expanded German Spending to be Private Credit Supportive,* 24 June 2025
- *European Banking: Earnings Trends and Outlook Amid Global Trade Tensions*, 23 June 2025
- *Supply Chain Is the Largest Source of Tariff Exposure for Middle Market Borrowers*, 19 June 2025
- *Crude Spike From Israel-Iran War Likely Short-Lived as Supply Adjusts*, 17 June 2025
- *Reaching a Final Destination? High Court Rules in Favour of Lessors in Russian Aircraft Insurance Test Case*, 16 June 2025
- *Navigating a New Normal: 2025 Wildfires Renew Volatility of Natural Catastrophe Losses for Canadian Insurers*, 10 June 2025
- *CRE Lending Continued to Pressure German Banks' Asset Quality in 2024*, 7 May 2025
- *Occupational Pensions: An Opportunity for Governments and Financial Institutions in an Ageing Europe*, 6 May 2025
- *From U.S. Trade Policy to Global Insurance Policies: Where Does It Matter and How Will Insurance Companies Respond?* 24 April 2025

- *Higher Tariffs Could Increase European Banks' Low Cost of Risk*, 15 April 2025
- *Implications of Heathrow Airport's Temporary Closure on Travel Insurers*, 21 March 2025
- *Navigating Liability: Collision in the North Sea and Marine Insurance Fallout*, 12 March 2025
- *Is It Time for an EU-Level Natural Catastrophe Insurance Scheme?* 24 February 2025

About Morningstar DBRS

Morningstar DBRS is a full-service global credit ratings business with approximately 700 employees around the world. We're a market leader in Canada, and in multiple asset classes across the U.S. and Europe.

We rate more than 4,000 issuers and nearly 60,000 securities worldwide, providing independent credit ratings for financial institutions, corporate and sovereign entities, and structured finance products and instruments. Market innovators choose to work with us because of our agility, transparency, and tech-forward approach.

Morningstar DBRS is empowering investor success as the go-to source for independent credit ratings. And we are bringing transparency, responsiveness, and leading-edge technology to the industry.

That's why Morningstar DBRS is the next generation of credit ratings.

Learn more at dbrs.morningstar.com.

MORNINGSTAR | DBRS