ALLIANZ COMMERCIAL

Cyber security trends 2023

The latest threats and risk mitigation best practice – before, during and after a hack

Contents

Introduction

Investments in cyber security are paying off but an evolving threat landscape will require much greater focus on early detection and response capabilities.

Improvements in cyber security and business continuity are helping to combat encryption-based ransomware attacks, yet the cyber threat landscape is continually evolving. 2023 has seen a worrying resurgence in ransomware and extortion claims, resulting in an uptick in costly incidents, demonstrating that although progress is being made, the threat posed by ransomware shows little sign of abating.

Reports note that the number of ransomware victims surged by as much as 143% globally during the first quarter of 2023 with January and February seeing the highest number of hack and leak cases in three years. Ransomware alone is projected to cost its victims approximately US$265bn annually by 2031.

Hackers are increasingly targeting IT and physical supply chains, launching mass cyber-attacks and finding new ways to extort money from companies, large and small. Most ransomware attacks now involve the theft of personal or sensitive commercial data for the purpose of extortion, adding further cost and complexity, as well as the increased potential for reputational damage and third-party liability. Allianz analysis of a number of large insurance industry cyber losses shows that the proportion of cases in which data is exfiltrated is increasing every year – from 40% of cases in 2019 to around 77% of cases in 2022, with 2023 on course to surpass last year's total.

Protecting an organization against intrusion remains a cat and mouse game, in which the cyber criminals have the advantage. Threat actors are now exploring ways to use artificial intelligence (AI) to automate and accelerate attacks, creating more effective AI-powered malware and phishing. Combined with the explosion in connected mobile devices and 5G-enabled Internet of Things, the avenues for cyber-attacks look only likely to increase in the coming years.

143%

increase in the number of ransomware victims globally during the first quarter of 2023

JANUARY AND FEBRUARY

saw the highest number of hack and leak cases in three years

US$265bn

is the approximate projected annual cost of ransomware to its victims by 2031

Preventing a cyber-attack is therefore becoming harder, and the stakes higher. As a result, early detection and response capabilities are becoming ever more important. An intrusion can quickly escalate, and once data is encrypted and / or stolen, the consequences and costs snowball – costs can be as much as, or even more than, 1,000 times higher than if an incident is not detected and contained early, Allianz analysis shows.

Ultimately, early detection and effective response capabilities will be key to mitigating the impact of cyber-attacks and ensuring a sustainable insurance market going forward.

Threat landscape: Resurgent ransomware targets data and supply chains

Ransomware remains the top cyber threat and the single largest cause of cyber insurance claims by some distance. Following a short hiatus in 2022, ransomware attack frequency has picked up again in 2023 as threat actors use data exfiltration and supply chain attacks to maximize their leverage.

In many ways, the last 12 months has been business as usual for ransomware gangs. They continue to evolve their tactics and business models in response to changes in cyber security and as they find new ways to extort money from businesses and public sector organizations.

According to research from cyber threat intelligence firm Black Kite[1], ransomware attacks surged in early 2023, with the number of victims in March nearly double that of last April and 1.6 times higher than the peak month in 2022. Akamai Technologies said the number of ransomware victims surged by 143% globally in the first quarter of 2023[2]. Meanwhile, January and February 2023 saw the highest number of ransomware hack and leak cases in the past three years, according to the NCC Group, which also noted that ransomware activity was up almost 50% year-on-year as of May 2023[3]. In future, ransomware alone is projected to cost its victims approximately US$265bn annually by 2031, Cybersecurity Ventures predicts[4].

A surge in data exfiltration attacks from the likes of LockBit and Clop in 2023 has seen the number of attacks reach new levels, while according to cryptocurrency firm Chainalysis, ransomware victims paid demands of US$449.1mn[5] in the first six months of this year, already close to last year's total of US$500mn. At the current rate, 2023 could end up as the second biggest year for ransomware revenue after 2021.

Key developments

- Ramsomware groups continue to adapt their tactics and business models in response to cyber security changes.
- Ransomware-as-a-Service (RaaS) remains a key driver for the ongoing frequency of attacks.
- Double and triple extortion attacks are not new, but they are now more prevalent, and potentially more impactful and costly for affected companies.
- Supply chain-enabled ransomware attacks have now become an established part of the ransomware playbook.
- Rise in mass ransomware attacks means insurers will need to better understand the interconnectivity and dependencies that exist between companies and within digital supply chains.

This year has witnessed several large mass ransomware attacks as threat actors used exploits in software and weaknesses in IT supply chains to target multiple companies. At the same time, ransomware gangs continue to fine tune their business models in order to carry out more attacks, faster. According to research from IBM X-Force[6], the average number of days taken to execute a ransomware attack has fallen from 60+ days in 2019 to less than four days in 2021.

In June, ransomware group Clop carried out a successful mass cyber-attack that is thought to have impacted thousands of companies, compromising the data of millions of individuals and businesses. Clop exploited a 'zero-day' vulnerability in MOVEit file transfer software to steal data from companies and public sector organizations, threatening to publish the data if they failed to pay a ransom demand.

The attack affected a number of large corporates, including energy giant Shell, British Airways, broadcaster the BBC, logistics firm DHL, insurer Genworth Financial, as well as the US Department of Health and Human Services and the US Department of Energy[7]. Genworth Financial alone reported that the personal information of nearly 2.5 million to 2.7 million of its customers was breached[8]. Clop is now the second-largest ransomware group by number of victims.

"As companies have enhanced network security and backup strategies, and as regulation dissuades companies from paying ransom demands, the chances of a successful encryption ransomware attack are becoming slimmer, and threat actors are changing strategies," explains **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial**. "The recent MOVEit supply chain attack is a good example of how gangs are increasingly resorting to mass attacks and data exfiltration."

RaaS groups responsible for majority of incidents

Ransomware-as-a-Service (RaaS) remains a key driver for the ongoing frequency of attacks. With access to RaaS kits and services, criminals lacking the skill to develop their own malware can launch ransomware attacks quickly and affordably. With prices starting from US$40 per month, RaaS kits enable cyber criminals to make millions from extortion demands with little financial investment.

"This is not a problem that is going away," says **Michael Daum, Global Head of Cyber Claims at Allianz Commercial**. "We often deal with the same attack groups. They change – they disappear, reorganize and then reappear under a different name – but the groups with the best tactics make the most money, and then they start re-selling their tools and expertise to others. They operate like successful businesses."

Ransomware attacks against large companies typically originate from a relatively small number of groups. For example, Allianz has handled several claims attributed to the likes of Black Basta, Clop and LockBit. According to the US Cybersecurity and Infrastructure Security Agency[9], LockBit was the most deployed ransomware variant across the world in 2022, with more than 1,700 attacks since 2020 in the US alone, and approximately US$91mn of ransoms paid.

"Cyber criminals' tactics continue to evolve," says Daum. "When we talk about ransomware, we are now really speaking about attackers applying various techniques in order to extort money. Where we used to see encryption, we now see attackers steal data or carry out Distributed Denial of Service (DDoS) attacks – with no encryption applied or in combination with encryption – in order to demand a ransom."

RaaS kits enable cyber criminals to make millions from extortion demands, with prices starting at

US$40 per month

LockBit was the most deployed ransomware variant across the world in 2022, with

1,700+

attacks since 2020 in the US

US$91mn

approximate cost of ransoms paid

Data exfiltration becomes the norm

Double and triple extortion – using a combination of encryption, data exfiltration and Distributed Denial of Service (DDoS) attacks to extort money – are not new, but they are now more prevalent, and potentially more impactful and costly for affected companies.

Allianz analysis of a number of larger insurance industry cyber losses (>€1mn) between 2019 and the end of the first half of 2023 shows that the proportion of cases in which data is exfiltrated increases from year to year – from 40% of cases in 2019 to around 77% of cases in 2022, with 2023 on course to surpass 2022's total.

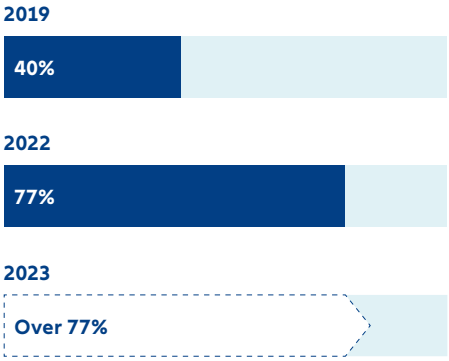
Once a threat actor has infiltrated a system, encrypting is much more difficult than stealing data, explains **Michael Daum, Global Head of Cyber Claims, Allianz Commercial**. "Attackers will 100% try to exfiltrate data before they try to encrypt. It's faster and easier compared to fully encrypting the victim's environment. In almost every extortion-focused intrusion, data will get exfiltrated."

Several factors are combining to make data exfiltration more attractive for threat actors. The scope and amount of personal information being collected is increasing, while privacy and data breach regulations are tightening globally. At the same time, the trend towards outsourcing and remote access leads to more interfaces for threat actors to exploit.

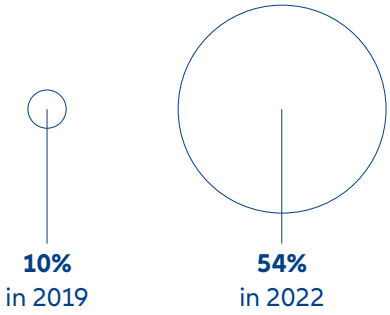
With potentially costly financial and reputational consequences, companies may feel under more pressure to pay ransoms where data has been stolen. The same Allianz analysis of a number of larger insurance industry cyber losses (>€1mn) between 2019 and the end of the first half of 2023 also shows that the proportion of companies paying a ransom has also increased from year to year – from as little as 10% in 2019 to 54% in 2022.

Meanwhile, companies are 2.5 times more likely to pay a ransom in cases where data has been exfiltrated, on top of the encryption, the analysis also shows (the share of companies paying a ransom when data was exfiltrated is 56% compared with the share of companies paying ransom without data exfiltration which is just 21%). However, recent mass hacks have also seen many companies refuse to pay.

The proportion of cases in which data is exfiltrated increases year on year



The proportion of companies paying a ransom has increased from year to year



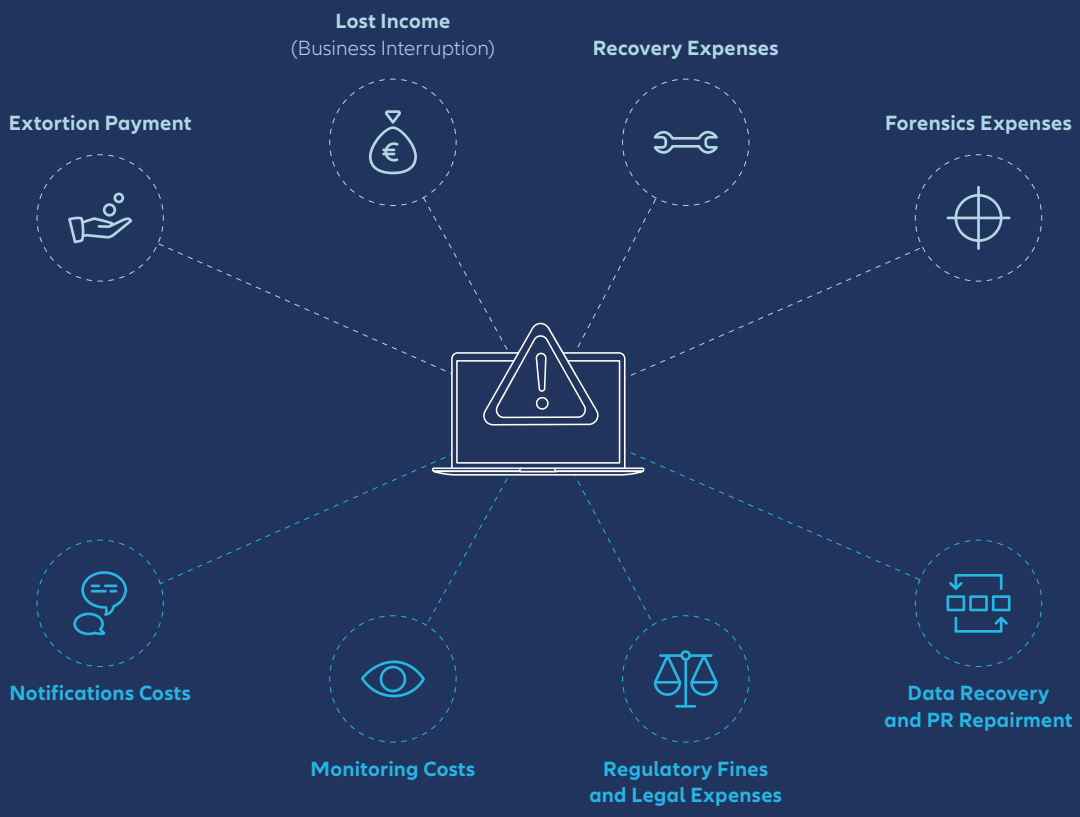
Companies are

2.5x

more likely to pay a ransom in cases where data has been exfiltrated, on top of the encryption

Ransomware costs – double extortion changes the rules and multiplies the cost

Potential costs from a 'conventional' ransomware attack
(which encrypts the attacked company's data without leaking it)



Potential **additional** costs from a ransomware attack which becomes **a data breach event**
(stealing and then publishing the data)

Costs description:

Single Extortion (encryption)

Extortion Payment: demanded by criminals

Lost Income (Business Interruption): The longer the period of time in which system accessibility is limited, the greater the loss.

Recovery Expenses: the cost of restoring data and ensuring full systems recovery.

Forensics Expenses: expenses incurred to investigate the source of the security vulnerability.

Double Extortion (encryption and exfiltration)

Notifications Costs: notifying customers, regulators and other required authorities of a data breach.

Monitoring Costs: monitoring services for identity theft/ fraud that has to be supplied to individuals whose data is stolen.

Regulatory Fines and Legal Expenses: due to third parties' claims whose private data is stolen.

Data Recovery and PR Repairment: Costs of a consultant, crisis management firm or law firm to limit effects of negative publicity.

Sources: Bitsight and Kovrr. Graphic: Allianz Commercial.

"However, paying a ransom for exfiltrated data does not necessarily resolve the issue," says Daum. "Especially in the US, the company may still face third party litigation for the breach of data. Once a company has paid a ransom for data exfiltration, there is no guarantee it will not be used for fraud or sold on the Dark Net anyway."

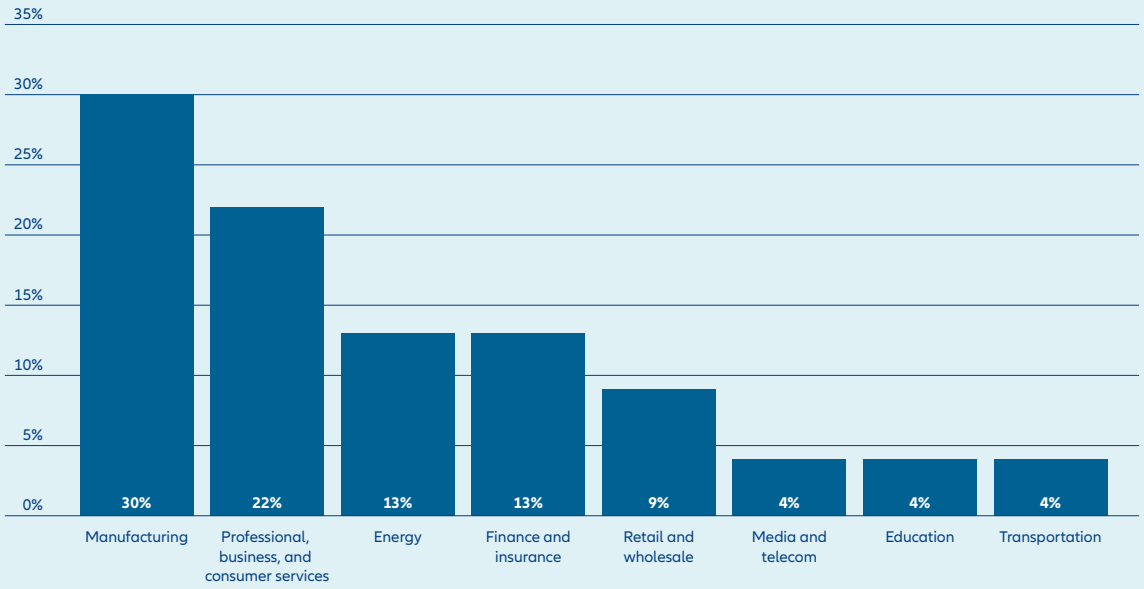
Indeed, there are very few cases where a company may believe that there is no other solution than paying the ransom to be able to re-access their systems or data. Any impacted company should always inform and cooperate with the police or national investigation authorities.

In the past, companies holding personal data and credit card information were targets of data breaches, but increasingly industrial and manufacturing companies that share ecosystems are falling victim to data exfiltration attacks. Manufacturing was the most targeted sector for ransomware cyber-attacks and the most extorted industry in 2022, according to IBM Security's 2023 X-Force Threat Intelligence Index[10].

"With data exfiltration, you can attack a standard manufacturing company with many different clients. If you can get data on these clients as well, the criminals can demand money from them also, and that is what we have seen in some claims now," says **Jens Krickhahn, a Regional Practice Leader, Cyber Insurance, at Allianz Commercial.**

Top industries targeted

The percentage of extortion cases by industry observed in incident response engagements in 2022.



Numbers do not add up to 100% due to rounding.

Source: IBM Security's 2023 X-Force Threat Intelligence Index

Threat actors target weak links in supply chains

Supply chain-enabled ransomware attacks are not new, but they have now become an established part of the ransomware playbook. Increasingly, threat actors are targeting companies in the IT supply chain, as well as companies that hold sensitive data in physical supply chains, in order to demand extortion payments from multiple companies.

Supply chain attacks first hit the headlines in 2019, following an intrusion at the system management company Solar Winds, which marked the start of one of the largest software supply chain attacks in history. In 2021, a similar attack involving IT management company Kaseya exploited a zero-day vulnerability in the company's remote management software to carry out ransomware attacks that are thought to have impacted some 1,500 businesses[11] and resulted in a US$70mn ransom demand.

In June 2023 a North Korea hacking group[12] penetrated software-as-a-service provider JumpCloud in order to target cryptocurrency companies, according to media reports. Blockchain analytics firm Chainalysis said last year that North Korean-linked groups stole an estimated $1.7bn worth of digital cash across multiple hacks.

"By attacking an IT supplier with a lot of dependent clients, the extortion power is even larger. You do not hit just one company, but many companies at one time," says **Michael Daum, Global Head of Cyber Claims at Allianz Commercial**.

Supply chain cyber-attacks were typically associated with sophisticated nation state hacker groups, but increasingly they are being used by RaaS groups to launch mass ransomware attacks. Much like the recent MOVEit extortion, ransomware gangs are now alive to the opportunities to exploit the interconnectivity of digital and physical supply chains and will target organizations with weak cyber security in order to infiltrate other companies elsewhere in the supply chain, circumventing more robust cyber security.

"You would expect that IT providers have sophisticated cyber security, but that is not always the case, and we have seen a growing number of incidents where there have been deficiencies. The large attacker groups are sophisticated and very savvy and are attracted to targets that hold interesting data or that give access to other companies, which enable them to demand extortion payments or launch future attacks," says Daum.

Mass attacks raise accumulation concerns

2023 has seen several mass ransomware extortion attacks, where RaaS groups exploit vulnerabilities in software and the interconnectivity of digital supply chains to exfiltrate data and demand ransoms from hundreds, if not thousands of companies.

In addition to the recent MOVEit attack, in which the Clop ransomware group used a zero-day vulnerability in widely used file transfer software, RaaS groups have launched other such attacks in 2023. Earlier this year Clop also used a zero-day flaw in the GoAnywhere file transfer software to steal data from over 130 companies[13]. In another separate attack, threat actors exploited a known vulnerability in unpatched VMware ESXi servers, compromising 3,800 servers worldwide[14].

Mass ransomware attacks are a potential "gamechanger" for the insurance industry, as they trigger multiple claims simultaneously, according to **Jens Krickhahn, a Regional Practice Leader, Cyber Insurance, at Allianz Commercial.**

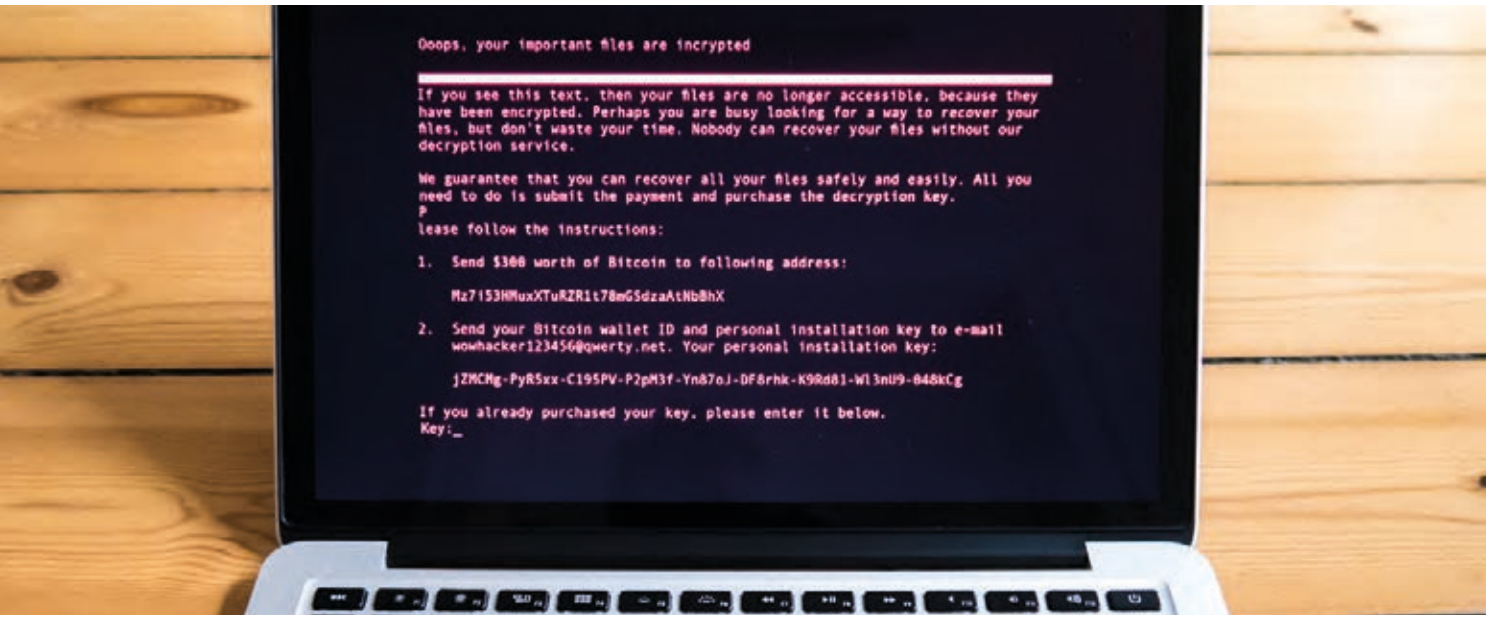
"This year we had our first event case, with 40 policies triggered at the same time. From a claims management side that creates a completely new scenario, as you are in contact with multiple insureds at the same time, on the same topic, with different service providers and vendors. The once theoretical risk of an accumulation exposure is now reality," says Krickhahn.

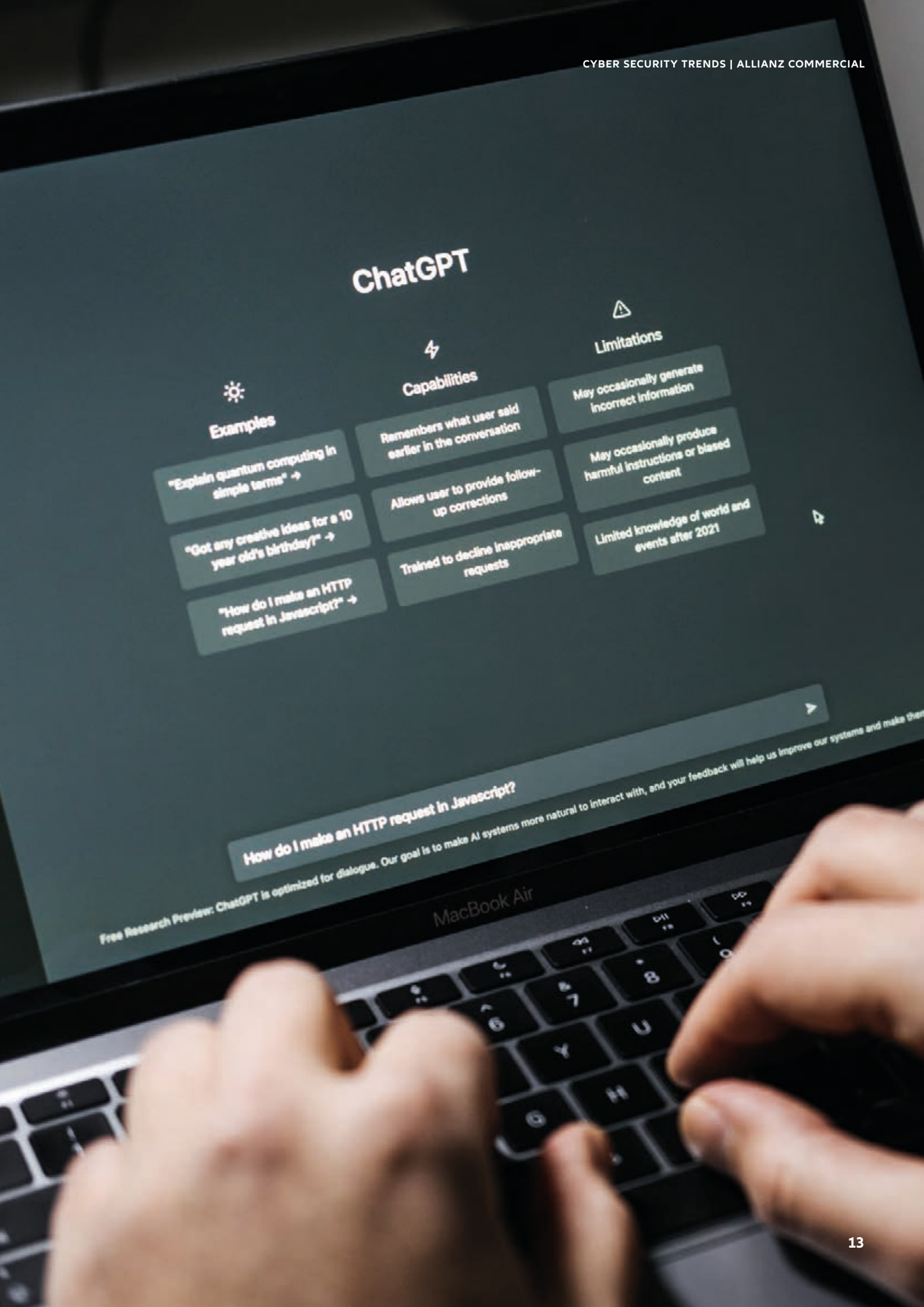
"A similar successful attack against a larger IT vendor or data center provider could have a global effect and a huge impact on the insurance industry.

"Having that knowledge today, many insurers will no doubt look at their exposure to different industries and sectors more carefully, and will need to consider capacity management, as well as coverage. Knowing that many companies are reliant on a single vendor, an insurer may need to consider solutions – such as aggregation clauses – just to manage the exposure."

Insurers will want to better understand the interconnectivity and dependencies that exist between companies and within digital supply chains, adds **Tresa Stephens, a Regional Head of Cyber at Allianz Commercial.**

"Modeling accumulation of cyber risk is challenging because the interdependencies between insureds and their vendors is so difficult to qualify and track. It's almost like we are underwriting many risks, not just the insured. We are looking at all their vendors and suppliers and need to understand the interdependencies in our portfolio."




ChatGPT
Examples
"Explain quantum computing in simple terms" →
"Got any creative ideas for a 10 year old's birthday?" →
"How do I make an HTTP request in Javascript?" →
Capabilities
Remembers what user said earlier in the conversation
Allows user to provide follow-up corrections
Trained to decline inappropriate requests
Limitations
May occasionally generate incorrect information
May occasionally produce harmful instructions or biased content
Limited knowledge of world and events after 2021
How do I make an HTTP request in Javascript?
Free Research Preview: ChatGPT is optimized for dialogue. Our goal is to make AI systems more natural to interact with, and your feedback will help us improve our systems and make them
MacBook Air

Future threats: AI, IoT and skills shortage to fuel future cyber-attacks

Artificial intelligence (AI) is widely expected to power future ransomware attacks, with automated attack processes, more convincing phishing, and faster malware development. However, it could also enhance cyber security, with more effective and faster detection and threat intelligence.

Threat actors are already using AI-powered language models like ChatGPT to write code. Generative AI can help less technically proficient threat actors write their own code or create new strains and variations of existing ransomware, potentially increasing the number of attacks they can execute.

"We can expect an increased utilization of AI by malicious actors in the future, necessitating even more stronger cyber security measures," says **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial**. "AI can be used to carry out more automated attacks, as well as develop new techniques to steal or poison data. When you think about the potential to combine AI with the proliferation of the Internet of Things (IoT) and the speed of 5G, for example, we may have a serious issue on the horizon."

Voice simulation software has been a recent addition to the cyber criminal's arsenal. In 2019 the CEO of a British energy provider transferred €220,000 to a scammer after they received a call from what sounded like the head of the unit's parent company, asking them to wire money to a supplier. The voice was generated using AI[15].

In August 2023, researchers at the Google-owned cybersecurity company Mandiant documented the first known instances of deepfake video technology designed and sold for phishing scams. The going rate was as little as US$20 per minute, US$250 for a full video or US$200 for a training session, although the researchers were unable to confirm that the services they identified on hacker forums were legitimate or whether a deepfake had been used in any scam.

Key developments

- AI-powered language models and voice simulation software recent additions to the cyber criminal's arsenal.
- Allianz Commercial has seen a growing number of incidents caused by poor cyber security around mobile devices.
- Technical skills crisis in cyber security is also increasing the cost of responding to an incident.

Companies will need to invest in AI-powered cyber security to counter the growing threat posed by threat actors, **Michael Daum, Global Head of Cyber Claims at Allianz Commercial,** adds.

"AI will help threat actors, but it is also a powerful tool for detection. We might see more AI-enabled cyber incidents in the future, but investment in detection backed by AI should catch more incidents early. If we can keep pace with developments in AI, there is always the chance it might not change the picture too much from today, neither in favor of the company nor the attacker."

Mobile devices expose personal and corporate data

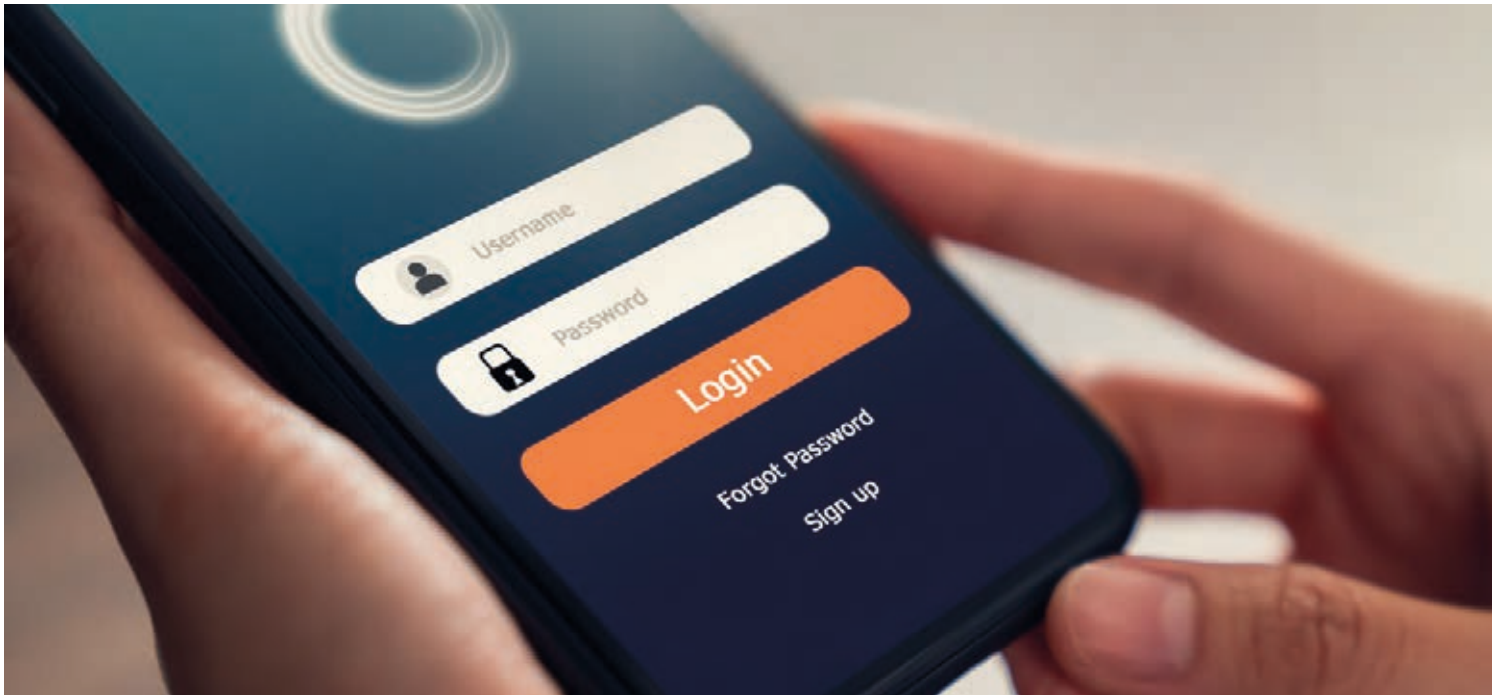
Lax security and the mixing of personal and corporate data on mobile devices is making for an attractive target for cyber criminals.

Allianz Commercial has seen a growing number of incidents caused by poor cyber security around mobile devices. During the pandemic many organizations enabled new ways of accessing their corporate network via private devices, without the need for multi-factor authentication (MFA). This also resulted in a number of successful cyber-attacks and large claims.

"Cyber criminals are now targeting mobile devices with specific malware in order to gain remote access, steal login credentials, or to deploy ransomware," says **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial**. "Increasingly we have corporate and personal information on the same device, and threat actors now see this as a potential vulnerability. Personal devices, in particular, tend to have less stringent security measures. Utilizing public wi-fi on these devices can increase their vulnerability, including exposure to phishing attacks via social media."

The roll out of 5G technology is also an area of potential concern. 5G will power more connected devices, including more sophisticated applications, such as driverless or assisted vehicles and smart cities. However, IoT devices do not have a good track record when it comes to cyber security, Baviskar continues.

"Many IoT devices are not inherently secure, while the sheer number of these devices globally and the addition of AI could result in a very serious cyber threat. Many of these devices are easily discoverable and will not have MFA mechanisms. Even today we see devices with default passwords that are available on the internet," says Baviskar.



Cyber security skills shortage affects cost and frequency

A growing shortage of cyber security professionals will increasingly complicate cyber security efforts, potentially increasing the chances of successful attacks in the future.

The current global cyber security workforce gap stands at 3.4 million people, according to the ISC2[16], a non-profit member organization for cyber security professionals, with demand for cyber professionals growing twice as fast as supply. Some 70% of organizations say they do not have enough cyber security staff to be effective. Gartner predicts that a lack of talent or human failure will be responsible for over half of significant cyber incidents by 2025[17].

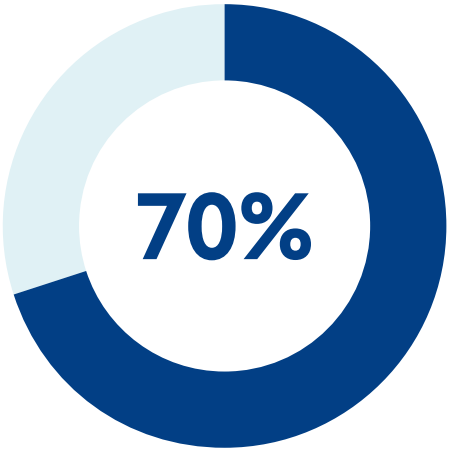
"There is a crisis in technical skills for cyber security," says **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial**. "Because technology is moving so fast, there are not enough experienced people to keep pace with the threats. It's very hard to get good cyber security engineers, which means companies are more exposed to cyber events. Without skilled cyber security people, it is harder to predict and prevent incidents, which could mean more losses in the future."

The shortage of cyber security experts also impacts the cost of responding to a cyber incident. According to the IBM Cost of a Data Breach Report 2023, organizations with a high level of security skills shortage had a US$5.36mn average data breach cost[18], around 20% higher than the average cost.

"IT specialists are a scarce resource, and IT security experts are even scarcer," says **Michael Daum, Global Head of Cyber Claims, Allianz Commercial:** "The volume of attacks and incidents is increasing at a higher rate than organizations can hire and train IT and cyber security professionals. And when there is more supply than demand, it leads to higher than inflation increases in fees for incident response and forensics."

The current global cyber security workforce gap stands at

3.4mn people



of organizations say they do not have enough cyber security staff to be effective

Claims: Stabilization trend threatened by mass attacks and data exfiltration

Cyber claims frequency picked up again during the first half of 2023, although improved cyber security over the past two years has helped control first party losses and improve the overall quality of risk.

Following a significant spike in ransomware losses in 2020 and 2021, the frequency of cyber insurance claims stabilized last year, reflecting improved cyber security and risk management actions among insured companies – such as the use of multifactor authentication or more effective backup strategies which made encryption-based ransomware less effective and reduced the business interruption impact. At the same time, law enforcement agencies targeting ransomware gangs and the Ukraine Russia conflict are thought to have curtailed the activities of threat actors.

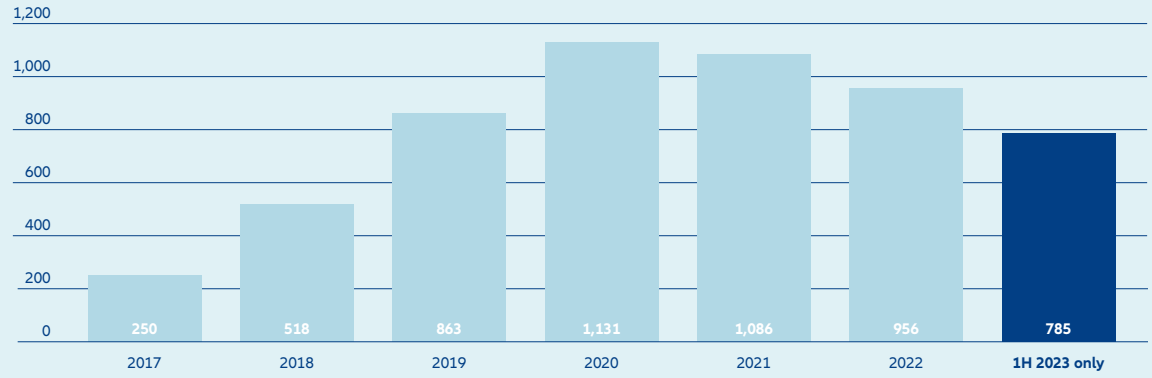
"Many companies addressed vulnerabilities and we have seen a notable improvement in governance around mergers and acquisitions (M&A), for example, which historically generated a number of large claims where due diligence failed to pick up issues with IT security or data privacy. Now we see a lot more consideration at a high level given to IT assets and cyber security during the M&A process," says **Tresa Stephens, a Regional Head of Cyber at Allianz Commercial**.

However, ransomware groups have changed tactics, with an increase in data exfiltration, and mass cyber-attacks that have exploited weaknesses in IT supply chains. The MOVEit mass cyber-attack, which affected over a thousand companies earlier this year, for example, contributed to the increase in the frequency of claims in 2023, affecting multiple policyholders simultaneously.

Key developments

- Ransomware and extortion-based attacks remain the largest source of cyber insurance claims by volume and frequency.
- In addition to extortion claims, there has also been an uptick in the number of data privacy claims in the US, related to biometric information.
- Allianz analysis of large cyber losses shows that the number of cases in which data is exfiltrated has significantly increased, as has the number of incidents becoming public.
- Allianz Commercial claims analysis shows that breaches that are not detected and contained early can be 1,000 times more expensive.

Number of cyber-related claims per year



Totals include all cyber-related claims per year. Numbers may change in future due to updated reporting.

Source: Allianz Commercial

"This year we have seen another uptick in claims frequency, following the stabilization of claims frequency last year. The attackers are now back, and focused again on Western economies, with more powerful tools, enhanced processes and attack mechanisms," says **Michael Daum, Global Head of Cyber Claims at Allianz Commercial**.

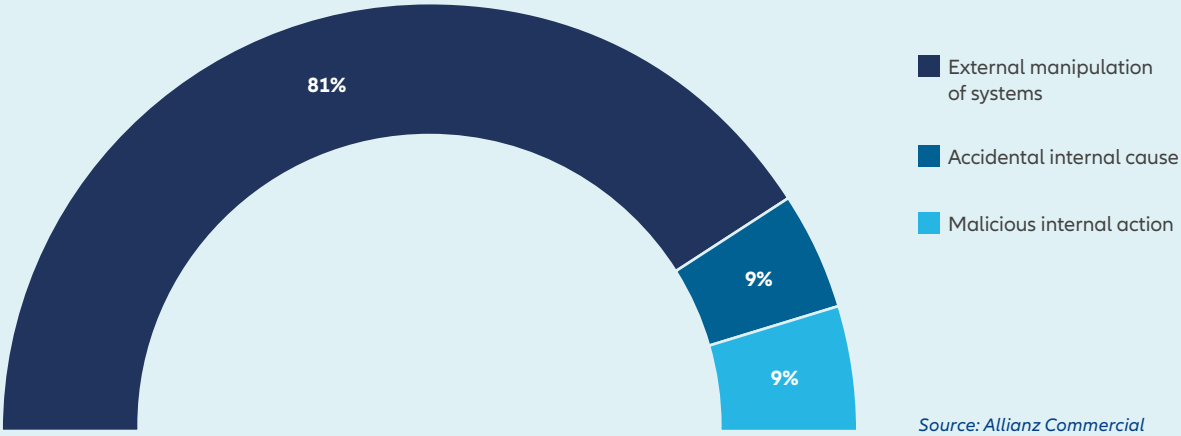
Ransomware and extortion-based attacks remain the largest source of cyber insurance claims by volume and frequency, accounting for more than 80% of claims from standalone cyber policies alone.

"MOVEit is a zero-day exploit in a data transfer software product that has hit thousands of companies and impacted millions of individuals. In the US we have seen claims, mostly from data exfiltration extortion," says **Marisa Anthony, Senior Complex Claims Handler, Cyber, Allianz Commercial**. "Even when MOVEit calms down, we fully expect it will be replaced by another attack. Frequency is to be expected in cyber, which is why early detection and response is key to controlling severity. As insurers we need to better understand the interconnectivity and dependencies that exist between companies and within digital supply chains."

> The attackers are now back, and focused again on Western economies, with more powerful tools, enhanced processes and attack mechanisms

Cause of loss by value of cyber claims

Based on the analysis of 3,366 claims worth €612mn (including the share of other insurers) between August 2019 and August 2023



Source: Allianz Commercial

Privacy and liability risks on watch

In addition to extortion claims, there has also been an uptick in the number of data privacy claims in the US, related to biometric information, such as voice or fingerprint data, as organizations increasingly capture this to improve online security. At the same time many track personal information such as location, health or behavior, as part of their product and service offering, or to aid sales and marketing.

The US does not have federal law covering data privacy, but a number of states have implemented strict laws, such as the California Privacy Rights Act and the Illinois Biometric Information Privacy Act (BIPA). Meanwhile, the number of data privacy and data breach class action lawsuits continues to rise as plaintiffs see this as a potentially lucrative and expanding area of litigation.

"We have seen some stabilization of first party cyber claims from prior underwriting years, directly as a result of improved risk quality and the efforts by insureds to shore up cyber security. But we have also seen a lot more activity on the regulatory and third-party liability side in the US. Companies are using biometric data more and more. At the same time, consumers are growing increasingly aware of their privacy rights and regulation continues to evolve in this area," says **Tresa Stephens, a Regional Head of Cyber at Allianz Commercial**.

Privacy laws, court judgements and awards are still a work in progress, making it difficult for companies and insurers to assess data privacy liability exposures, which are less predictable than more established casualty lines.

"We see growing traction in litigation, such as biometric claims, geo-tracking, voice and fingerprint and online tracking allegations. For the most part, these claims are all grounded in privacy issues, and the failure to inform people how their biometric data is being collected and used. While such claims are not new, they have been ramping up, and we see new favorable laws and judgements that make it easier and more profitable for the plaintiff's bar to bring such claims," says **Marisa Anthony, Senior Complex Claims Handler, Cyber, Allianz Commercial**. "Defending these actions is much more expensive than a typical general liability claim. The hourly rate for breach and defense counsels can be very alarming, particularly given recent inflation."

Data exfiltration and inflation drive up claims costs

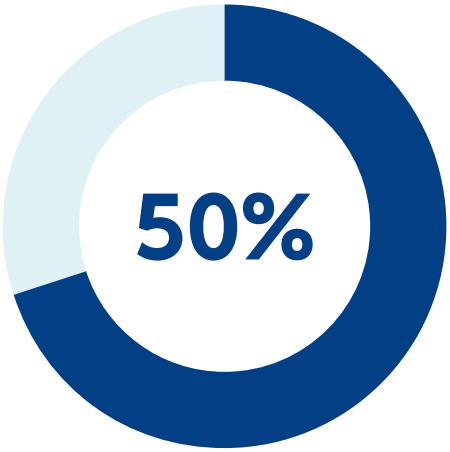
More sophisticated attacks and inflation are increasing the cost of large cyber losses. The size and complexity of an organization and its IT infrastructure is a key factor contributing to the cost of large cyber claims. Once a cyber-attack progresses past a certain point, the combination of first party restoration costs, business interruption and third-party liability easily result in a large loss.

"Managing cyber security throughout a large organization is very challenging, with different business units, suppliers and locations around the world as well as mergers and acquisitions. You might be 99% cyber safe, but if there is one open door, it's likely that attackers will find it. That is a scenario we have seen quite frequently, and once a large organization is hit, it often results in a large loss," says **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**

Business interruption remains the key loss driver for ransomware attacks, as it does for many forms of cyber-attack – Allianz analysis shows that it accounts for 50% of all cyber-related losses by value.

Allianz analysis of a number of larger insurance industry cyber losses (>€1mn) between 2019 and the end of the first half of 2023 shows that the proportion of cases in which data is exfiltrated increased from 40% in 2019 to 77% in 2022, with 2023 on course to surpass this. Along with this increase in data exfiltration, first party recovery and response expenses are increasing, while the cost of notification and third-party liability can also be significant. The average cost of a data breach in 2023 was US$4.45mn, a 15% increase over three years, according to the IBM Cost of a Data Breach 2023 report[19].

Business interruption accounts for



of all cyber-related losses by value

Data exfiltration can significantly add to the cost of a cyber claim, according to **Jens Krickhahn, a Regional Practice Leader, Cyber Insurance, at Allianz Commercial:** "Data exfiltration can take the potential claim value to a completely new dimension. A pure first party claim could be settled within two years, but with data exfiltration, not only do these claims take longer to settle, but the impact of a data exfiltration claim can also climb dramatically with litigation and regulatory investigations, while legal and IT forensics costs can be extremely expensive. If data has been stolen, you must know exactly what data has been exfiltrated, and you may have to notify your customers, who could claim compensation or threaten litigation," says Krickhahn.

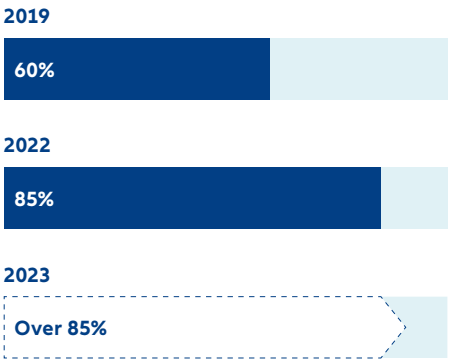
Allianz analysis of claims notifications shows that breaches that were not detected and contained early, and therefore ultimately involve data exfiltration, can be as much as, or even more than, 1,000 times more expensive than those that were.

Exfiltration incidents carry a higher reputational risk and are a bigger drain on the resources of the company and leadership, making effective data breach response critical, explains Daum.

"In the past, the ratio of claims that went public was much lower. With data exfiltration, hackers threaten to publish stolen data on dark forums, so the stress level is much higher. With the increased level of public scrutiny and pressure, preparation is more important than ever before. It's also why you need legal and PR experts working on this. We are seeing more claims where this support is needed, because cyber-attacks are playing out more in the public sphere," says Daum.

Indeed, Allianz analysis of a number of larger insurance industry cyber losses (>€1mn) between 2019 and the end of the first half of 2023 shows that the proportion of cases becoming public increases from year to year. In 2019 this totaled 60%, rising to 85% in 2022, with 2023's total on course to surpass this.

The proportion of cases becoming public increases from year to year



Mitigation: Early detection is key to combating emerging cyber threat

The vast majority of cyber-attacks are contained quickly and, if insured, often fall within policy deductible levels, or are not even notified. According to Allianz analysis, just 2% of claims drive the overall loss amount, and in almost all cases these would have benefited from early detection. Meanwhile, good data management is essential to mitigating the impact of data exfiltration attacks, as are a growing number of specialist services.

Prevention drives frequency, while detection determines severity, according to **Michael Daum, Global Head of Cyber Claims at Allianz Commercial**. "Some 90% of incidents are contained early, and most cases stay within policy retention levels. However, if the attack is not stopped in the early stages, we rarely see them being caught during the next stages. Once the attacker has exfiltrated and encrypted it is too late and becomes very expensive," Daum explains.

The key to avoiding damaging cyber-attacks and mitigating losses is to detect an attack in its early stages, according to Daum. "With growing reliance on outsourcing and data flows between companies, and with the potential use of artificial intelligence by threat actors, protecting the perimeter of an organization will no longer suffice.

"Companies cannot prevent. They can only reduce the number of attacks that surpass the first line of defense. There needs to be detection and response because it's no longer possible to prevent every attack, no matter how much you invest in IT security. Companies need to catch these attacks before the next stage and prevent the most severe incidents that might bring their business to a halt and damage their reputation," says Daum.

Allianz analysis of claims notifications shows that breaches that were not detected and contained early can be as much as, or even more than, 1,000 times more expensive than those that were.

Key developments

- The key to avoiding damaging cyber-attacks and mitigating losses is to detect an attack in its early stages.
- Companies should direct additional cyber security spend on detection and response. Only one third of companies discover a breach through their own security teams.
- Companies that are routinely and properly managing their data, and making sure it is stored appropriately, and deleted when it is no longer required, will reduce their risks.
- Smaller companies need to develop a clear understanding of their potential risks and allocate ample resources in terms of personnel, IT infrastructure, and budget to implement tailored security measures.
- Midcorps must identify their crucial IT assets, then collaborate with cyber security service partners to deploy detection and monitoring tools at the network perimeter and endpoints.

"An attack that is detected early and contained may cost €20,000. But if the intrusion is not detected and escalates, the resulting business interruption and breach costs could easily reach €20mn *(see example)*. Multifactor authentication has been one of the most effective measures over the past few years, but looking forward, detection tools (e.g. security operations center (SOC), security information and event management (SIEM), extended detection and response (XDR), intrusion detection (IDS) and intrusion prevention (IPS) systems) will be the next logical step for most companies to invest in," says Daum.

Human oversight and triage is also required to manage the flood of alerts, typically conducted in a SOC.

Time is key, when it comes to mitigating the impact of a ransomware incident, as business interruption and recovery costs quickly rack up once hackers have encrypted or stolen data, explains **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial**.

"You cannot protect what you cannot see. If you have an undetected loophole in your network, it's a potential Achilles heel. And if you do not have effective early detection, it can lead to longer unplanned downtime, increased costs, and have a greater impact on customers, revenue and profitability. Early detection can also be more cost effective than after-the-event intervention," adds Baviskar.

The lion's share of IT security budgets is currently spent on prevention, with around 35% of the budget directed to detection and response. However, the effectiveness of detection and response capabilities drives the size of loss.

Early detection technology is readily available and effective, according to Baviskar. "Detection systems are constantly improving and can save lots of pain, decreasing detection and response times. This is something we look for in our cyber risk assessments and underwriting."

€20,000 or €20mn? How early detection and response can make all the difference

Profile: A manufacturing company with 2,000 employees.

Incident outcome 1: One or more of the employees' computers is successfully attacked. The attack is detected and contained early (for example, before the attacker has been able to gain admin access rights).

Costs: Overall costs for forensics and restoration total approximately €20,000.

Incident outcome 2: In the same situation, the attacker is not detected and contained early and is able to successfully gain a foothold in the company's IT system, achieving the ultimate attacker goal (i.e., domain admin rights). The attacker is able to fully encrypt and extort the company.

Costs: Overall loss for business interruption (two weeks), ransom, full restoration, third party claims of personal data lost, total approximately €20mn (1,000 times more).

Allianz analysis of claims notifications shows that breaches that were not detected and contained early can be as much as, or even more than

1,000x more expensive

than those that were

"You can never be 100% safe. The cyber threat is increasing with an expanding attack surface, more sophisticated attacks, data exfiltration and mass ransomware attacks. Add in the proliferation of the Internet of Things and artificial intelligence to the mix, and increasing levels of regulation, rising breach costs and growing third party liability, and the case for investment in early detection and response capabilities grows ever stronger," says Baviskar.

Companies should direct additional cyber security spend on detection and response, rather then add more layers to prevention, advises Krickhahn: "We would not recommend that companies reduce budgets on prevention, rather they should just give IT security a budget to build up detection to the same level, if not more. It should be an automatic end-to end mechanism that starts with prevention, then follows through with early detection and response."

Only one-third of companies discover a data breach through their own security teams, highlighting a need for better threat detection, according to IBM[20]. Yet when attackers disclose a breach, it costs organizations an average of nearly $1mn more compared to internal detection.

"Many companies tend to be reactive to cyber-attacks, rather than proactive. They should invest in early detection as part of a more proactive approach. The investment in detection compared to the potential loss is quite small, but once you invest in detection you are better prepared to protect yourself and your critical systems," says Baviskar.

Early detection and response will also help deter future cyber-attacks, according to **Marisa Anthony, Senior Complex Claims Handler, Cyber, Allianz Commercial**: "Good detection and response will significantly frustrate threat actors and will make companies a less attractive target. Repeated efforts to find and detect the threat actor and shut them down immediately causes the threat actor to start again. Threat actors look for the easiest target most of the time."

Preparing for the worst

With increasing levels of data privacy regulation worldwide, good data management is also essential to mitigating the impact of data exfiltration attacks.

"Companies that are routinely and properly managing their data, and making sure it is stored appropriately, and deleted when it is no longer required, will reduce the amount of data that is at risk. We recently handled a claim where a hard drive had not been properly managed, and attackers exploited information that was over 10 years old. Had the company purged its data this costly claim would not have happened," says **Marisa Anthony, Senior Complex Claims Handler, Cyber, Allianz Commercial**.

The costs of legal and specialist IT and breach response services are also on the rise, with increased rates and the challenge of having to deal with more complex attacks. For example, with data exfiltration attacks it typically takes longer for vendors to figure out exactly what data has been stolen, which can be a very expensive process.

"The cost of external experts is rising, which makes the cost of a claim more expensive. In the US, for example, a lawyer might have charged €1,000 per hour a few years back, and today they would charge €1,500 for a similar case," explains **Jens Krickhahn, a Regional Practice Leader, Cyber Insurance, at Allianz Commercial.** "And as the complexity of claims increases, external experts spend more time resolving issues, so we see not only higher rates, but more people working on these more complex claims for longer."

With specialist data breach services in high demand, and the rise in data exfiltration attacks, organizations need to secure the services of vendors in advance. One recent supply chain attack claim for a European manufacturer in the US resulted in total extortion demands in the double-digit millions. And in that case, the insured was not sure which data had been compromised, requiring very expensive e-discovery costs.

"One of the learnings is that we strongly recommend clients prepare for these attacks with crisis plans, exercises and by appointing and contracting specialist vendors. This is very important. You do not want to be in the situation where you are attacked and must find providers and negotiate at short notice," says Krickhahn.

"If you have not put in place agreed rates, in advance of an attack, for the services and rates of these specialist vendors, you will likely face extremely high rates. But if you prepare and are ready for such attacks, and utilize the panel of expert vendors included in your policy, and their rates, you will be in a better position, and will likely reduce the impact and cost of the claim for your company," adds Anthony.

Vendor services that come with most cyber insurance policies can help manage data exfiltration attacks and mitigate the financial and regulatory impact. For example, breach coaches, which are popular in the US, can help mitigate the costs of a data breach, with more informed decisions around when to notify and who will need to be notified. In the heat of a ransomware event with data exfiltration, breach coaches can help with specialist legal advice that can avoid unnecessary expenses and avoid non-compliance with privacy laws.

> Companies that are routinely and properly managing their data, making sure it is stored appropriately and deleted when it is no longer required, will reduce the amount of data at risk

Pre-event, companies should familiarize themselves with their cyber insurance coverage and the services that may come with it, advises Anthony. "It seems fundamental, but insureds can learn a lot from studying their policy. They can take advantage of the support provided by the policy, review vendor information and make sure vendor key contacts are integrated into the response plan or contact vendors in advance and conduct tabletop exercises."

Policyholders should also take advantage of claims workshops to ensure their insurance coverage responds as needed, suggests Daum. "We offer claims scenario workshops, where the client can bring specific examples from its business, and we map it against their policy coverage and wordings. I would recommend that when you identify your top cyber risk scenarios you discuss them with your broker and insurer to make sure in principle whether they are covered or not."

Anthony advises insureds to document a cyber incident as it happens, recording costs and losses: "What stands out for me, is the need for the insured to think mathematically about the claim as the incident unfolds, and how they will need to substantiate the claim. For example, they will need proof of loss, and they will need to communicate timely detailed information on the event transparently.

"When they think of cyber, a lot of people focus on the ransom, but business interruption is often the much trickier and more difficult part of the claim to manage through. The further you are from the event, the clarity of the detail can get blurry. There are situations where just a few hours are huge in terms of business interruption and can be very difficult to substantiate. You need to be able to tell the story and quantify the value of damage."

Reliance on outsourcing puts small and mid-sized firms at risk

Small to mid-sized companies may be more at risk of cyber-attack due to their reliance on outsourcing for services, including managed IT and cyber security providers.

As large companies have hardened their cyber security, cyber criminals are increasingly targeting smaller companies, which often have less financial resource to invest in prevention and response capabilities. According to Mastercard's RiskRecon[21], data breaches at small businesses globally jumped 152% during 2021, while during the same time period breaches at larger organizations rose 75%. More than half (54%) of SMEs in the UK had experienced some form of cyber-attack in 2022, up from 39% in 2020, according to Vodafone[22].

"SMEs are particularly vulnerable to cyber-attacks and are disproportionately impacted compared with better prepared and resourced larger companies. They have more limited cyber security skills and are more heavily dependent on third parties including cloud service providers. They also tend to have less financial support to absorb the business interruption consequences," says **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial.**

If a small company with poor controls or inadequate risk management processes suffers a significant cyber incident, the reality is there is a chance it might not survive in the long run. In recent years, progress has been made, and there has been good collaboration between insurers, brokers and clients, but ultimately more awareness of, and risk management education about, cyber risk is still needed, and the insurance industry has a responsibility to help smaller companies with this process.

"To effectively address cyber security challenges, smaller companies should remain vigilant and have a clear understanding of the risks involved and allocate ample resources in terms of personnel, IT infrastructure, and budget to implement the required security measures," says Baviskar.

"Initiating a conversation with an MSSP (Managed Security Service Provider) can serve as an excellent initial move, allowing for the creation of an IT budget and strategy tailored to the business's specific priorities."

Mid-sized businesses can take a proactive approach to tackle cyber threats by first ensuring that their cyber security strategy effectively identifies their most crucial information system assets. Then, they should proceed to deploy appropriate detection tools and techniques tailored to uncover and nullify potential threats attempting to gain network access. These measures encompass the use of detection and monitoring software both at the network perimeter and on endpoints, often involving collaboration with cyber security service partners.

What are the weak areas where companies should strengthen their cyber controls?

From an underwriting perspective, insurers such as Allianz Commercial assess each risk individually, strongly focusing on the IT security level and cyber hygiene of a company. Based on Allianz Commercial underwriting and risk engineering questionnaires, a number of companies still need to improve their frequency of IT security training; network segmentation for critical environments; and patch management in particular. Companies' cyber incident response plans and cyber security governance can be among the weakest areas.

The good news is that insurers are now seeing a very different conversation on the quality of cyber risk than we were a few years ago and are therefore gaining much better insights as the cyber insurance market matures. Many customers are working with Allianz Commercial to improve their security levels

"But as the cyber threat also continues to mature, the mitigation and response capability must mature also," says **Tresa Stephens, a Regional Head of Cyber at Allianz Commercial**.

"Moving forward, insurers will want to understand more about how insureds are using technology, and how forward-looking they are in anticipating how the regulatory environment will change. For example, insureds can expect more questions from underwriters in areas like the application of artificial intelligence (AI), and the security of AI data sets," says Stephens.

Ultimately, cyber insurers have a role that goes beyond pure risk transfer, helping clients adapt to the changing risk landscape and raising their protection levels. The more insurers can partner with their clients, the more the impact of losses will hopefully reduce in future.

References

1 Black Kite, Ransomware Threat Landscape Report 2023
2 Akamai Research: Rampant Abuse Of Zero-Day And One-Day Vulnerabilities Leads To 143% Increase In Victims Of Ransomware
3 NCC Group, Cyber Threat Intelligence Report, March 2023 / Howden Predicts Global Cyber Insurance Premiums Could Exceed Usd 50 Billion By 2030, July 5, 2023
4 Cybersecurity Ventures, Global Ransomware Damage Costs To Exceed $265 Billion By 2031, June 4, 2021
5 Wired, Ransomware Attacks Are On The Rise, Again, July 12, 2023
6 IBM Security X-Force Threat Intelligence Index 2023
7 World Economic Forum, Wide-Ranging MOVEit Hack And Other Cybersecurity News To Know This Month, July 17, 2023
8 Reuters, MOVEit Hack Claims Calpers And Genworth As Millions More Victims Impacted, June 24, 2023
9 Cybersecurity & Infrastructure Agency, Understanding Ransomware Threat Actors: LockBit, June 14, 2023
10 IBM Security X-Force Threat Intelligence Index 2023
11 National Counterintelligence And Security Center, Kaseya VSA Supply Chain Ransomware Attack, August 10, 2021
12 Reuters, North Korean Hackers Breached A US Tech Company To Steal Crypto, July 21, 2023
13 Bleepingcomputer, Fortra Shares Findings On GoAnywhere MFT Zero-Day Attacks, April 19, 2023
14 Cybersecurity & Infrastructure Security Agency, ESXiArgs Ransomware Virtual Machine Recovery Guidance, February 8, 2023
15 Bloomberg, The Next Wave Of Scams Will Be Deepfake Video Calls From Your Boss, August 25, 2023
16 ISC2, Revealing New Opportunities For The Cybersecurity Workforce,
17 Gartner, Gartner Predicts Nearly Half Of Cybersecurity Leaders Will Change Jobs By 2025, February 22, 2023
18 IBM Security, Cost Of A Data Breach Report 2023
19 IBM Security, Cost Of A Data Breach Report 2023
20 IBM Security, Cost Of A Data Breach Report 2023
21 RiskRecon By Mastercard, Small Business, Mighty Attack Surface, August 23, 2022
22 Vodafone, Half Of SMEs Experience Surge In Cyber-Attacks – Vodafone Research Reveals, February 15, 2023

About Allianz Commercial

Allianz Commercial is the center of expertise and global line of Allianz Group for insuring mid-sized businesses, large enterprises and specialist risks. Among our customers are the world's largest consumer brands, financial institutions and industry players, the global aviation and shipping industry as well as family-owned and medium enterprises which are the backbone of the economy. We also cover unique risks such as offshore wind parks, infrastructure projects or Hollywood film productions.

Powered by the employees, financial strength, and network of the world's #1 insurance brand, as ranked by Interbrand, we work together to help our customers prepare for what's ahead: They trust on us for providing a wide range of traditional and alternative risk transfer solutions, outstanding risk consulting and multinational services as well as seamless claims handling.

The trade name Allianz Commercial brings together the large corporate insurance business of Allianz Global Corporate & Specialty (AGCS) and the commercial insurance business of national Allianz Property & Casualty entities serving mid-sized companies. We are present in over 200 countries and territories either though our own teams or the Allianz Group network and partners. In 2022, the integrated business of Allianz Commercial generated more than €19 billion gross premium globally.

Contacts

For more information contact your local Allianz Commercial Communications team.

Asia Pacific
Shakun Raj
shakun.raj@allianz.com
+65 6395 3817

Ibero/LatAm
Laura Llauradó
laura.llaurado@allianz.com
+34 660 999 650

North America
Jo-Anne Chasen
jo-anne.chasen@agcs.allianz.com
+1 917 826 2183

UK and Nordics
Ailsa Sayers
ailsa.sayers@allianz.com
+44 20 3451 3391

Central and Eastern Europe
Andrej Kornienko
andrej.kornienko@allianz.com
+49 171 4787 382

Mediterranean/Africa
Florence Claret
florence.claret@allianz.com
+33 158 858863

Lesiba Sethoga
lesiba.sethoga@allianz.com
+27 11 214 7948

Olivia Smith
olivia.smith@allianz.com
+27 11 214 7928

Global
Hugo Kidston
hugo.kidston@allianz.com
+44 203 451 3891

For more information contact az.commercial.communications@allianz.com

Follow Allianz Commercial on

Twitter / X **@Allianz_COMML** and

LinkedIn

www.commercial.allianz.com

Allianz Global Corporate & Specialty SE

Dieselstr. 8, 85774 Unterfoehring, Munich, Germany

Images: Adobe Stock

October 2023