

NOT IF, BUT HOW

Munich RE 



Munich Re Global Cyber Risk and Insurance Survey 2022

Better understanding of our client's needs

More action required for higher cyber resilience

Anticipating the risks of tomorrow is embedded in our DNA at Munich Re, which is why we have been involved in managing cyber risk from the first moment it became a consideration - and continue to keep pace with its lightning-fast development. As the challenges this risk class poses to the global economy grow, we, and the insurance industry as a whole, need to provide proper solutions capable of addressing risk capacity and sustainability for this line of business.

The numbers clearly show that the need for cyber security and insurance is increasing steadily: Munich Re estimates global cyber premiums to be \$9.2 billion (beginning of 2022) and expects that they will reach approximately \$22 billion by 2025. Given the ever-increasing frequency and severity of cyber-attacks, our survey reveals that the insurance gap is disproportionately high. And the mismatch between risk awareness and implementation of protection measures and the need for more capacity for larger risks remains a real challenge in what is an increasingly difficult environment for the entire insurance industry.

2021 serves as a good example of this mismatch. It witnessed multiple ransomware attacks which also targeted supply chains and critical infrastructure. These wide-spread attacks and newly discovered security vulnerabilities continue to raise awareness among the public along with decision-makers in business and politics. In addition, possible state-sponsored cyber-attacks from all sides are putting additional pressure on the limits of insurability.

Our task is to understand the main obstacles to adopting proper cyber solutions and services for businesses and individuals, as well as the pain points the global economy faces when it comes to cyber preparedness. In order to get first-hand insight into these questions, as well as to assess the general level of knowledge on contemporary cyber insurance solutions in the market, Munich Re expanded its Global Cyber Risk and Insurance Survey to obtain a representative overview of the status quo.

The survey we conducted included 7,000 participants from 14 countries, all industries and company sizes, and covered the topics of risk awareness, threat exposure for companies and private individuals, and the role of cyber insurance with its cover elements and services.

Better be safe than sorry.



„Cyber insurance is fundamental for the successful digitalisation of the economy. Munich Re continues to offer capacity, and our goal as market leader is clear: to jointly develop innovative, datacentric cyber solutions with our clients and partners.

Our offering increases our insureds' resilience and improves the protection of digital business models. Munich Re significantly contributes to a sustainable market, which is essential for our clients.“

Torsten Jeworrek, Member of the Board of Management



„Our approach in cyber insurance is unchanged: disciplined in underwriting and stringent in risk management. Our experts continually refine our internal models on the basis of our own and third-party data, and with a particular focus on accumulation

risks. We are in constant dialogue with our cedants and model providers regarding current cyber threats and accumulation scenarios to ensure that our approaches are state-of-the-art at all times. Volatile cyber insurance business can only be written sustainably and reliably for clients under these conditions.“

Jürgen Reinhart, Chief Underwriter Cyber

Contents

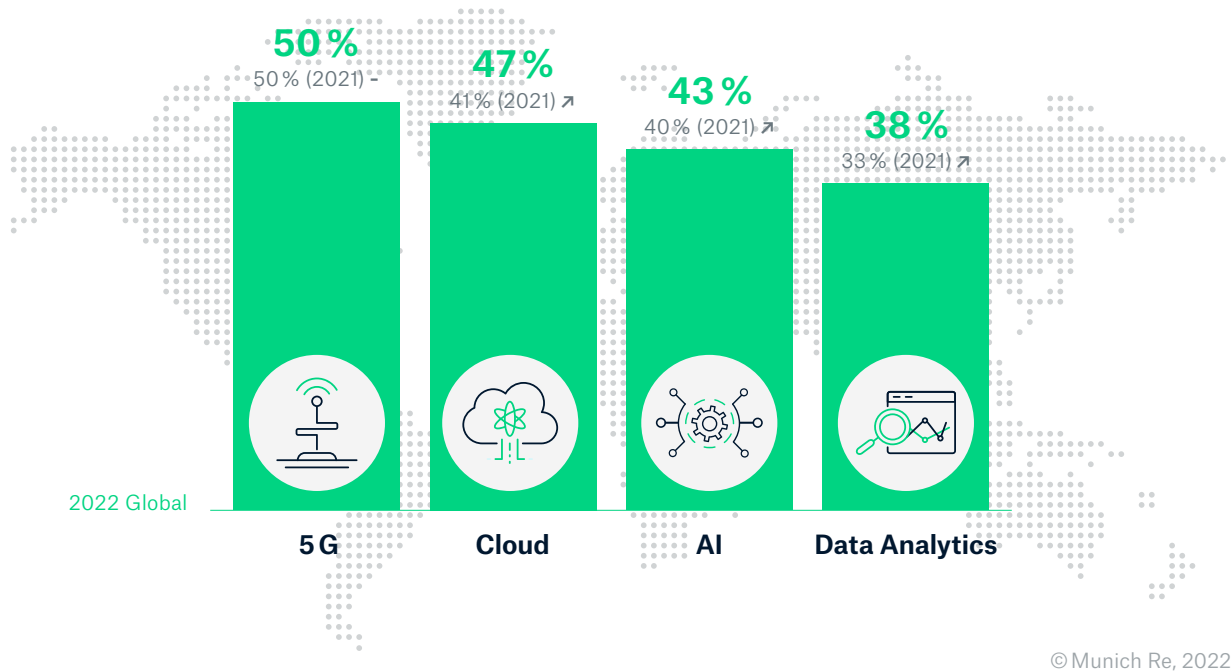
	1. Management Summary	05
	Survey Result Highlights	
Commercial Cyber	2. Risk awareness	07
	3. Cyber threat landscape	10
	3.1 The main cyber threat vectors	10
	3.2 The status of the economy's cyber threat defense	11
	4. Commercial cyber insurance	12
	5. Protection measures, pre- and post-incident services	16
Personal Cyber	6. Cyber security in private life	18
	7. Boosting Cyber Resilience	23
	8. Methodology of the Survey	25

1. Management Summary

Digitalisation in most areas of business and life continues unabated. And all companies surveyed are focusing more strongly on new, smart technologies. The list of technological drivers is headed by 5G, cloud services, artificial intelligence, and data analytics. Highly IT-oriented countries like India and China, as well as South Africa and Brazil lead the list of nations that see the biggest potential in digitalisation. Only 12% of C-Level participants surveyed do not consider digital trends in 5G, cloud services, AI and data analytics relevant to their businesses.

Everyone believes in digitalisation

What are the most relevant technology trends for your company? (C-level)



In line with these developments, security vulnerabilities and cyber-attacks are also on the rise. **On a global level, attacks such as online fraud, ransomware and data theft increased year-on-year as our data shows.**

Although awareness among surveyed managers, beyond incidents they themselves experienced, has risen by nearly 10% since our global survey in 2021, the perception of the threat landscape and what needs to be done to properly address it still varies greatly by country.

As a result, protection measures remain relatively low. For example, **83% of surveyed representatives said that their own company is not adequately protected against digital threats.** This high number comes as a surprise in light of the fact that business models increasingly rely on digitalisation and that awareness of associated threats is high. The need for action is clear.

83% of all C-Level respondents globally report that their company is not adequately protected against cyber threats



© Munich Re, 2022

On a positive note, compared to the previous year, the availability of cyber insurance appears to have gained further traction, as there has been a 21% increase in the number of companies that have already taken out cyber insurance. Currently, 35% of the decision-makers surveyed are also considering taking out cyber insurance as an essential part of their risk management. According to the survey, interest in cyber insurance is cross-sectoral. However, even in more mature cyber markets like the US, too many respondents have still had no contact with an insurance provider to inform themselves about security solutions and insurance protection against digital threats and potential cyber incidents. The insurance industry has yet to be commonly perceived as part of the solution.

The situation is no different in private life. Here, the discrepancy between risk awareness and underinsurance is even higher. We must assume that the far-reaching consequences of a cyber-attack have not penetrated the consciousness of most individuals. It is likely that many consider themselves not attractive enough to hackers and that any potential consequences of a security breach would be minor.

Overall, the responses to the comprehensive questionnaire in our survey underscore the need for the global insurance industry to increase efforts to make cyber risks more visible, conditions more understandable, and products easier to assess. Adequate risk management is a prerequisite for cyber insurance and poses major challenges for all stakeholders.

One thing is clear: Digital disruption is progressing on a global level and associated dependencies are advancing enormously – and they make no allowance for those who are not sufficiently prepared. In response, the insurance industry has proven that it can provide real value-add for its clients with comprehensive solutions that adapt to the rapidly changing risk landscape. Munich Re, in particular, constantly innovates as a leading cyber reinsurer. We offer primary insurers and corporates long-standing expertise, sophisticated solutions, and adequate coverage.

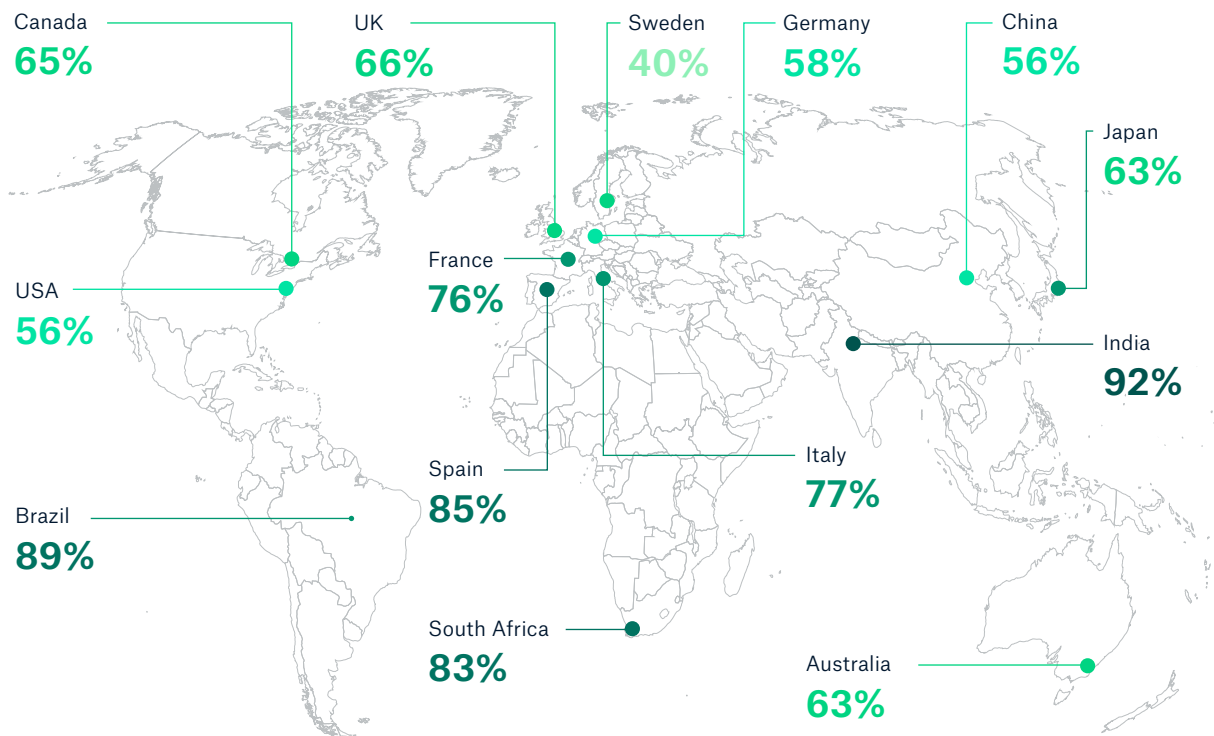
In the following chapters we go into further detail on our survey results. For comprehensive country-based insights, as well as for more information about our products and services, please contact your Client Manager or our cross-divisional team of cyber experts at Munich Re.

2. Commercial Cyber: Risk awareness

According to our survey, there are drastic differences in cyber risk awareness across the globe: North American and Northern European as well as Australian and some Asian markets are quite concerned about a potential cyber-attack. Southern European, Latin American, African, and Indian C-Level respondents are highly concerned. The most concerned market from last year, Brazil, was superseded by India, which was surveyed for the first time. In India, 92% of C-Level management stated that they were concerned or extremely concerned about a cyber-attack. As in the previous year, the counterweight to this sentiment rested in Northern Europe – where Sweden continues to take a relaxed approach to the threat: 23% of the Swedish C-Level is not at all concerned about a potential cyber-attack. This comes as a surprise as Sweden is one of the most digitalised countries in the world and its companies were also among the 86% of respondents that answered that they are not adequately defending themselves against cyber threats.

The world map below shows the percentage of C-level executives concerned about a potential cyber-attack on their company.

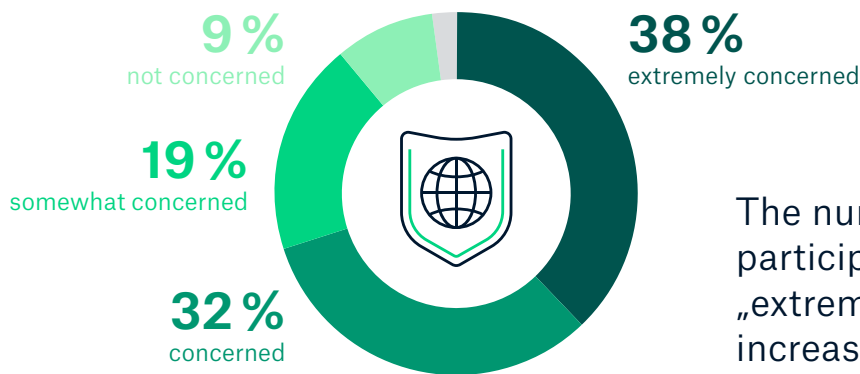
How concerned are you about a potential attack on your company?



© Munich Re, 2022

It is striking that the SME segment (small and medium-sized enterprises) seems to have the fewest concerns: 39% of C-Level respondents are not or only somewhat concerned. Our overall assessment repeatedly shows that this segment has dealt with the topic the least and is furthest away from so-called cyber-readiness. Yet, it is in this segment that losses are far more devastating in relation to company revenue than in large companies that usually have more resources to cope with a cyber-attack.

How concerned are you about a potential attack on your company?



The number of C-level participants who are „extremely concerned“ has increased from 30 to 38%.

© Munich Re, 2022

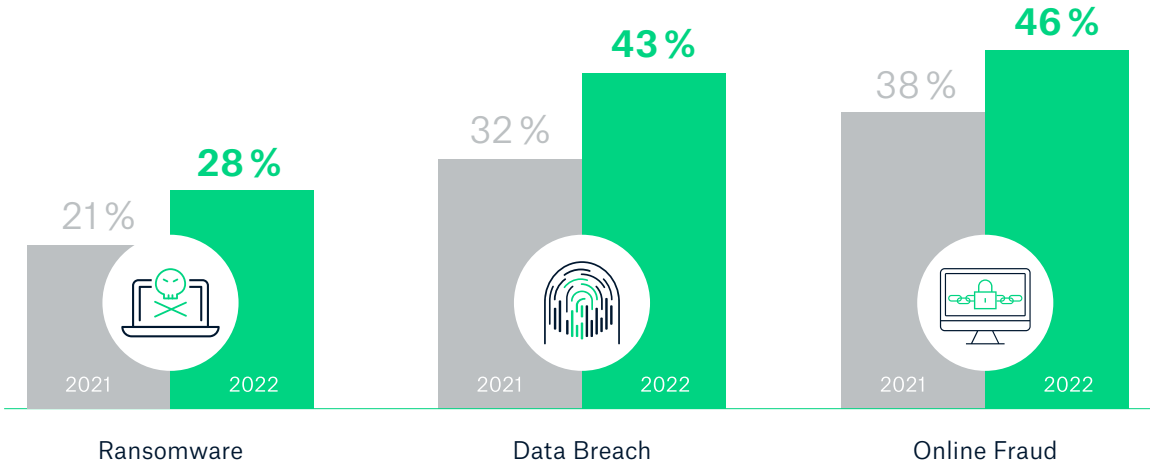
On the other hand, it is not surprising that, among survey participants, the C-levels in the IT, finance and telecommunications sectors have the highest level of alertness. The public sector, on the other hand, is the most relaxed about the situation as only 61% are concerned or extremely concerned which is the lowest value in comparison.

3. Commercial Cyber: Cyber threat landscape

Publicly visible attacks like the Colonial Pipeline ransomware attack show only a slice of reality. Countless low-threshold attacks are targeted at individuals and smaller companies en masse. These are barely publicised but, in total, generate damage running to billions of dollars. Little wonder that the still relatively young “business field” of cybercrime-as-a-service is booming, with the capability to inflict damage on virtually anyone in cyberspace. The key for all decision-makers is to understand the “why, how, and what” of attacks along with any potential vulnerabilities they might have – and then effectively arm themselves through prevention, recovery, and risk transfers.

3.1 The main cyber threat vectors

Which of the following have you ever been affected by?

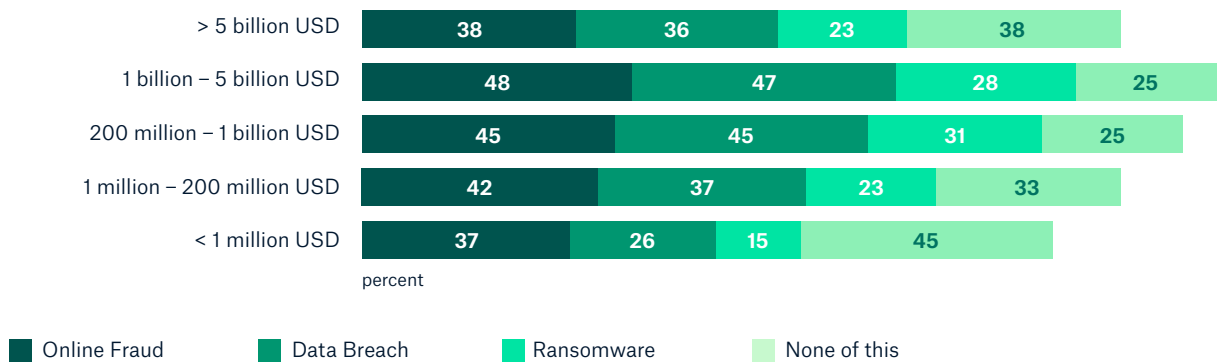


© Munich Re, 2022

Our survey shows that more than 71% of respondents have already been affected by ransomware or a cyber-attack causing fraud or breach of data. Online fraud tops the list of attack vectors at 46%, just ahead of data breach (43%), followed by ransomware (28%). Companies with revenue between \$200 million and \$5 billion are the most affected. Large corporations (over \$5 billion in sales) with the highest prevention capabilities and IT budgets are still heavily affected at 60%, but seem to be somewhat better protected.

Companies affected by cyber crime

Which of the following have you ever been affected by? (Global total)



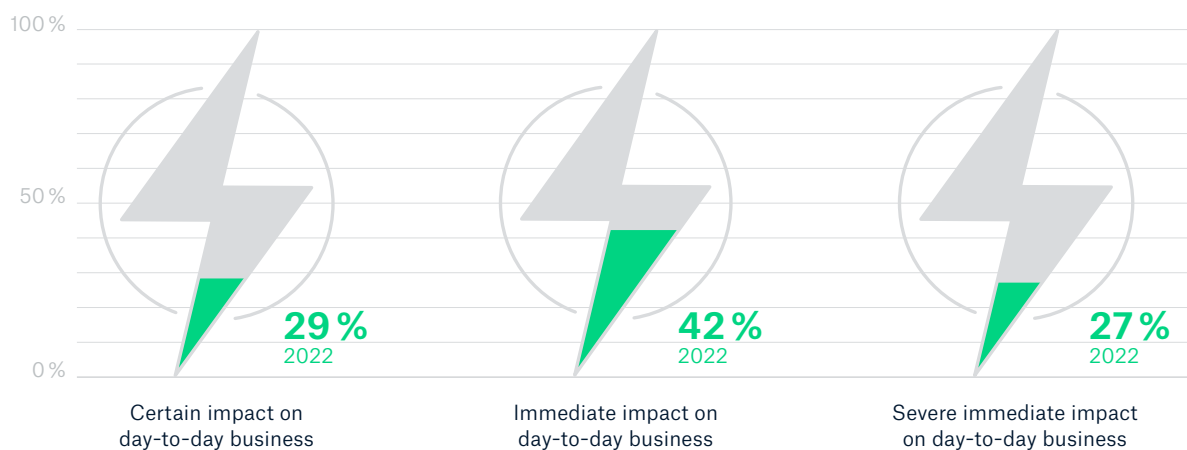
© Munich Re, 2022

Looking at our results regionally, we see that India, China and South Africa rank among the top three affected countries overall. Across all attack types, there has been a significant increase in cases in each region since our last global survey.

With regard to ransomware attacks, 98% of C-level respondents said the attack had an impact on day-to-day operations: in 42% of cases, the incident had an immediate impact, and in 27%, an even worse severe immediate impact on day-to-day business. These numbers illustrate the immense threat posed by a digital weapon like ransomware.

Impact of ransomware attacks

How strong was the impact of the ransomware attack on a day-to-day business?



© Munich Re, 2022

Unlike the results on awareness and protection measures, the clustering of results by company size for this question shows that there is little difference between small and large companies in terms of impact and damage when a cyber incident occurs: 95% of companies with revenues of up to USD 1 million also suffered a direct negative impact on their day-to-day business.

3.2 The status of the economy's cyber threat defense

On average, at a global level 83% of all C-Level respondents report that their company is not adequately protected. Given the risk landscape and the frequency and severity of cyber incidents, the self-assessment of C-level participants remains disappointing. The percentage of those who said that their organisation is not adequately protected against cyber-attacks ranged from 74% to 93% across all countries surveyed. The U.S., as the most saturated cyber market, shows the highest confidence in its protective measures with 26%. On average, every second company has already been affected by online fraud or data breach incidents, and every 5th by ransomware attacks. The human factor plays the biggest role in the eyes of the respondents: unwary employees and too few or inadequately trained staff are the top 2 reasons given, followed by poor integration of security solutions and lack of collaboration between individual departments.

What are the main challenges in improving cyberthreat defense in your company?



© Munich Re, 2022

In addition, with regard to the above-mentioned awareness data (58% concerned or extremely concerned), it is surprising to see that the level of concern about a potential attack is disproportionately lower than the knowledge of one's own unprotectedness (83%). This clearly shows that cyber incidents are still underestimated in terms of their impact on business operations and their far-reaching financial consequences.

4. Commercial Cyber Insurance

The business potential for the insurance industry remains extremely high in the cyber line of business. However, the results of our study show that the insurance industry must become even more active in sales and explanation. In addition to necessary educational work (as described in the course of the study), the insurance industry must emphasise the cyber topic more strongly in discussions with its clients and seek dialogue. Compared to the previous year, the first-contact ratio has improved significantly, but the percentage of those who have never been offered cyber insurance by their insurer is still surprisingly high at 33%.

Cyber offering

Has commercial cyber insurance ever been offered to your company? (Global C-Level)



© Munich Re, 2022

According to our results, 35 % of C-level participants are considering cyber insurance for their company. This shows significant business potential for the insurance industry.

Company cyber insurance status

Would you take out a cyber insurance policy for your company?



2022 Global
(C-Level)
n = 2,404

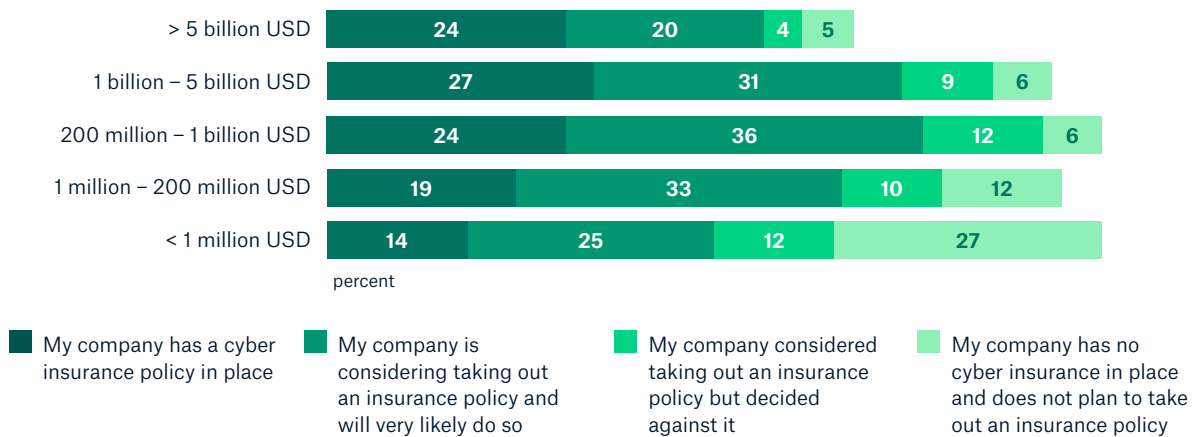
© Munich Re, 2022

Slightly more survey participants than in the previous year stated that they already have a cyber policy in place. However, while demand and the official market figures have indeed increased, global market figures overall still show a significant insurance gap with a penetration rate estimated below 5%.

Another 20% of respondents either actively decided against cyber insurance or didn't consider insurance protection at all.

Companies affected by cyber crime

Would you take out a cyber insurance policy for your company?

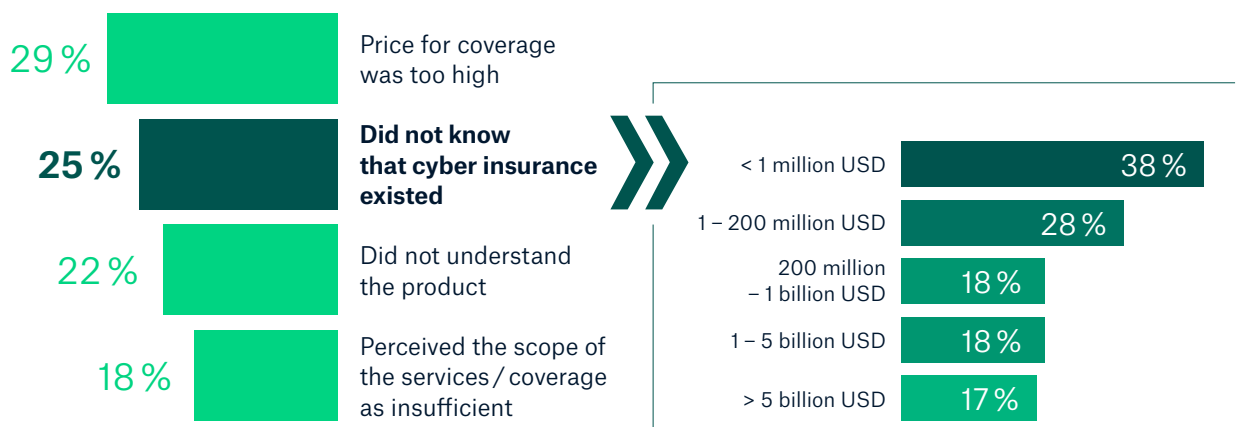


© Munich Re, 2022

A closer look at the data shows that large companies with high revenues are particularly aware of the risk of cyber-attacks and the benefits of holistic cyber insurance. Here, the percentage of those who have decided against an insurance policy is significantly lower. Among companies with more than \$5 billion in revenue, only 4% explicitly decided against cyber insurance and only 5% did not even consider it at all.

Why does your company have no cyber insurance in place?

Global (C-Level)



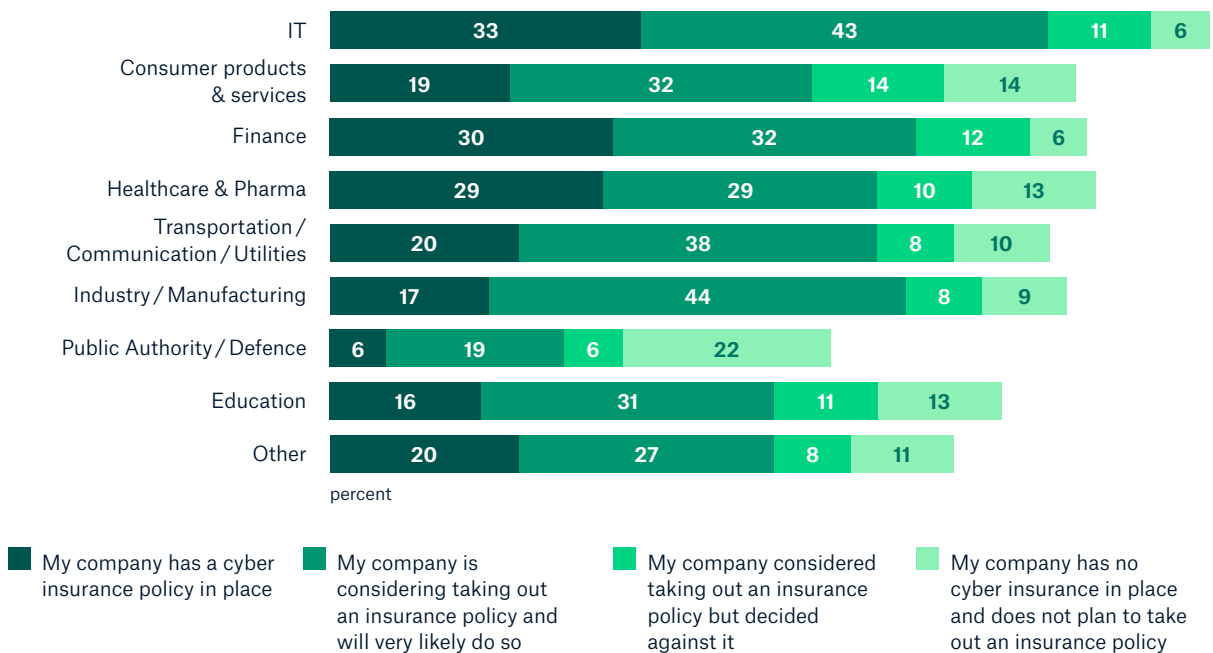
© Munich Re, 2022

Taking into consideration that a significant amount of the C-level respondents that have no cyber policy in place seem to be totally unaware of the opportunities that holistic cyber solutions offer, there are untapped business opportunities even here. They either stated that they did not know that cyber insurance exists (25%) or that they did not understand the product (22%). Again, particularly in the SME segment, the lack of knowledge about risk transfer solutions was highest at almost 40%. In view of the average loss figures, however, the cost-benefit calculation would be more than clearly in favour of a cyber insurance solution, in particular for the SME segment. These numbers emphasise the need of more wording standardisation to avoid any ambiguities. There is a clear need for the insurance industry to better explain their solutions to the market.

On the positive side, IT (33%), healthcare/pharma (29%) and finance (30%), which are the sectors most affected by cyber-attacks, have the highest values in terms of insurance contracts already concluded. When it comes to the specific consideration of taking out an insurance policy, the manufacturing industry shows the highest values at 44%. Particularly in view of the increasing number of ransomware and supply chain attacks in recent years, this industry is coming under increasing pressure to deal with the threat situation.

Company cyber insurance status

Would you take out a cyber insurance policy for your company?

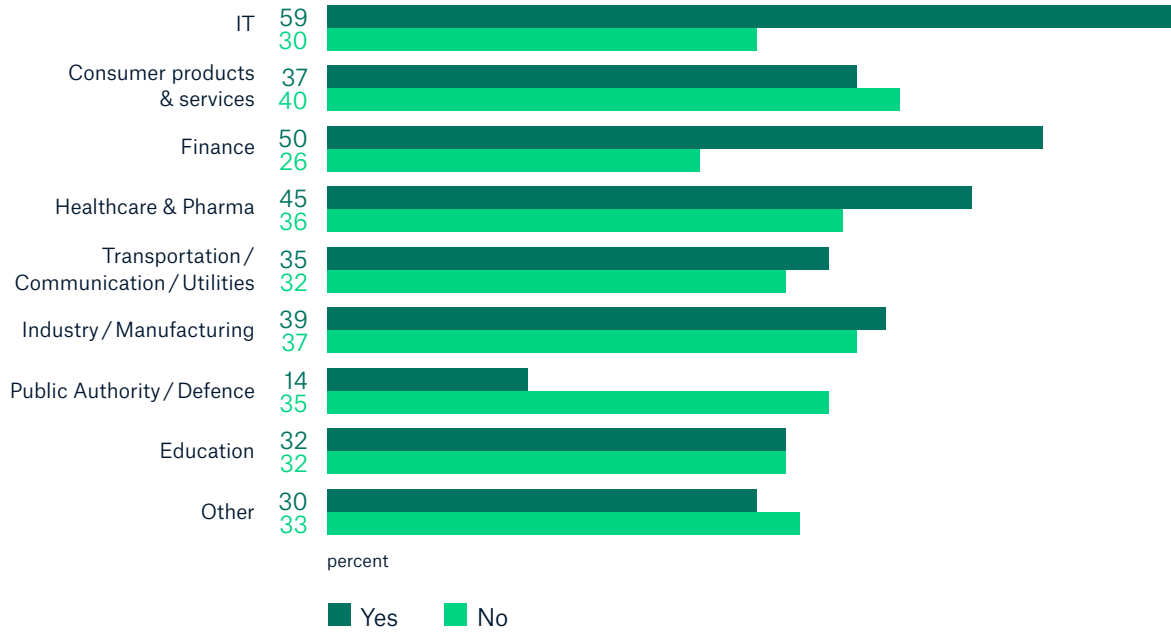


© Munich Re, 2022

These values are largely consistent in relation to the contacts between insurers and policyholders.

Cyber offering

Has commercial cyber insurance ever been offered to your company? (Global C-Level)



© Munich Re, 2022

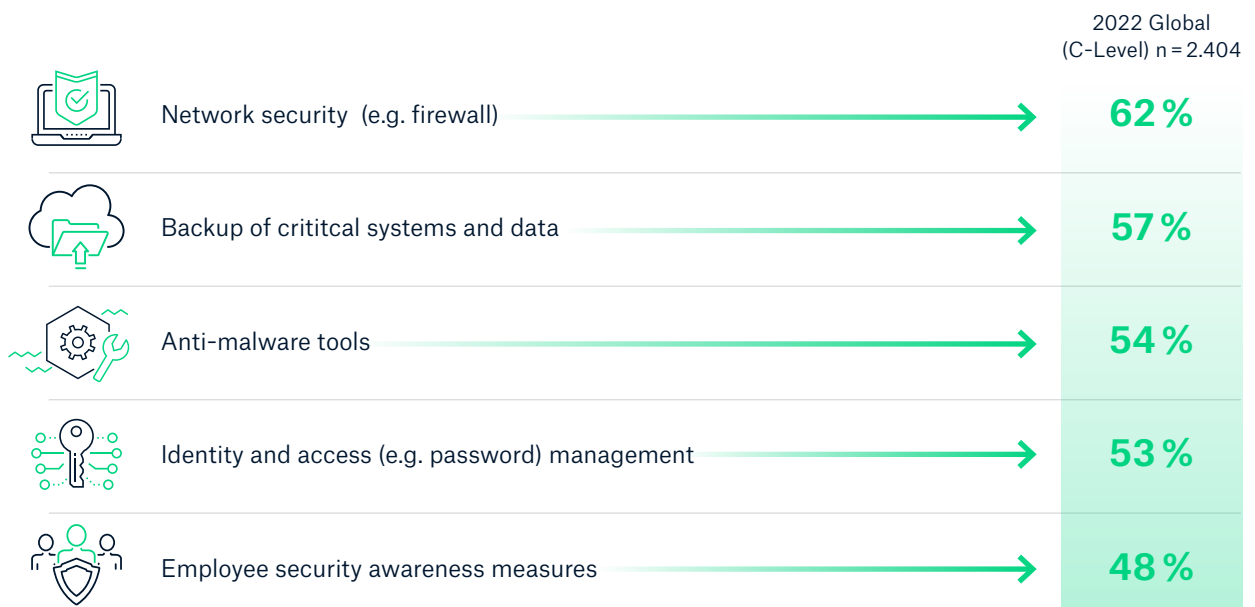
5. Commercial Cyber: Protection measures, pre- and post-incident services

The cyber insurance market has changed noticeably in recent years. In view of the high risk dynamics, a clear hardening of the market became apparent, capacity limits were reached, and underwriting guidelines became increasingly strict. Precisely because legal regulation or minimum security standards are still reluctantly implemented, the insurance industry must limit access to coverage and demand adequate security controls. The better the resilience of clients, the lower the risk for becoming a victim of a cyber-attack.

On average, at least half of respondents believe that precautionary measures such as network security, backups, identity management, anti-malware tools or employee training should be part of an insurance policy. The latter, in particular, is seen as one of the main reasons for insufficient cybersecurity. Again, the SME segment stands out with the lowest percentages and finds these precautionary measures most dispensable. On the other hand, most countries surveyed are aware that protection (even if not in conjunction with insurance) is important, ranging from 86% to 99%. Japan was the outlier here, with 22% saying they did not need any of these services.

Pre-incident services for commercial lines

Which of these services should be covered by cyber insurance solutions for protection against cyberattacks?



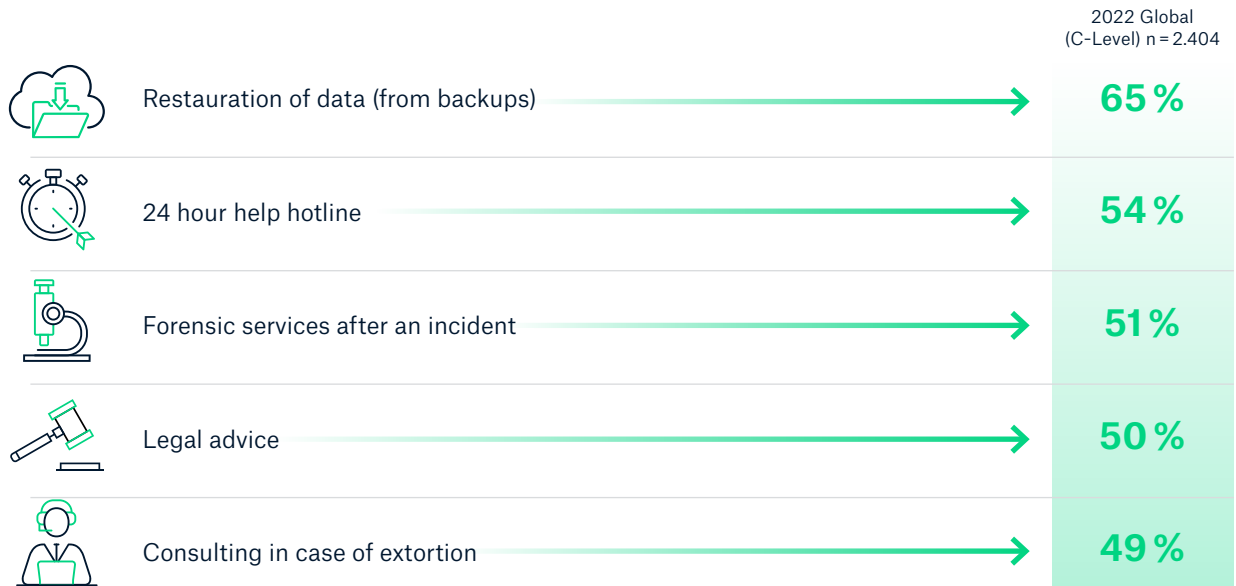
© Munich Re, 2022

For post-incident services, respondents focused on data recovery (65%), a help hotline (54%), forensic (51%) and legal advice (50%) after an attack. Only 36% saw the reputational aspect as a relevant post-incident factor. As described at the beginning of the chapter, while customers expect these services more from the insurance industry (25%) than from authorities or associations, half of the respondents (44-45%) expect these offerings more from the portfolio of cyber-security and IT service providers. On average 11% (2% less than last year) think they are fine without any post-incident-services.

Again, the SME sector and government agencies stand out and see the least benefit in post-incident services. And as in the case of preventive measures, Japan (21%) is the country most likely to think that it can manage without any services at all.

Post-incident services

Which of these services should be covered by cyber insurance solutions for recovery after a cyber incident?



© Munich Re, 2022

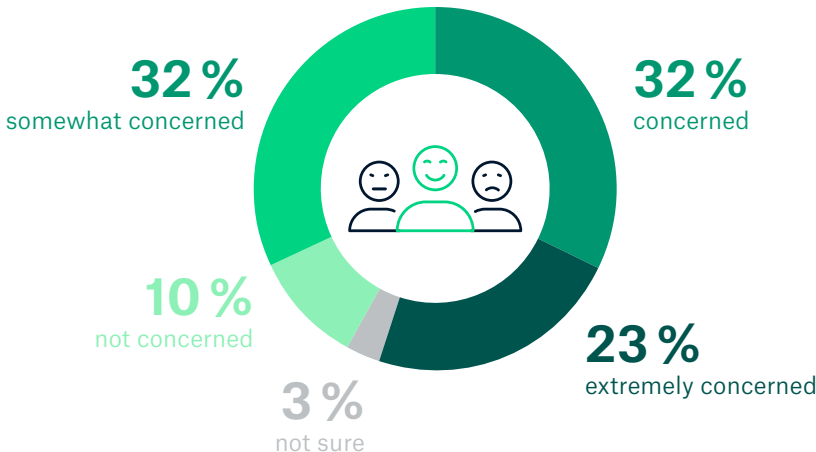
6. Personal Cyber: Cyber security in private life

The cyber threat business is not only profitable for criminals targeting companies. Private individuals also fall victim to cyber-attacks, and even if individual losses are smaller, the damage to the individual may be just as existential - or unpleasant at the very least - and could be mitigated by appropriate measures such as insurance. In the following chapter, we turn our attention to the private cybersecurity of the same individuals who answered our questions on corporate security – and their perception of their own exposure in private.

In terms of their own private cybersecurity, only 10% stated that they are not concerned at all. 55% were concerned or even extremely concerned about their digital security.

How concerned are you about a cyber attack in your private life?




2022 Global / n=7,004



© Munich Re, 2022

The high level of concern is no wonder, as 56 percent of respondents say they have already been the victim of a cyber-attack in their personal lives. Malware attacks as well as online fraud were the most common attacks, before private data breaches and identity theft. As with companies, attacks on the private lives of survey participants also show an increase compared to last year.

Have you ever been effected by one of the following?

		2022 Global (C-Level) n = 7,004	2021 Global (C-Level) n = 5,507
	Malware	20%	18%
	Fraudulent actions when buying or selling online	20%	18%
	Fraudulent transfers from my bank account	17%	15%

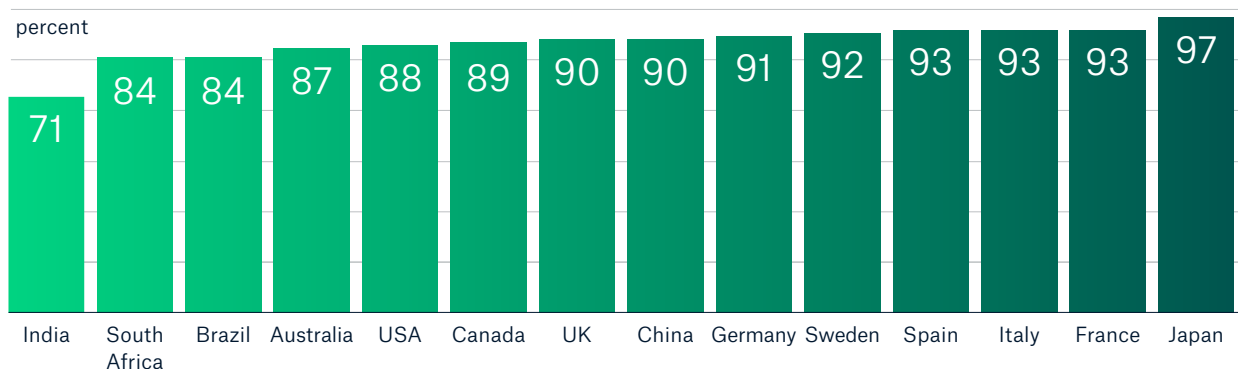
© Munich Re, 2022

In China, India, South Africa, and Brazil, most survey participants have already been the victim of an attack in private (65-77%). In the European countries surveyed, the number of people successfully attacked has increased by an average of approximately 10% since last year. At approximately 50%, Europe represents the average number of victims of private cyber incidents. Japan was the only country here to report fewer private cyber victims than last year and also the lowest number of victims overall at just 30%.

Surprisingly, Japan at 97% nevertheless remains the country with the greatest awareness that private protection against cyber-attacks is inadequate and could be improved. And while the question regarding personal cyber security status revealed a high level of awareness of insufficient protection overall, 48% of respondents still said that they were well or very well protected against cyber-attacks in their private lives.

However, the potential for improving one's own cyber security becomes apparent when one takes a look at the low scores of those who stated that their protection was very good: only 11%. Conversely, 89% are aware that they are not fully protected. The country comparison in the chart makes this potential for improvement even clearer.

Room for improvement with regards to cyber security

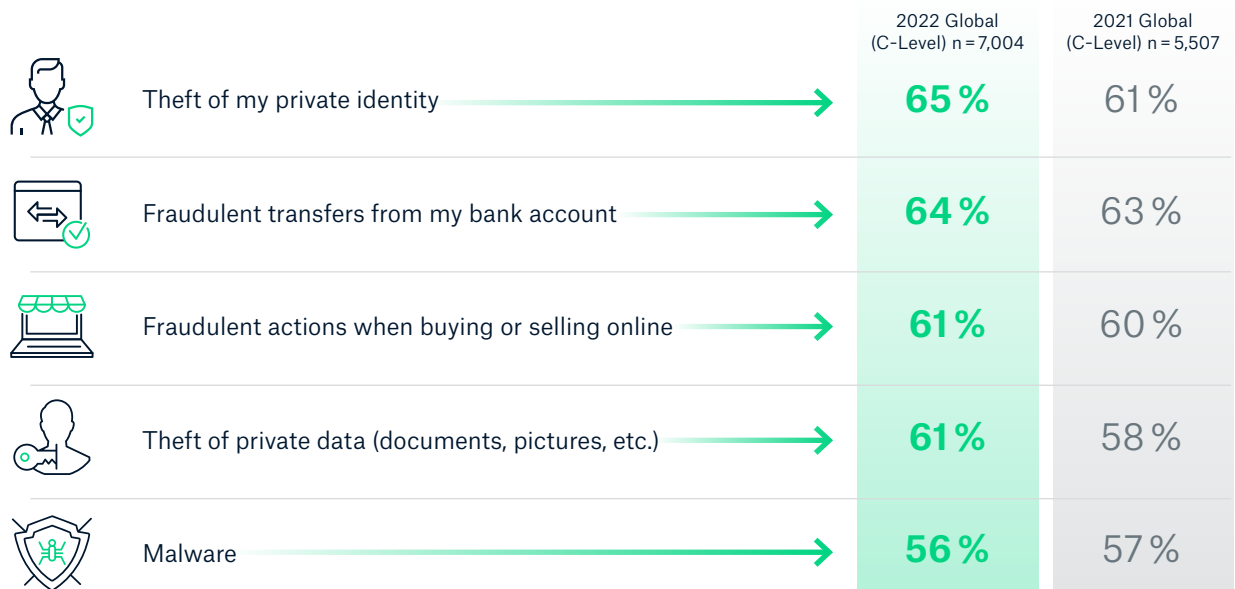


© Munich Re, 2022

Across the board online fraud, identity theft, and private data breach were the most feared cyber incidents.

Cyber concerns

What are your biggest concerns with regards to your cyber exposure in your private life?



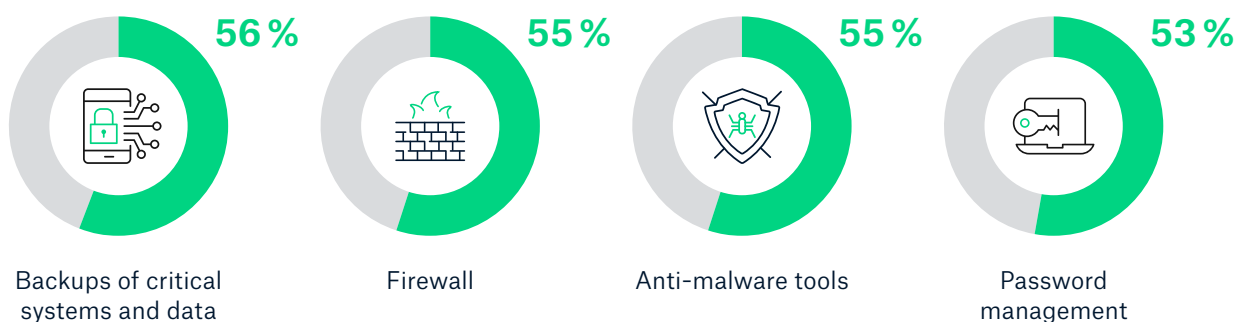
© Munich Re, 2022

The country average also clearly shows an improvement in understanding how important additional protective measures and assistance services are. Only 14% of respondents said they did not need any precautionary services and only 16% said they did not need any assistive services in the event of a cyber-attack.

More than half of those surveyed felt that the preventive services backup management, firewall, and other anti-malware protection measures were a useful part of a cyber policy. In terms of post-crisis measures, data recovery, help hotline, and legal advice were among the top three services. The need for post-incident services increased slightly year-over-year for all measures.

Pre-incident services

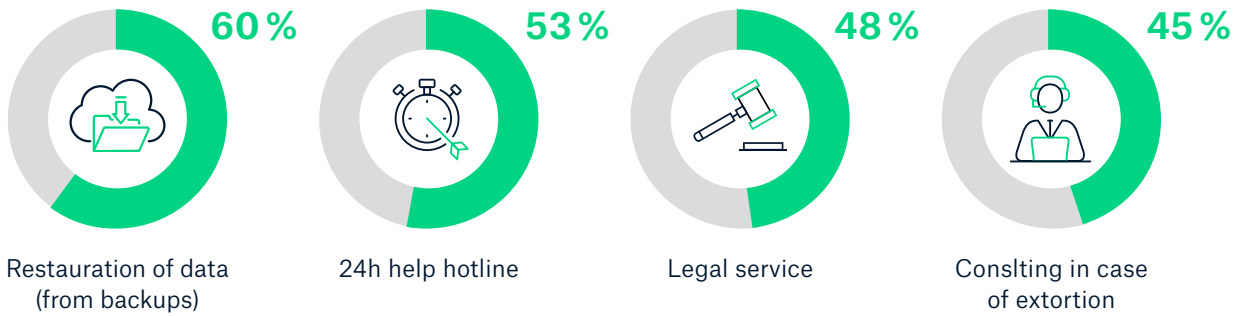
Which of these services should be covered by cyber insurance solutions when it comes to **avoiding** a cyber attack?



© Munich Re, 2022

Post-incident services

Which of these services should be covered by cyber insurance solutions when it comes to **providing help** in case of a cyber attack?

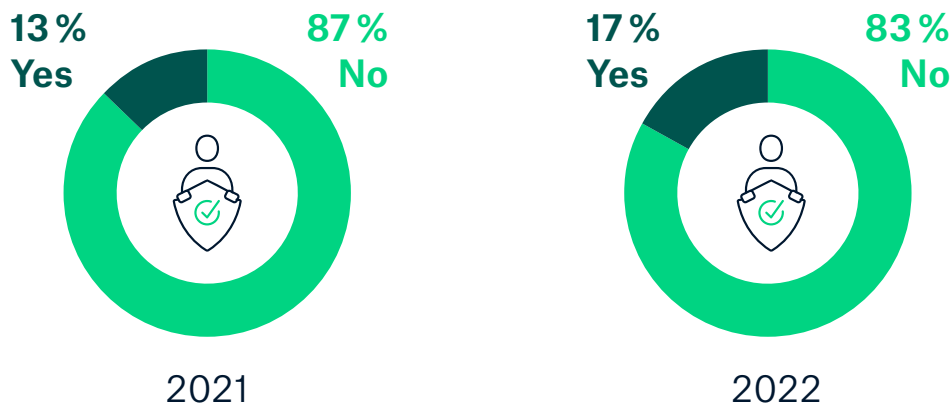


© Munich Re, 2022

In the private sector, it is also positive to see that the number of those who have already been offered private cyber insurance has increased significantly (from 13% to 17%).

Personal cyber insurance offering

Have you ever been offered cyber insurance for your private life?



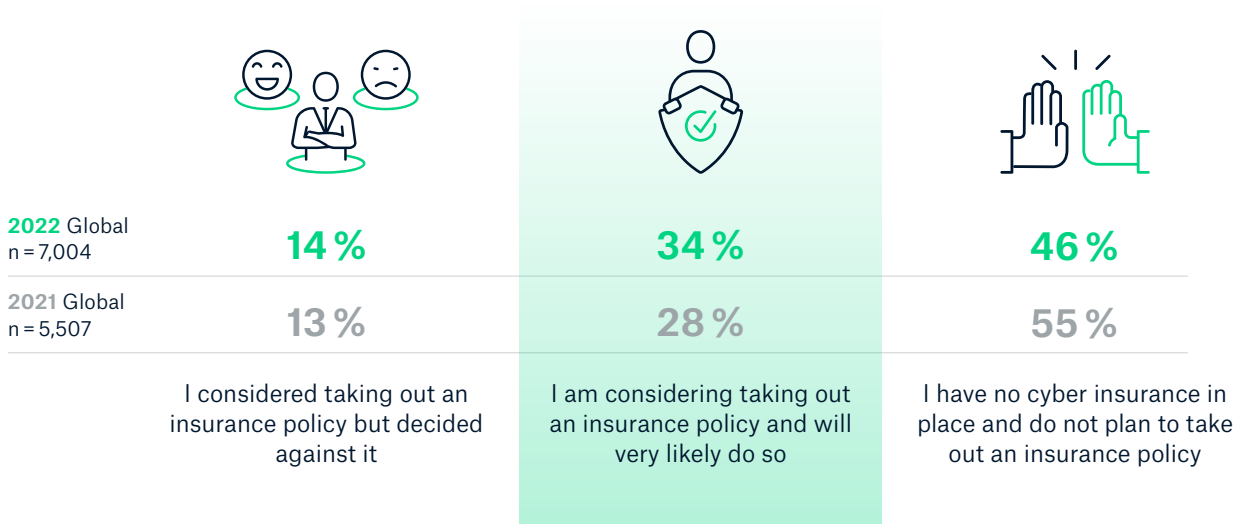
© Munich Re, 2022

In the private sector, it is also positive to see that the number of those who have already been offered private cyber insurance has increased significantly (from 13% to 17%).

And not only has the offer increased, but the number of those who have taken out explicit cyber insurance for themselves and their family (6%) or are planning to do so (34%) has also risen noticeably in each case.

Personal cyber insurance status

Would you take out a cyber insurance policy for yourself?



© Munich Re, 2022

However, it is also clear here that, despite high concern about becoming a victim of a cyber-attack, the understanding of how cyber insurance can contribute to one's own security is still far lower than it is in the business context. At 46%, almost half of the survey participants state that they have no ambition at all to take out personal cyber insurance for their private lives.

7. Boosting Cyber Resilience

Digitalisation and cyber-attacks are increasing relentlessly - among companies and private individuals. Supply and demand for cyber insurance have increased slightly, but most respondents are still not adequately protected or even prepared. In view of the market situation, the requirements on the part of insurers to provide access to products and solutions and to ensure sustainability for this line of business are also increasing. The potential for cyber insurers is high, but resilience and readiness are a prerequisite for tapping into this potential.

Amongst other things, it is also the duty of the insurance industry to explain the importance of resiliency measures on risk exposure to their clients and customers – and this would include discussing influencing factors such as premiums, prices, coverages, limits, terms and conditions, and access to insurance. This also requires insurance carriers to set standardised (minimum) requirements within a transparent risk assessment and underwriting approach.

When it comes to quantifying cyber risks, Munich Re has its own cyber underwriting tool that provides in-depth exposure and risk assessment, premium calculation, and probable maximum damage estimation. The parameters for these calculations were recently updated to reflect the risk dynamic and data monitored. Furthermore, the implementation of the updated underlying ISO 27002 standard is already underway.

Due to a lack of historical data and non-existent or inconsistent legal obligations related to reporting ransomware or cyber business interruption events, pricing cyber risks adequately is still a challenge. However, the insurance industry finds itself able to collect and analyse more and more information from covered losses. Insurers and Munich Re are in a uniquely privileged position to collect proprietary information from risk owners. This data can then be analysed for the purpose of minimising cyber threats, actual losses (related, e.g., to type and severity of breaches and business interruption), technology solutions and practices used by risk owners to minimise losses, or company demographics (e.g., industry, company size, geography, number and type of data stored, dependency from ICT).

Cyber insurance, together with other stakeholders, can leverage this data to reshape cyber risk assessment and better explain the modelling of cyber risks to its insured. Overall, better data analysis can identify causal factors of a particular claim and identify the best means of risk mitigation. Looking to the future, insurers should carefully evaluate (and re-evaluate) the types of incentives offered to provide appropriate cyber security. As a basic tenet, insureds should not be rewarded for having basic controls in place – this should be a mandate for risk eligibility. But the minimum acceptable thresholds should be continuously evolved to mirror the greatest threats to an insured at any given time. Finally, in this context, it is worth underlining that collecting data is just one half of the equation – the data must also be useful in terms of analysis and the insurance industry must have the capabilities to analyse and share it in a meaningful way. With this in mind, Munich Re has established a dedicated team to improve data analysis and risk quantification.

The ultimate goals must be to deter attacks (like ransomware) and disrupt cyber criminals' business models, as well as to help organisations prepare against breaches and respond to attacks more effectively. This is why Munich Re, amongst others, actively supported the US Ransomware Action Task Force implemented by the US Institute for Security and Technology, which has issued a comprehensive set of recommendations on the above-mentioned goals. In terms of further initiatives, Munich Re will continue to focus on more incentives for the sharing of information, more partnerships – both domestic (public/private/government) and global, and better regulation of cryptocurrency, to mention but a few.

Insurers continue to be at the forefront of promoting cyber hygiene, offering services and solutions to prevent and mitigate cyber-attacks, and implementing underwriting guidelines to support these efforts. However, it is well known that cyber-attacks and ransomware are used by sanctioned states to fund themselves. This is a government issue that only the government can address. Ill-advised, poorly conceived and implemented sanctions have caused and continue to fuel the ransomware problem. Regulators and policymakers have been too slow to develop any viable means of preparing or responding to cyber-crime. Munich Re supports national and international anti-ransomware actions and collaboration on disrupting ransomware operations.

Munich Re Cyber Experts and Client Managers are available if you would like to see insights from the country-specific evaluations or if you want to learn more about our cyber insurance solutions. [Better be safe than sorry.](#)

8. Methodology of the Survey

The survey was conducted on behalf of Munich Re by the global market research company, Statista, in December 2021 and analysed with Munich Re's internal experts in January and February 2022.



Respondents

- Global: More than **7,000** in total in **14** countries
- Representative results globally and for each country
- Results representative for commercial and private lines business through C-Level/ Employee split



Countries

- Australia
- Brazil
- Canada
- China
- France
- Germany
- India
- Italy
- Japan
- Spain
- South Africa
- Sweden
- UK
- USA



Company sizes

- 1 - 9 employees: **12 %**
- 10 - 249 employees: **34 %**
- 250 - 2499 employees: **26 %**
- > 2500 employees: **25 %**



Company's annual revenues

- > 1 million USD: **17 %**
- 1 million - 200 million USD: **28 %**
- 200 million - 1 billion USD: **12 %**
- 1 billion - 5 billion USD: **8 %**
- > 5 billion USD: **6 %**



Surveyed industries

- Consumer products & services: **17 %**
- Information technology: **14 %**
- Finance: **10 %**
- Transportation/ Communication/ Utilities: **10 %**
- Industry/ Manufacturing: **10 %**
- Education: **9 %**
- Healthcare & Pharma: **7 %**
- Public Authority/ Defence: **6 %**
- Other: **16 %**

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

© 2022

Münchener Rückversicherungs-Gesellschaft
Königinstrasse 107, 80802 München, Germany

Picture credits:

Cover image: Stanislaw Pytel/ Getty Images

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.