

NOT IF, BUT HOW

Munich RE 

Munich Re Global Cyber Risk and Insurance Survey 2026

Commercial lines cyber insurance:
Expanding protection against cyber threats



“Nothing of sustainable value comes without effort. With strong commitment to innovation and focused effort, our industry has repeatedly succeeded in insuring new risks: we cover for the success of rocket launches and renewable energy. Despite some doom, we also created a US\$15 billion cyber insurance market, poised for further profitable growth. I am deeply convinced that cyber insurance is of critical relevance in a world extremely driven by AI and data. For own benefit, companies and families alike need to recognise their digital exposure and the respective value of cyber risk cover. It’s a call to us insurers to act smart and ambitious in ensuring we address their cyber protection gap, for therein lies nothing less than a massive market opportunity. Munich Re remains a driving force and continues sharing insights to expand cyber protection.”

Stefan Golling

Board of Management
Global Clients and North America

The fourth edition of Munich Re's "Global Cyber Risk and Insurance Survey" shows that cyber resilience is widely recognised as a strategic corporate priority. Insurance continues to play a central role in managing the rapidly growing exposure to digital risks. Building resilience is crucial, as cyber incidents can threaten the very existence of companies and cause far-reaching harm, extending to entire economies and societies.

Effective and comprehensive cyber insurance coverage is a key component of every company's risk management strategy.

The magnitude of the cyber threat is striking: if cybercrime were a country, it would be the world's third-largest economy. By 2028, global cybercrime costs are expected to reach US\$14 trillion, according to Statista, surpassing the current combined GDP of Germany, Japan and India. Having been a market leader in cyber insurance for more than 15 years, Munich Re can draw on its deep underwriting expertise, disciplined risk management, and long-term perspective to develop a sustainable market even in uncertain times.

This year's survey incorporates insights from over 9,500 respondents across 20 countries, covering all industries and company sizes. It examines technological dependencies, evolving threat patterns, levels of cyber risk awareness, the role of cyber insurance, and the expectations of clients operating in an increasingly digitalised environment.

Content

1. Executive summary	05
<hr/>	
2. AI dominates current technology trends	07
3. High levels of concern amongst decision-makers	10
4. Cybersecurity preparedness and resilience remain insufficient	13
5. Unlocking the potential of cyber insurance in an expanding market	15
6. Conclusion	17
<hr/>	
7. Methodology of the survey	18

1. Executive summary







- Artificial Intelligence (AI) has emerged as a particularly important technology for companies.
- At the same time, digital dependencies and systemic vulnerabilities are increasing.
- Risk awareness and concerns among C-level executives remain high.
- The great majority of C-level executives consider their organisation's level of protection to be inadequate.
- Organisations primarily purchase cyber insurance to safeguard against financial losses from business interruptions or liability claims – and to gain access to specialised response services.
- A significant share of C-level leaders – well over a third – are actively considering purchasing cyber insurance. Higher uptake rates may be expected in future.

Everybody believes in digitalisation and critical digital dependencies and systemic risks will further grow.	89% of C-Level do not consider their protection level adequate.	The majority of C-Level is currently considering to buy a cyber insurance policy and also interest of private individuals is high.
Risk awareness and level of concern within C-Level is high and will be further extended through frequency and severity of cyber attacks.	Need for action and improvement is obvious. Building up cyber resilience is a socio-economic issue.	By closing the protection gap this high potential for cyber insurance needs to be unlocked.

2. AI dominates current technology trends

AI has become the most influential technology. Beating out previous topics of focus such as data analytics, cloud computing, robotics and blockchain. Only 2% of C-level respondents consider all these technologies irrelevant to their business – a major change from 12% in 2022 and consistent with Munich Re’s 2024 findings.

Technology trends with significant relevance for businesses (C-Level)

	AI 	Cloud 	Data Analytics 
2026 Global	71%	52%	53%
2024 Global	62%	57%	55%
	Robotics 	Blockchain 	None of them 
2026 Global	25%	24%	2%
2024 Global		31%	2%

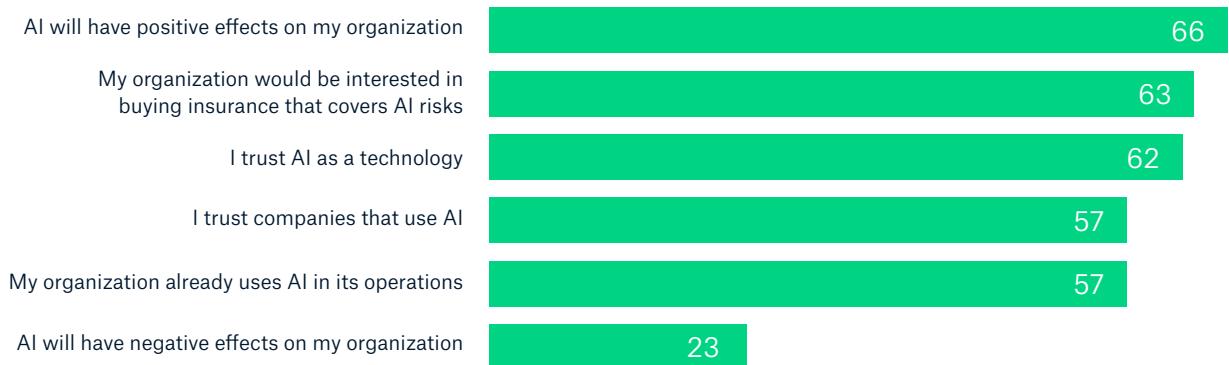
© Munich Re, 2026

A closer look at AI reveals both its strategic importance and a high degree of trust. Today, 57% of organisations already use AI in their business operations, a figure expected to continue rising. While only 23% of global C-level respondents expect AI to have negative effects on their organisation, two thirds anticipate positive impacts. Their trust extends not only to the technology itself but also to companies applying it responsibly.

Artificial Intelligence (AI) in the spotlight

Global C-Level

%



© Munich Re, 2026

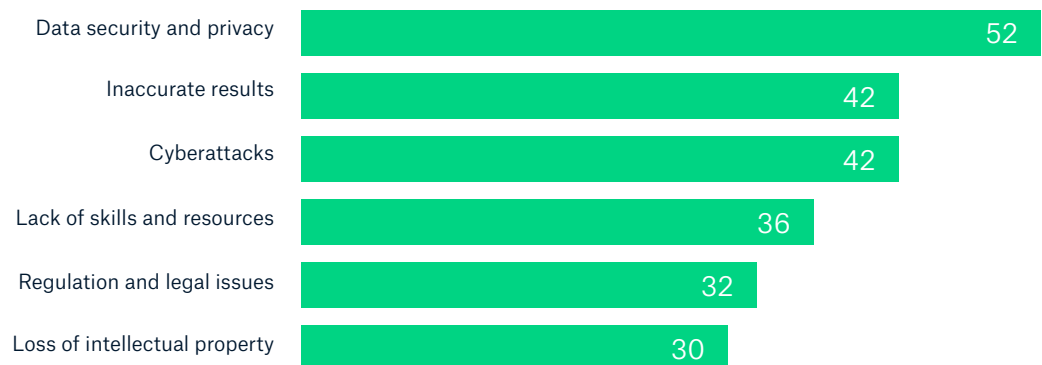
Despite the overall optimism, concerns remain. Executives emphasise the need to integrate AI responsibly into business processes, ensuring that opportunities are capitalised on, while risks – including model misuse, data exposure and operational errors – are minimised.

Key concerns regarding Artificial Intelligence

What worries you most about using or implementing AI in your organization

Global C-Level

%



© Munich Re, 2026

AI-related exposures in cyber insurance

AI introduces a broad range of exposures across both first-party and third-party risk categories, with particular sensitivity in Media Liability and Technology E&O policies. In most cyber policies, AI falls under the standard definition of computer systems, meaning it may typically be covered even when not explicitly referenced.

Cloud dependencies are crucial for business operations

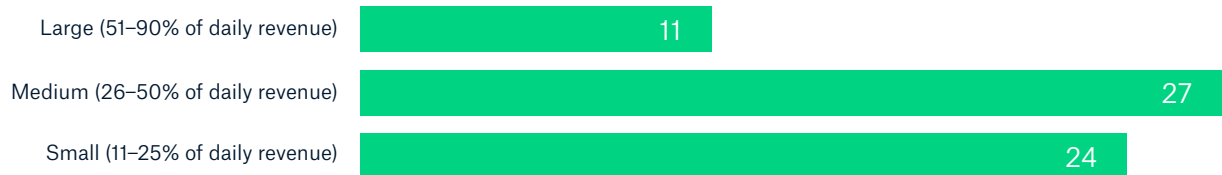
Although AI is considered to be more strategically relevant, usage of cloud services is far more deeply embedded in current operations. While 57% of companies use AI, an overwhelming 98% rely on cloud services – reflecting the central role that cloud providers play in today’s digital economy. This reliance underscores the need to assess and quantify potential risks arising from cloud outages, whether malicious or accidental.

Cloud dependencies and the substantial loss potential associated with cloud disruptions are key reasons why Munich Re models cloud outages in a dedicated accumulation scenario. Efforts to more precisely quantify such scenarios will help to further grow confidence in this line of business.

Financial impact of a 1-day cloud outage

Global C-Level

%



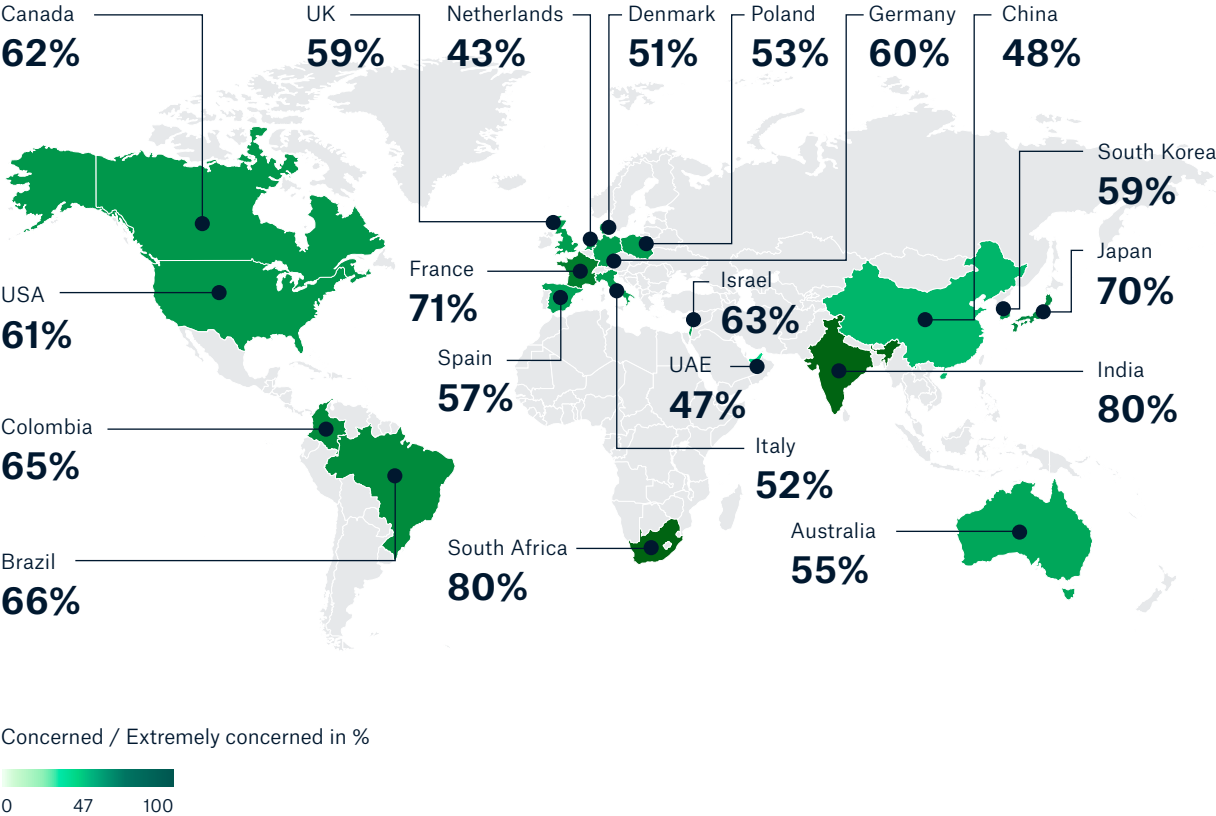
© Munich Re, 2026

3. High levels of concern amongst decision-makers

Concerns about cyberattacks vary significantly across regions. Respondents from South Africa, India, France and Japan reported the highest levels of concern, while those in the Netherlands, the Emirates and China were more relaxed in their assessments. The world map below visualises the proportion of C-level executives who stated that they were “concerned” or “extremely concerned” about the possibility of a cyberattack on their company.

How concerned are you about a potential attack on your company? (C-Level)

Global Average: 60%



© Munich Re, 2026

Rising impact of cyberattacks on companies

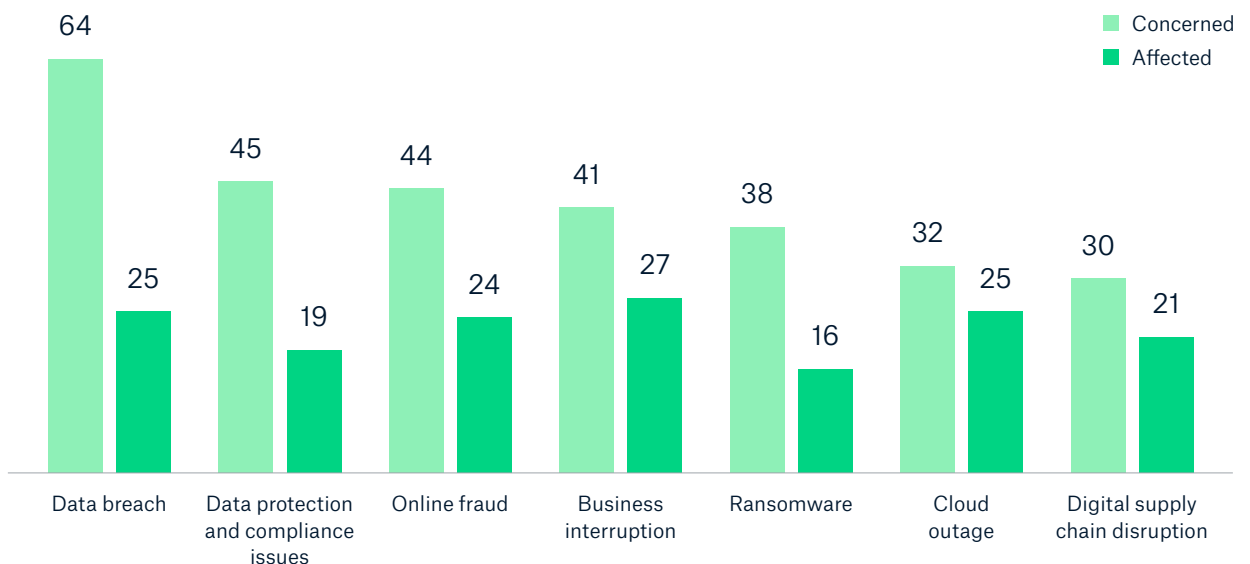
The survey not only captures executives' concerns but also examines the types of cyber incidents that organisations have experienced. Findings, backed by global threat data, clearly show that these concerns are justified.

While the level of concern exceeds actual experience, the gap is narrowing as attacks grow more frequent and sophisticated.

Cyber threats: C-level concerns compared to actual events affecting their companies

Global C-Level

%



© Munich Re, 2026

From Munich Re's perspective, major insured loss drivers include ransomware, data breaches, and fraudulent activities such as Business Email Compromise (BEC) and Distributed Denial of Service (DDoS). In addition, non-malicious events, such as cloud outages, are increasing.

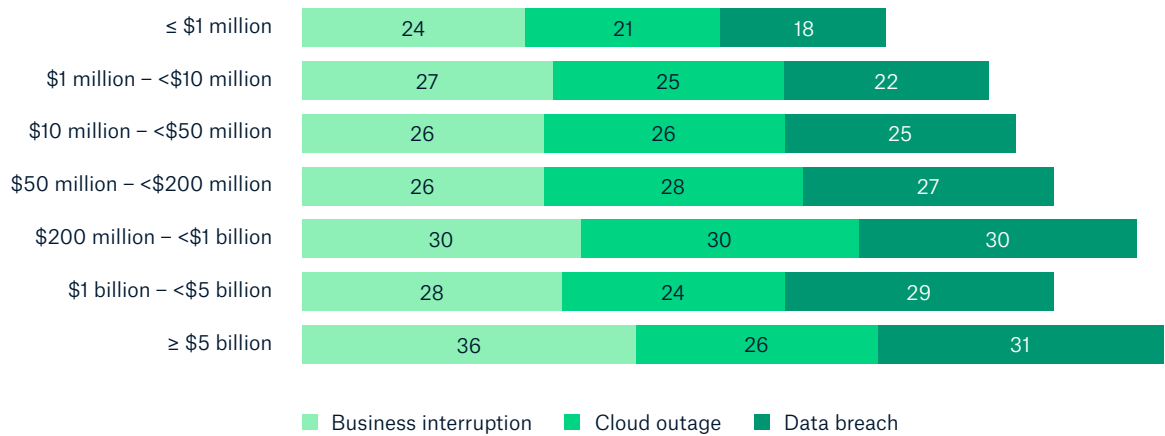
Company size appears to influence exposure; however, both small and large organizations encounter similar risk patterns.

Cyber threats

Which of the following has your company ever been affected by?

Global C-Level

% (Annual Revenue in USD)



© Munich Re, 2026

Munich Re experts expect cybercrime to become increasingly automated and democratised through the widespread use of AI tools – lowering the skill level required to launch an attack. This will expand access to sophisticated attack capabilities, amplifying threats particularly for micro and mid-sized companies. The assumption that “my company is too small or uninteresting to be attacked” is now obsolete. As a result, cyber insurance will be indispensable for organisations of all sizes in the future.

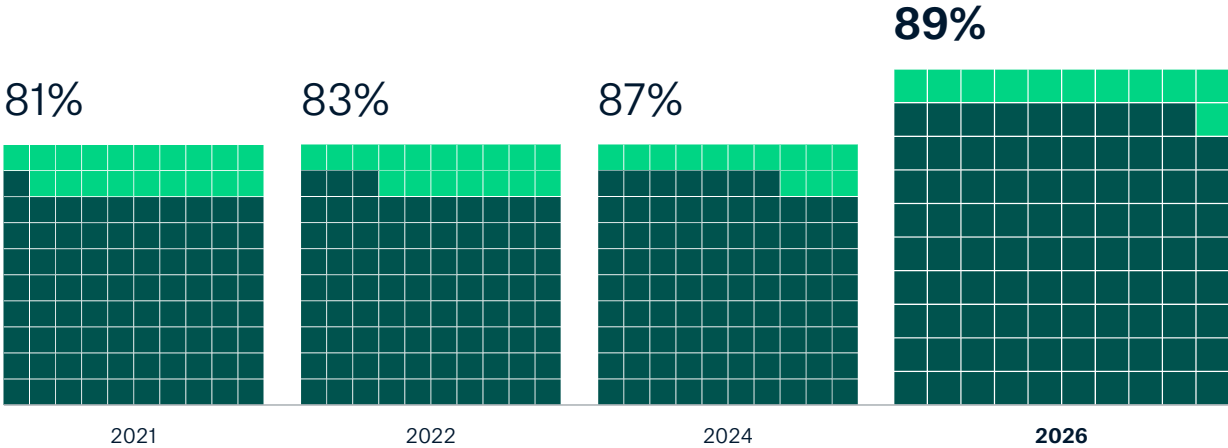
4. Cybersecurity preparedness and resilience remain insufficient

Despite high levels of concern, awareness, and first-hand experience with cyberattacks, resilience levels still have room for improvement. 89% of global C-level respondents feel that their company is not adequately protected – up from 81% in 2021. Considering the current risk landscape and the increasing frequency and severity of cyber incidents, this self-assessment is concerning.

Cyber threats

Our company is not adequately protected against cyberattacks.

Global C-Level



© Munich Re, 2026

This reflects persistent challenges facing IT security and risk management teams. Despite technological advances, human factors remain key to defending against cyberattacks.

Cyber threat defense

What are the main challenges in improving cyber threat defense in your company?

Global C-Level

		2026
	Low security awareness among employees →	40%
	Lack of human resources/skilled personnel →	31%
	Poor integration/interoperability of security solutions →	30%
	Lack of budget →	24%
	Digital supply chain dependency →	23%

© Munich Re, 2026

5. Unlocking the potential of cyber insurance in an expanding market

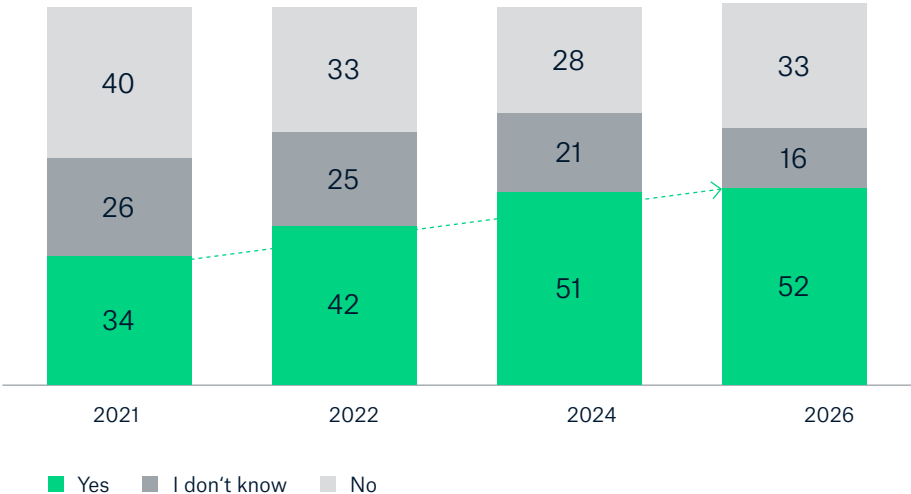
The business potential for cyber insurance remains high, as a substantial share of risks is still uninsured. Munich Re’s survey highlights emerging interdependencies, growing threat levels and – crucially – increasing interest in cyber insurance.

One key aspect is that many decision-makers still haven’t been offered cyber insurance. Expanding distribution and improving product transparency will be essential to unlocking the full economic and societal value of cyber coverage.

Cyber sales

Has commercial cyber insurance ever been offered to your company?

Global C-Level
%



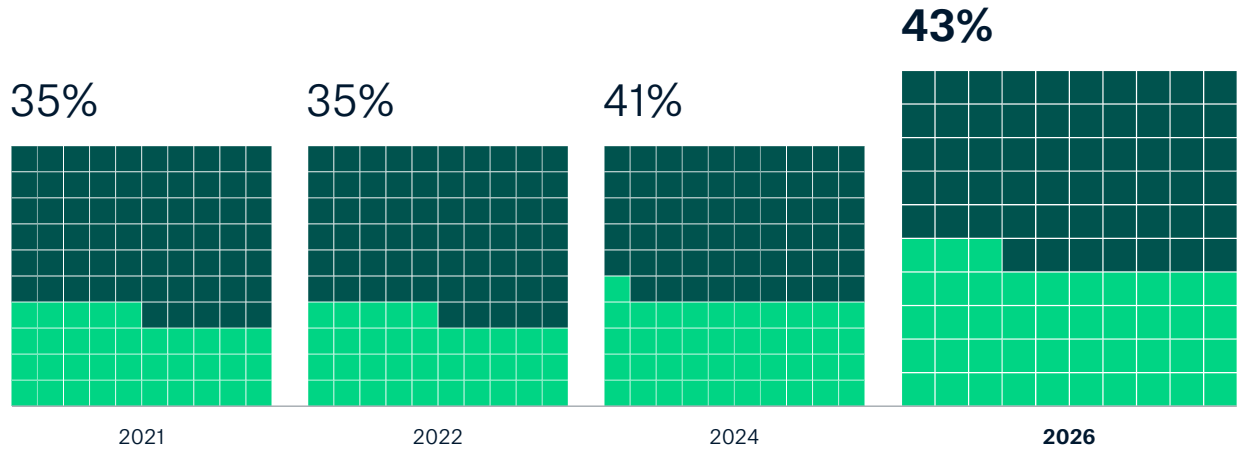
© Munich Re, 2026

Most C-level respondents are actively seeking information about cyber insurance. If the industry succeeded in clearly demonstrating the protective value of cyber coverage, a significant proportion of executives would consider purchasing a policy.

Would you take out cyber insurance for your company?

Global C-Level

My company is considering taking out an insurance policy and will very likely do so.



© Munich Re, 2026

From an insurance perspective, the main reasons for buying cyber insurance are self-evident:

Major reasons for companies to have cyber insurance

Global C-Level

		2026
	To reimburse financial losses in case of business interruption	48%
	To reimburse financial losses in case of liability	48%
	To get access to expert support and services	43%
	For peace of mind	39%
	Because business partners or clients require it	21%

© Munich Re, 2026

6. Conclusion: Building resilience – Munich Re’s commitment to cyber insurance

Digitalisation is transforming the global economy and our everyday lives. AI has become a defining technological force, shaping innovation and competitiveness across industries. While expectations regarding its positive impacts remain high, organisations must also proactively address emerging risks.

Demand for cyber insurance is expected to grow, as it is increasingly seen as indispensable. It provides comprehensive protection, enabling companies to overcome severe financial losses from cyberattacks and digital disruptions.

Munich Re is committed to supporting these efforts by advancing its modelling capabilities, sharing its expertise, and collaborating across sectors. Our goal is to strengthen protection for organisations of all sizes and help build a sustainable digital world.



“Companies need to place the highest priority on resilience and protection in the face of evolving digital opportunities and challenges. Navigating the dynamic cyber landscape calls for adequate C-level action. Munich Re supports the efforts to strengthen business resilience. Leveraging strong underwriting expertise, threat intelligence, claims data analytics, and advanced accumulation modelling, cyber experts at Munich Re transform evolving cyber threats into effective insurance solutions. As vital part of corporate risk management, cyber insurance is proven, relevant, and ready to expand.”

Thomas Blunck
CEO Reinsurance

Gain detailed insights on cyber risks and insurance

Munich Re’s cyber experts and client managers are available to provide deeper insights, additional data and country-specific analyses based on our Cyber Risk and Insurance Survey 2026.

7. Methodology of the survey

The survey was conducted on behalf of Munich Re by the global market research company Statista in December 2025 and analysed with Munich Re's internal experts in January and February 2026.



Respondents

- Global: More than **9,500** in total in **20** countries
- Representative results globally and for each country
- Results representative for commercial and private lines business through C-Level/employee split



Company sizes

- 1–9 employees: **12 %**
- 10–249 employees: **36 %**
- 250–2,499 employees: **29 %**
- ≥2,500 employees: **21 %**



Countries

- Australia
- Brazil
- Canada
- China
- Colombia
- Denmark
- France
- Germany
- India
- Israel
- Italy
- Japan
- Netherlands
- Poland
- South Africa
- South Korea
- Spain
- UAE
- UK
- USA



Company's annual revenues

- <\$1m: **15 %**
- \$1m–\$10m: **19 %**
- \$10m–\$50m: **14 %**
- \$50m–\$200m: **12 %**
- \$200m–\$1bn: **10 %**
- \$1bn–\$5bn: **10 %**
- ≥\$5bn: **5 %**



Surveyed industries

- Consumer Products: **4 %**
- Education: **9 %**
- Energy, Utilities: **3 %**
- Finance: **9 %**
- Healthcare, Pharma: **7 %**
- Industry, Manufacturing: **9 %**
- IT: **16 %**
- Professional Services: **10 %**
- Public Authority, Defence: **5 %**
- Telecommunications: **3 %**
- Tourism, Entertainment, Media: **4 %**
- Transportation, Logistics: **6 %**
- Other: **16 %**



Position

- Management/CEO: **11 %**
- Division Management: **10 %**
- Team/Department Mgmt.: **22 %**
- Employee: **48 %**
- Self-employed/Freelancer: **8 %**

Get in touch



Martin Kreuzer

Senior Risk Manager Cyber Risks

E-Mail: MKreuzer@munichre.com



Axel von dem Knesebeck

Corporate Underwriting Cyber

E-Mail: AKnesebeck@munichre.com

© 2026

Münchener Rückversicherungs-Gesellschaft
Königinstrasse 107, 80802 München, Germany

Picture credits: da-kuk / Getty Images;
Andreas Pohlmann

Münchener Rückversicherungs-Gesellschaft (Munich Reinsurance Company) is a reinsurance company organised under the laws of Germany. In some countries, including in the United States, Munich Reinsurance Company holds the status of an unauthorised reinsurer. Policies are underwritten by Munich Reinsurance Company or its affiliated insurance and reinsurance subsidiaries. Certain coverages are not available in all jurisdictions.

Any description in this document is for general information purposes only and does not constitute an offer to sell or a solicitation of an offer to buy any product.