Allianz

Khozinul / Adobe Stock

ALLIANZ COMMERCIAL

Cyber security resilience 2025

Claims and risk management trends

commercial.allianz.com

Melinda Nagy / Adobe Stock

Contents

Executive summary

The cyber risk and insurance landscape in 2025 reveals a complex and evolving threat environment where insured companies are becoming increasingly resilient against attacks with strengthening of cyber security and preparedness and response capabilities helping to mitigate the impact of large cyber losses in 2025 to date. However, the reliance on digital supply chains, impact of expanding privacy regulation, and more sophisticated social engineering attacks targeting employees are broadening the scope of potential losses.

Claims and loss trends

Analysis of **Allianz Commercial** cyber claims shows the overall frequency of notifications during 1H, 2025 was in line with a year earlier (around 300 claims), after a significant year-on-year increase during 2023 compared with 2022. Overall claims severity has declined by more than 50% during 1H, 2025 while the frequency of large loss claims (> €1mn) is down around 30%. However, the risk landscape is expanding beyond direct cyber-attacks. In this year's report, contingent business interruption, technology failures and privacy litigation emerge as main sources of losses – incidents such as wrongful collection or processing of data, and outages accounted for a record 28% of the value of large claims in 2024.

Ransomware shifts to mid-sized and less well-protected firms

Ransomware remains the biggest driver of cyber insurance claims analyzed by frequency and value, accounting for around 60% of the value of large claims (>€1mn) during 1H, 2025. High-profile attacks across many industries underscore ongoing threats, although there are signs international co-ordination by law enforcement agencies and the strengthening of cyber security by large corporates is having a positive impact. Yet ransomware groups continue to grow in number – a 50% increase during 1H, 2024 alone – and sophistication, adopting tactics and leveraging artificial intelligence (AI) to target weaknesses in cyber security, namely employees and suppliers.

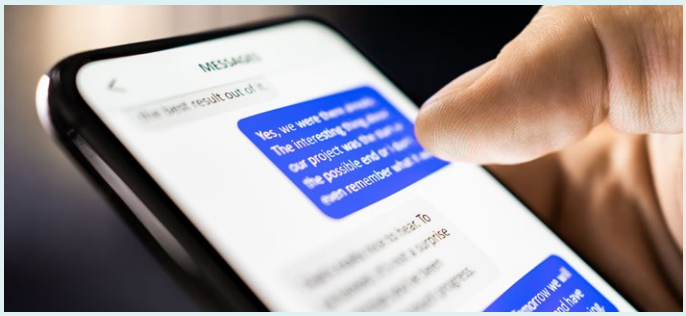
Attackers are also shifting focus from well-protected large corporations, particularly in the US and Europe, where the bar for a successful attack is now much higher, to mid-sized and smaller firms, which are less resilient, as well as firms in other territories, such as in Asia or Latin America. Ransomware was involved in 88% of data breaches at small and medium firms compared to 39% at large firms, according to Verizon, while cyber incidents also ranks as the top risk for smaller companies in the **Allianz Risk Barometer**.

Artem / Adobe Stock

Data exfiltration a top loss driver

As large companies have improved their response capabilities, recent years have seen a shift from purely extortion-based ransomware attacks to double extortion including data exfiltration – 40% of the value of large cyber claims (>€1mn) during 1H, 2025 included data theft, up from 25% in the whole of 2024. Losses involving data exfiltration were more than double the value of those without.

Data exfiltration is easier and faster for attackers than encryption and increases the likelihood of ransom payments. The average global data breach cost hit a record high (almost US$5mn) in 2024, driven by factors such as the impact of stricter data privacy regulation. Meanwhile, encryption rates in attacks fell to their lowest level in six years.



terovesalainen / Adobe Stock

The rise of sophisticated social engineering and credential-based attacks

Recent cyber-attacks display common tactics, including using sophisticated social engineering and compromised credentials to access networks, such as impersonating an employee locked out of an IT system. Many attacks also leverage suppliers or IT supply chains to access sensitive information. Approximately 60% of breaches in 2024 involved a human element, with third-party involvement doubling to 30%, according to Verizon. Attackers increasingly use compromised access credentials obtained via phishing or sold on the dark net, with a surge in specialist "brokers" operating in this space.

Scattered Spider, a hacking group behind recent attacks against casinos, retailers, airlines, and insurers, has used compromised access credentials and social engineering and phishing tactics to gain access to an organization's systems rapidly. More than 10 attacks were attributed to the group during 1H, 2025. Credential-based intrusions now outpace malware-based attacks, with 80% of attacks in the past year malware-free, compared to 40% in 2019, according to cyber security firm CrowdStrike. Generative AI is having a notable impact, helping threat actors create more convincing social engineering, and phishing emails and calls (vishing).

Manufacturers, professional services, and retailers most impacted sectors

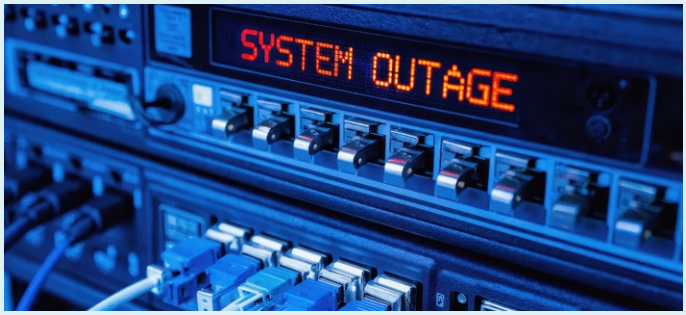
Retailers top the list of industries attacked during 1H, 2025 and are the third most impacted sector by cyber incidents, behind manufacturing and professional services, according to analysis of large cyber claims (>€1mn) since 2020. Companies in the manufacturing sector accounted for 33% of these claims by value, followed by professional services/ consulting firms (18%), and retail companies (9%).

Retailers often have high revenues, handle large volumes of personal data, and are vulnerable to business interruption, which all provide leverage when making extortion demands. They also tend to have large numbers of staff, suppliers and IT systems, which create a wide attack surface, while cyber security is typically less advanced than sectors like banking.

Supply chain dependency risks

The emergence of claims related to growing dependencies of IT supply chains is a key emerging trend. Contingent business interruption (CBI) supply chain events accounted for 15% of large cyber claims (>€1mn) by value in 1H, 2025, compared with 6% in 2024, according to **Allianz Commercial** analysis. Such losses can result from both attacks and technical faults, causing disruption to a critical service such as software or cloud services. Cloud intrusions increased 136% in 1H, 2025 compared to all of 2024, according to CrowdStrike. Disruption can also extend to physical products if an insured's supplier is unable to deliver goods required for production, while incidents can also result in a data breach.

Although many companies have improved their own cyber security controls, the risk of breaches at their IT suppliers and partners is harder to control. Vendors need to be well managed from a contractual perspective, but also around access control, monitoring and audits of suppliers.



aznan / Adobe Stock

Non-attack incidents broaden the scope of potential losses

Attack-driven losses continue to drive cyber insurance claims, but losses from events such as technical faults and data privacy liability are accounting for a greater proportion than previously – a record 28% of the value of large claims (>€1mn) analyzed during 2024.

Business interruption due to technical failure was present for the first time in **Allianz Commercial's** large loss claims data in 2024, accounting for around 10% by value, in part due to one of the largest outages in history at CrowdStrike. Such outages can result from technical glitches or human error.

rookielion / Adobe Stock

Privacy regulation and litigation continues to develop

Data breaches and privacy actions relating to wrongful collection and processing of data, for example, have increased in recent years, accounting for a record 18% of large claims (>€1mn) by value analyzed in 2024, triple the share of three years earlier.

Meanwhile, during 1H, 2025, technology/media professional indemnity claims accounted for a quarter of large cyber claims by value, up from 21% in 2024. Many are for legal actions against technology companies related to service performance, technical failings, and alleged breaches of privacy regulations and requirements, but can result from attacks too.

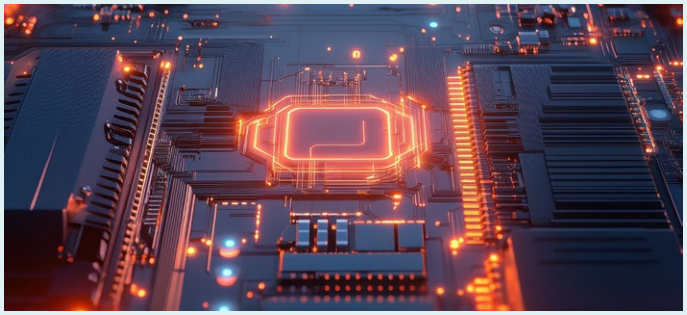
Recent years have seen a significant rise in class actions related to breaches of data privacy laws. Litigation reached unprecedented levels in 2024, with some 1,500 data privacy actions filed in the US alone. Compliance with diverse and changing privacy regulations is a significant challenge for companies, especially with advances in technology such as AI and biometrics. AI systems could facilitate breach of privacy regulation through unauthorized collection/use of data.

kaliel / Adobe Stock

Detection, response, and training – helping to reduce the cost of claims

Recent cyber-attacks have demonstrated the value of effective cyber hygiene, early detection, and incident response capabilities and their roles in reducing potential claim costs. Analysis shows in over 80% of large claims, insureds' decisions significantly influenced loss size, with many incidents preventable through basic controls such as patching, segmentation, backups, and multi-factor authentication (MFA). Detection and response capabilities can reduce claim costs by a factor of 1,000 and their importance is reflected in the forecasted growth of the global managed detection and response (MDR) market, expected to quadruple in size over the next decade.

Seventyfour / Adobe Stock



narin_nonthamand / Adobe Stock

Widening gap: insureds grow more resilient

The stable trend in overall cyber claims frequency so far this year (2025) stands in contrast to the wider threat landscape. Last year saw a new record for internet crime losses reported to the FBI's Internet Crime Complaint Center (IC3) – US$16.6bn.

The cyber-resilience gap between uninsured and insured organizations is widening. For example, in Germany, insurance industry figures show that the loss impact of cyber insureds increased by around 70% over four years, well below the 250% increase in the economic impact of cyber crime during the same period.

This resilience gap reflects cyber insurance policyholders' heightened awareness of risk and their actions to mitigate it, many of which are a condition of obtaining insurance. It also reflects the effectiveness of risk prevention services and advice and incident response assistance provided by insurers. Regular tabletop exercises and preparedness training can improve response effectiveness, minimizing business interruption, which accounts for over 50% of cyber claim values. Business interruption losses are closely corelated to early detection and containment and incident response, and business continuity planning will significantly reduce costs. Conversely, weak communication, coordination and indecision can prolong the impact of an event.

The transformative potential of AI-powered detection

AI is a hot topic among insureds, as organizations come under competitive pressure to adopt AI tools in an evolving regulatory environment. Attackers are using AI to automate and scale ransomware attacks, develop sophisticated malware, and craft convincing phishing campaigns. At the same time AI is helping to transform cyber security, speeding up and automating threat detection and response, and increasing company resilience. On average, organizations that used AI and automation in prevention saved US$2.2mn in breach costs, versus those that did not, according to IBM.

Regulation will raise the resilience bar

New regulations like the EU's Digital Operational Resilience Act (DORA) and the Network and Information Security Directive (NIS2) aim to raise cyber security standards across critical sectors, including supply chains. These frameworks will require enhanced risk management, incident reporting, and resilience testing, particularly benefiting mid-sized companies currently underprepared for such requirements.

Insurance market outlook

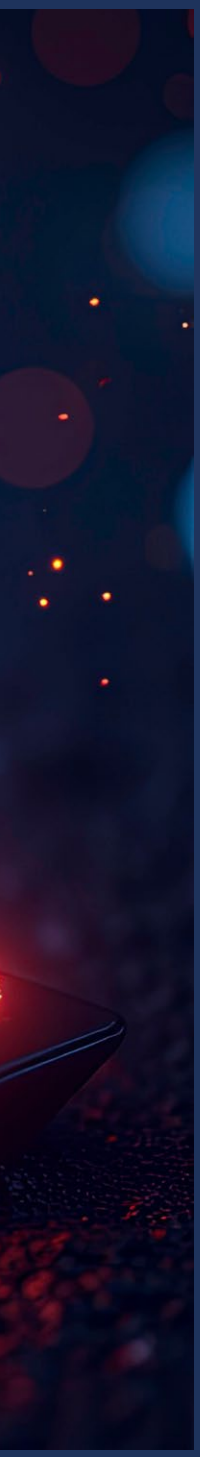
While cyber insureds have made significant strides in mitigating large cyber losses through improved security and preparedness, the evolving threat landscape and regulatory pressure requires ongoing vigilance and investment. Cyber insurance remains a crucial component in managing these risks, providing both financial protection and access to expertise that enhances overall cyber resilience. The global cyber insurance market is expected to more than double to nearly US$30bn by the end of the decade, driven by increasing digitalization and growing awareness. Despite relatively low penetration, demand is rising, especially among mid-sized firms and regions with a historically low uptake.

Claims and loss trends

Spirit / Adobe Stock

CLAIMS AND LOSS TRENDS

Cyber insureds take back control and gain momentum against attackers, but challenges remain



Strengthening of cyber security and preparedness and response capabilities by insured companies is showing encouraging signs of paying off, helping to mitigate the impact of large cyber losses in 2025 to date.

Analysis of Allianz cyber, technology errors and omissions and media claims shows that the overall frequency of notifications in the first half of 2025 was in line with activity a year earlier during 1H, 2024 (around 300 claims), after a significant year-on-year increase in frequency during 2023 compared with 2022. Overall claims severity has declined by more than 50% during 1H, 2025 while the frequency of large loss claims (>€1mn) is down by around 30%.

"The positive trend we see so far in 2025, particularly with regards to large cyber claims activity, is likely the result of insureds' cumulative investments in cyber security, detection and response, as well as trends in ransomware attacks, which tend to favor those companies which are well-protected and prepared," says **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**

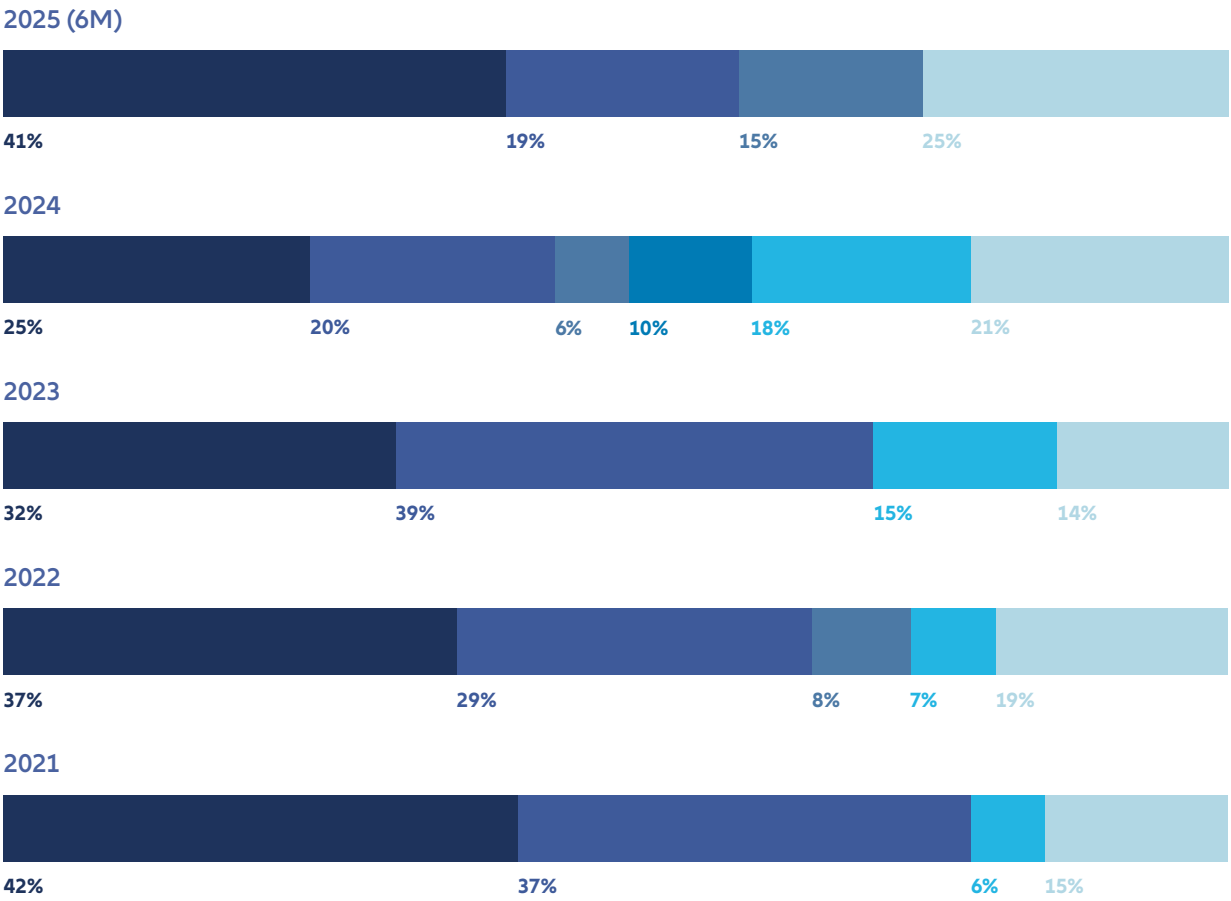
"A number of ransomware events have hit the headlines this year, but overall, we see that insured losses from these attacks have declined in 2025 to date. Insureds' increased detection and response capabilities are helping to stop attacks at an early stage. Every step an attacker progresses, and every minute that they are in the system, the impact goes up exponentially. The cost of a ransomware attack that progresses to data theft and encryption can be 1,000 times higher than an incident that is detected and contained early."

However, at the same time, an expanding risk landscape is broadening the potential scope of losses for companies, with non-attack incidents, such as wrongful collection and processing of data, as well as technical failure, having accounted for a record 28% of large claims by value during 2024. And while ransomware remains the top loss driver of all claims analysed, organizations continue to face new challenges and threats in the cyber space, such as their growing reliance on digital supply chains, the impact of expanding privacy regulation, and the increasing number of social engineering attacks which are targeting the weakest link in any well-protected company – the employee.

"At the same time, an expanding risk landscape is broadening the potential scope of losses for companies

Cyber claims analysis: Expanding risk landscape visible – incidents by loss category

By % share of total claims value – large claims only (>€1mn)



KEY

- Attack-driven losses (with data exfiltration)
- Attack-driven losses (without data exfiltration)
- Contingent business interruption (CBI)/supply chain)
- Business interruption due to technical failure
- Non-attack data breaches (e.g., wrongful collection and processing of data)
- Tech/media professional indemnity (e.g., legal actions related to service performance etc.)

Source: Allianz Commercial. Large claims analysis only (>€1mn) between 2021 and 2025 (6M) with a total value in the dataset in excess of €400mn

Trends

- ↑ **Share of tech/media professional indemnity losses increasing**
- ↑ **Non-attack data breach losses, driven by wrongful collection/processing of personal data, have risen in recent years but not seen yet during 1H, 2025**
- ↑ **Business interruption due to technical failure present for the first time in 2024, not only CrowdStrike driven**
- ↑ **Contingent business interruption extensions covering supply chain risks resurfaced in 2024**
- ↓ **Share of attack-driven losses has declined over time – from 80%+ in 2021**

CLAIMS AND LOSS TRENDS

Ransomware migrates to mid-sized and less well-protected firms as threat actors adapt to hardened cyber security

Ransomware remains the biggest driver for cyber insurance claims by frequency and loss value. Attack-driven losses accounted for around 60% of the value of large cyber insurance claims (>€1mn) analyzed by **Allianz Commercial** during 1H, 2025.

This year has seen a series of disruptive cyber-attacks against retailers in Europe and the US, including Marks & Spencer, Co-op and United Natural Foods. In July, Australian airline Qantas[1] confirmed that the data of up to six million customers may have been compromised in a cyber-attack.

While the ransomware threat shows little indication of abating, there are signs that international co-ordination by law enforcement agencies and the strengthening of cyber security by large corporates is having an effect on cyber insurance claims.

In early 2024, the operations of two leading ransomware-as-a-service (RaaS) groups – LockBit and Noberus – were disrupted by an international law enforcement operation. In July 2025, the UK's National Crime Agency[2] arrested four people (aged between 19 and 20) in connection with cyber attacks against UK retailers in 2025, which were reportedly carried out by ransomware affiliate Scattered Spider.

What is RaaS?

Ransomware-as-a-service (RaaS) is a cyber crime business model in which ransomware developers sell ransomware code or malware to other hackers, called "affiliates" who then use the code to initiate their own ransomware attacks.

However, ransomware activity has also rebounded as attackers and their affiliates realigned or were replaced by other groups, such as RansomHub (currently inactive), Akira, Qilin and DragonForce. Cyber security firm CrowdStrike[3] identified 26 new cyber-attack groups in 2024, bringing the total number it monitors to 257. The number of publicly disclosed ransomware attacks broke records in the first quarter of 2025 with a 45% increase compared to Q1 2024, according to ransomware prevention firm, BlackFog[4].

"The sweet spot for attackers is a company with large revenues, lots of personal records and that is easy to penetrate. But these targets are becoming harder to find, so they are moving down the chain where companies are less well protected," says **Michael Daum, Global Head of Cyber Claims at Allianz Commercial.** *"Our incident response partners are very busy dealing with incidents, mostly involving uninsured and smaller companies."*

Ransomware is now disproportionately affecting mid-sized and smaller organizations. According to telecoms firm, Verizon[5], ransomware was a component of 88% of data breaches involving small and medium-sized firms, compared with 39% of breaches at large firms. A survey by the World Economic Forum[6] found that the number of small organizations that believe their cyber resilience is inadequate has increased sevenfold since 2022, while the number of large organizations reporting insufficient cyber resilience has nearly halved. Cyber incidents also ranks as the top risk for smaller and mid-sized companies in the **Allianz Risk Barometer.**

"The bar for a successful attack against a well-protected large corporate is now much higher. And while hackers will succeed against large firms from time to time, there has been a shift in successful attacks away from large companies in the US and Europe towards smaller and mid-sized firms and those in other territories, such as Asia and Latin America," says **Daum.**

CLAIMS AND LOSS TRENDS

Data exfiltration ranks as top loss driver

As large companies have improved their response capabilities, recent years have seen a shift from purely extortion-based ransomware attacks to double extortion including data exfiltration.

Around 40% of large cyber claim (>€1mn) by value during 1H, 2025 included data exfiltration, up on 25% for the full year 2024. Losses were also more than double those from attack-driven claims without data exfiltration, **Allianz Commercial** analysis shows.

"We continue to see a shift in ransomware towards data exfiltration. It is much easier to steal data than to encrypt – it takes less preparation and work on the part of attackers," says **Caitlin Ewing, Complex Claims Analyst at Allianz Commercial.**

Data breach was cited as the most concerning cyber risk in this year's **Allianz Risk Barometer,** while the average cost of a global breach reached a record high at almost US$5mn ($4.88mn), according to the IBM Cost of a Data Breach 2024[7] report. Recent cost increases have been driven by a number of factors including the impact of stricter data privacy regulation.

What is data exfiltration?

Data exfiltration, also known as data extrusion or data exportation, is data theft: the intentional, unauthorized, covert transfer of data from a computer or other device. It is now a common feature of ransomware attacks to increase the chance of victims paying a ransom.

Data encryption is at the lowest level in six years, with 50% of attacks now resulting in this, down from 70% in 2024, according to cyber security firm Sophos[8].

During 2024, telecommunications company AT&T suffered two breaches which resulted in the data of tens of millions of customers and former customers being found in a dataset on the dark web[9]. In August 2025, it was reported[10] that it may have to pay individuals up to $7,500 in cash payments as part of a $177mn class action settlement for both breaches.

Artem / Adobe Stock

CLAIMS AND LOSS TRENDS

The rise of social engineering – threat actors target employees as the weakest link

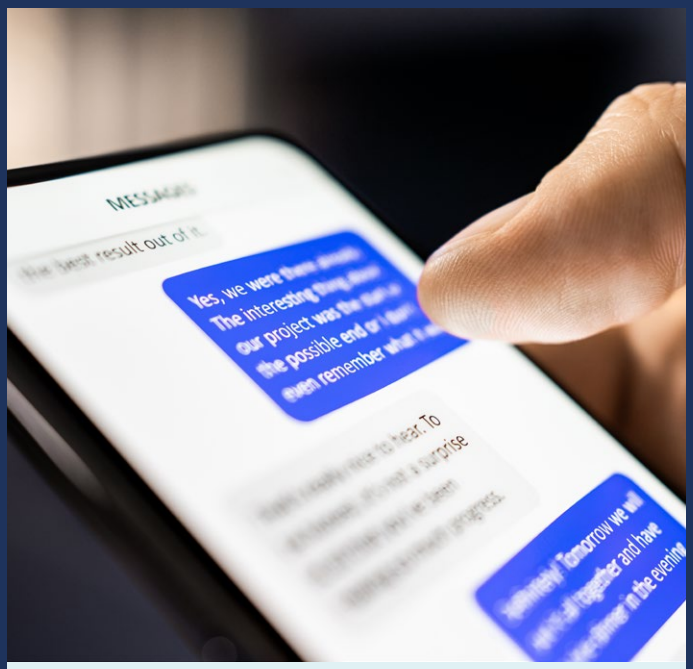
Recent cyber-attacks display several common themes, including the use of more sophisticated social engineering and compromised credentials to gain access to an organization's network. Many attacks also leverage suppliers or IT supply chains as a way to breach the otherwise robust cyber security of victim companies.

Around 60% of breaches in 2024 involved a human element, according to telecoms firm, Verizon[11], while the number that involved a third party doubled to 30%. Business email compromise (BEC) is the most common type of cyber incident, while phishing and social engineering are the most frequent initial intrusion vectors, according to consultant, Cybereason[12] – accounting for 46% of attacks it analyzed.

As organizations have strengthened their defenses, cyber criminals are targeting employees that are vulnerable to social engineering, according to **Caitlin Ewing, Complex Claims Analyst at Allianz Commercial.**

"Social engineering attacks have become a common way for hackers to gain access to sensitive information by exploiting human interactions. People are perceived as the weakest link in cyber security, and threat actors will look to exploit this," says **Ewing.** *"Social engineering is now a prominent driver of cyber claims. For threat actors, it is easier to effect, especially with AI. In the past, it was easier to spot with mistakes and unusual language, but now there are fewer obvious red flags."*

> Social engineering is now a prominent driver of cyber claims



terovesalainen / Adobe Stock

Four key stages to social engineering attacks

- **Information gathering:** Prior to attacks, scammers often utilize information shared on social media, such as an employee's job title or responsibilities, in order to deliver a convincing impersonation.
- **Building trust or creating urgency:** Hackers can either spend time building rapport to gain a person's trust or introduce a sense of urgency by creating a fake emergency to get the victim to take action.
- **Exploitation:** After their targets have either begun to trust them or respond to a fake emergency, hackers then trick people into turning over sensitive information.
- **Covering their tracks:** Once their goal is achieved, hackers can look to erase any sign of their activities.

CLAIMS AND LOSS TRENDS

Keys to the kingdom: Credentials overtake malware

Related to social engineering and phishing is the growing use of access credentials, such as usernames and passwords, as the initial point of access in a cyber-attack. Compromised credentials is now the most common attack vector, according to telecoms firm, Verizon[13].

Ransomware groups are using credentials obtained via phishing attacks or stolen in cyber-attacks, including those targeting IT suppliers, and sold on the dark net. In addition, specialist brokers gain access to organizations and sell this on to other threat actors, including ransomware groups. According to cyber security firm CrowdStrike[14], access broker activity surged in 2024, with advertised accesses increasing by nearly 50% over 2023.

Scattered Spider, a hacking group believed to be behind recent attacks against casinos, retailers, airlines and insurers, has used compromised access credentials and sophisticated social engineering and phishing tactics to gain access to an organization's systems. It is enjoying its most prolific year yet in 2025 with more than 10 publicly reported attacks attributed to it during the 1H. One scenario involves threat actors contacting an organization's IT help desk impersonating a legitimate employee in a bid to reset a password and/or multi-factor authentication (MFA). Once inside the IT system, the hackers then look to deploy ransomware, encrypting data and exfiltrating personal data. In one 2025 incident, the threat actor moved from account takeover to ransomware deployment in just 24 hours, 32% faster than in 2024, according to CrowdStrike[15]. Researchers have noted that one of the group's major strengths is the fact that its members are largely native English speakers who can convincingly act as American or British employees to get into a targeted company's online systems.

The focus on credentials is part of an overall move away from malware. In 2024, CrowdStrike[16] observed a 35% year-over-year increase in interactive intrusions, where hackers employ hands-on keyboard actions, rather than malware, to mimic legitimate user or administrator behavior. Some 80% of attacks over the past year were malware-free, up from 40% in 2019.

nuanjan / Adobe Stock

Social engineering remains a favored entry point for cyber criminals, as it is relatively quick and simple compared with hacking into a well-protected system, explains **Rishi Baviskar, Global Head of Cyber Risk Consulting at Allianz Commercial.**

"Using credentials is easier than hacking. Once they get the 'keys to the kingdom' hackers can quickly access a system, elevate their access privileges and then move through the system."

Countering social engineering and credential-based attacks comes down to basic cyber hygiene, according to **Baviskar:**

"Multi-factor authentication (MFA), strong access controls, and training all help to reduce the risks of these kinds of attacks. And if user access is limited to essential business purposes only, it makes it much harder for the hackers. Companies need to adapt and develop counter measures to different scenarios as attackers change tactics."

While cyber criminals are looking to circumvent cyber security measures, MFA remains a must-have security control. Only 36% of firms that fell victim to a Business Email Compromise (BEC) attack had MFA on their compromised accounts, according to Cybereason[17].

"Multi-factor authentication (MFA) has been a real game-changer. It is so much harder to intrude with MFA. Although we are seeing some cases where attackers use interception techniques or MFA fatigue to circumvent authentication, the lack of MFA would be a much bigger problem," says **Baviskar.**

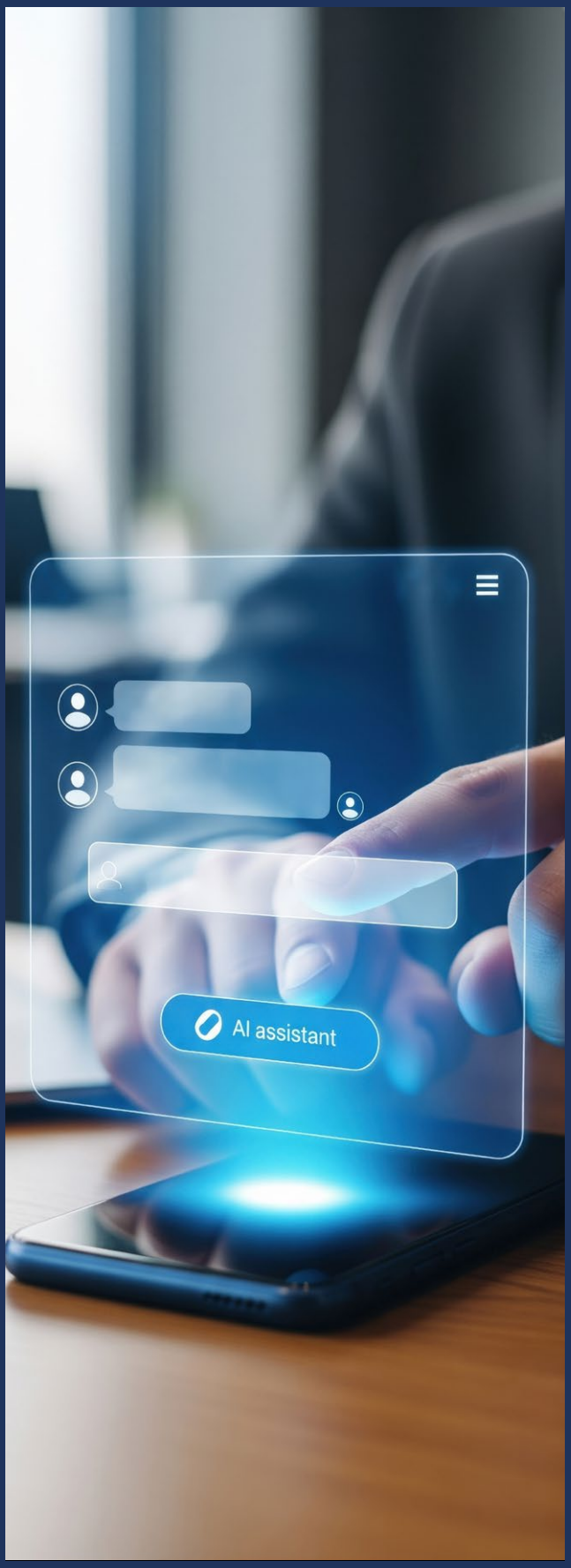
CLAIMS AND LOSS TRENDS

AI driving more effective social engineering and malware

Cyber criminals and nation state groups have been avid adopters of artificial intelligence (AI), which is increasing productivity and sophistication. For example, threat actors are using AI to increase the speed and scope of ransomware attacks, as well as develop attack tools and more natural looking malware coding, which is harder for antivirus software to detect.

Generative AI is having a notable impact on social engineering, helping threat actors to create more convincing and personalized social engineering, phishing emails and credential harvesting sites. Research[18] has shown that the click-through rate for AI-generated phishing emails is comparable to that of content created by humans. Criminals are also using AI to use deep fakes to defraud companies or acquire access credentials.

"Attackers are using AI to automate and speed up the process of cyber-attacks – and we can see the volume and frequency of attacks is increasing – which puts the emphasis back on the need for defense. If you have weak cyber security or do not invest in detection and response, then attackers are likely to break through. It only takes one successful attack," says **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial.**



photchara / Adobe Stock

> Attackers are using AI to automate and speed up the process of attacks, which puts the emphasis back on the need for defense

CLAIMS AND LOSS TRENDS

Retailers becoming the most targeted sector

Retailers top the list of industries attacked during 1H, 2025 and are the third most impacted sector by cyber incidents, behind manufacturing and professional services, according to analysis of large cyber claims (>€1mn) by value since 2020. Companies in the manufacturing sector accounted for 33% of claims by value, followed by professional services and consulting firms (18%) and retail companies (9%).

Retailers in the UK have been the victims of successful attacks over the past 12 months, which have included Harrods, Marks & Spencer and the Co-operative Group. Ahold Delhaize, one of the world's largest food retailers, also suffered a data breach last year following a ransomware attack at its US operation, while French luxury goods brand Louis Vuitton[19] was hit by multiple cyber-attacks this year.

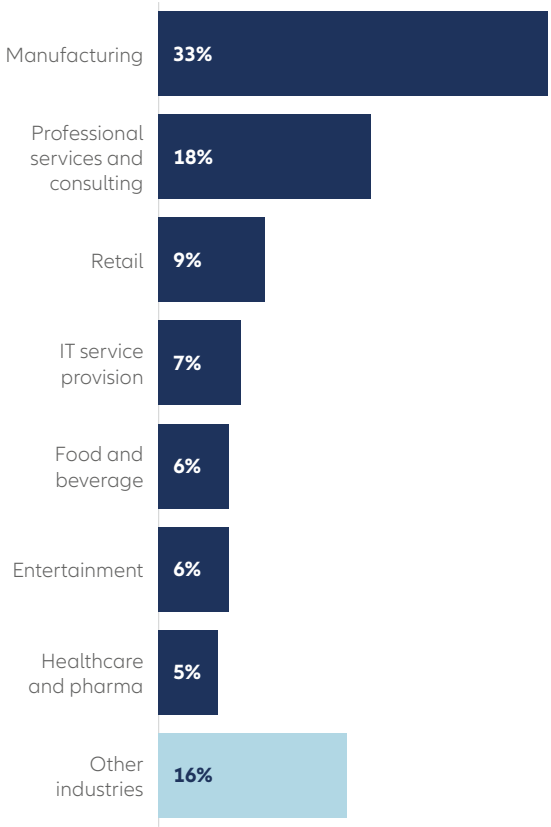
Many of the attacks against retailers are thought to be the work of ransomware group Scattered Spider and featured several common themes, including the use of double extortion and sophisticated social engineering.

Retailers present many of the characteristics that cyber criminals look for, such as high revenues, large volumes of personal data and vulnerability to business interruption – all factors that provide leverage when making extortion demands. Retailers also tend to have large numbers of staff, suppliers and IT systems, which create a wide attack surface, while cyber security is typically less advanced than in sectors like banking.

Sector-focused cyber attacks can create aggregation issues for insurers, according to **Tresa Stephens, Head of Cyber, North America, Allianz Commercial:** *"We have seen several attacks in the past year targeting specific sectors, such as retail, while healthcare and education have been targeted previously. When attackers go after a specific industry it just reinforces the need for insurers to manage their exposures and maintain a diversified portfolio,"* says **Stephens.**

Most impacted industries according to large cyber claims (>€1mn)

% share according to value of claims



Source: Allianz Commercial. Large claims analysis only (>€1mn) between 2020 and 2025 (6M) with a total value in the dataset in excess of €450mn

In September 2025, British luxury car maker, Jaguar Land Rover said its retail and production activities had been "severely disrupted"[20] following a cyber security incident. The attack was linked to members of the Scattered Spider group, as well as other hackers.

CLAIMS AND LOSS TRENDS

CBI/supply chain emerges as a key threat

A key trend over the past 18 months has been the emergence of claims related to growing dependencies of IT supply chains. Contingent business interruption (CBI) supply chain events accounted for 15% of large cyber claims (>€1mn) by value in 1H, 2025, compared with 6% in 2024, according to **Allianz Commercial** claims analysis. CBI losses are a particular concern because they can result from both attacks and technical faults.

The past year has witnessed a number of significant CBI supply chain attacks. CDK Global, which provides software to the automotive industry, was hit with a ransomware attack affecting thousands of US auto dealerships in 2024. Blue Yonder, a supply chain software company, was affected by a ransomware attack in November 2024 that caused disruption to customers, including major UK food retailers Morrisons and Sainsbury's.

"Contingent business interruption has been a distinct trend. If there is an event involving a business partner it can have a significant impact on your business, even when you are well prepared," says **Caitlin Ewing, Complex Claims Analyst at Allianz Commercial.**

Supply chains are emerging as an important driver of cyber claims and present a significant risk of CBI. Over half of large organizations (54%) identified supply chain challenges as the biggest barrier to achieving cyber resilience, according to a recent World Economic Forum report[21].

A cyber-attack or a technical fault impacting a third party's IT systems can result in disruption to a critical service – such as software or cloud services – for insureds. Cloud intrusions increased 136% in the first half of 2025 compared to all of 2024, according to cyber security firm, CrowdStrike[22]. Disruption can also extend to physical products if an insured's supplier is unable to deliver goods required for production as the result of an IT outage or cyber-attack.

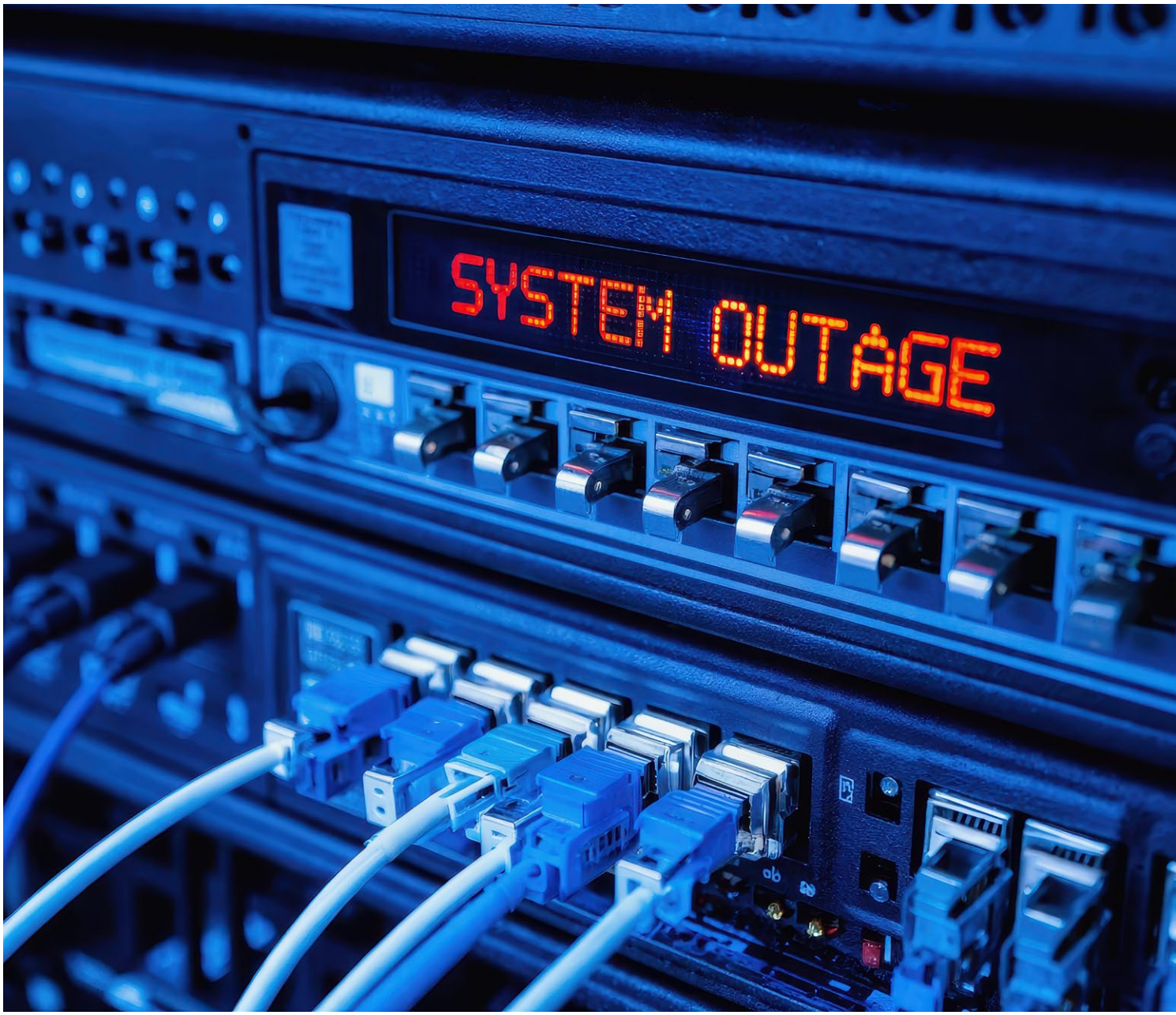
"Most businesses now rely on third party suppliers for essential digital services, such as software, cyber security and data storage and processing. As a result, it is important to understand these critical dependencies and the potential impact on an organization should they go down due to an outage, technical failure or a cyber attack," says **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

Supply chain is the number one emerging threat topic for cyber insurance at present, according to **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.** In addition to potential CBI losses, cyber incidents at a third-party supplier can also result in a data breach, such as the loss of access credentials or personal data.

"Many companies have done a great job of boosting cyber security controls, detection and response, and mitigating the total cost of a cyber incident. But there remains the risk of breaches at their IT suppliers and partners. That is much harder to control. Looking forward, vendors need to be well controlled and managed, from a contractual perspective, but also around access control, monitoring and audits of suppliers," says **Daum.**

> The risk of breaches at companies' IT suppliers and partners is much harder to control

Expanding risk landscape drives non-attack losses



aznan / Adobe Stock

EXPANDING RISK LANDSCAPE DRIVES NON-ATTACK LOSSES

Tech failure and outages make first large claims appearance

While attack-driven losses continue to drive cyber insurance claims, losses from technical faults and data privacy liability are accounting for a greater proportion than previously – a record 28% of the value of large claims (>€1mn) analyzed in 2024.

Business interruption due to technical failure was present for the first time in **Allianz Commercial's** large loss claims data in 2024, accounting for around 10% of the value of large claims, in part due to the outage at cyber security service provider CrowdStrike, one of the largest IT outages in history, affecting an estimated 8.5 million Windows systems worldwide. The outage caused significant disruption for healthcare, retail, financial services and hospitality, as well as leading to thousands of flight cancelations and several port closures in the US and Europe.

System outages can result from a range of technical glitches or human errors. Fashion retailer H&M[23] was temporarily unable to make instore payments following an IT outage earlier this year, while a cloud storage system misconfiguration caused a data breach at German car manufacturer Volkswagen[24] that compromised the data of 800,000 electric vehicle owners in late 2024.

Technology failures are not uncommon, according to **Rishi Baviskar, Global Head of Cyber Risk Consulting:**

"When a critical piece of software or service provider goes down, it can result in significant business interruption and a large loss for businesses and their insurers – comparable in size to a ransomware event. It could be a software bug, a flawed update, misconfiguration or an outage and it can have a cascading effect that causes issues for multiple insureds."

Data centers that house cloud and outsourced IT services are also vulnerable to natural catastrophes, such as floods, power outages and extreme weather events, such as heatwaves and water shortages. Failure of cooling systems can cause systems to go into failsafe mode, resulting in potential service outages.

Utilities outages, such as power blackouts, can also lead to data loss and IT service disruption. The April 2025 blackout in Spain and Portugal is estimated to have caused some €1.6bn[25] in losses to the public and private sector. This year has seen communication network outages in Spain, France, Czech Republic and India. During the first half of 2025, Allianz has tracked more than 10 major outages.

> When a critical piece of software or service provider goes down, it can result in significant business interruption and a large loss for businesses and their insurers

EXPANDING RISK LANDSCAPE DRIVES NON-ATTACK LOSSES

Privacy regulation and litigation continues to develop

Non-attack data breaches and privacy actions, such as wrongful collection and processing of data, have increased in relevance in recent years, accounting for a record 18% of cyber claims by value in 2024, according to **Allianz Commercial's** large claims (>€1mn) analysis, triple the share of three years earlier.

Meanwhile, during 1H, 2025, technology/media claims accounted for a quarter of large claims by value, up from 21% in 2024. Many of these claims are for legal actions against technology companies related to service performance, technical failings and alleged breaches of privacy regulations and requirements, but they can also be related to attacks.

rookielion / Adobe Stock

Recent years have seen a significant rise in US class actions related to breaches of data privacy laws, which continue to be introduced and developed by state legislators. Data privacy litigation reached unprecedented levels in 2024, with some 1,500 data privacy actions filed last year alone, according to law firm Duane Morris[26].

"Non-attack data breach claims and tech/media professional indemnity claims have become significant as companies collect more data on individuals, and with a changing regulatory and legal landscape. In the US, state privacy laws continue to develop while the plaintiff's bar is extremely entrepreneurial, finding new opportunities to bring class actions against companies for potential breaches of data privacy," says **Caitlin Ewing, Complex Claims Analyst at Allianz Commercial.**

Biometrics sparked a wave of class action litigation in recent years, as courts have tested new privacy legislation in this area, such as the Illinois Biometric Information Privacy Act (BIPA). A recent clarification to BIPA has narrowed the scope of potential damages, but more recently class action litigation has expanded to include the Illinois Genetic Information Privacy Act, explains **Ewing.**

There have also been hundreds of class actions filed against companies for unauthorized sharing and use of data related to new technologies, including web-tracking technology such as pixel and session replay software. Plaintiffs are bringing actions using both state privacy and wiretapping laws.

Data privacy class actions continue to be filed in the US, but it remains to be seen how they will pan out, says **Tresa Stephens, Head of Cyber, North America, Allianz Commercial:** *"The plaintiff's bar is hungry and is looking to use new privacy regulation along with existing laws to challenge the way some companies use technology and push back against a perceived surveillance culture."*

For example, a multitude of lawsuits have been filed related to the so-called Daniel's Law in New Jersey – which restricts the disclosure of certain public officials' home addresses.

> Organizations are collecting data on individuals across multiple countries and states, each with its own data privacy laws and regulations

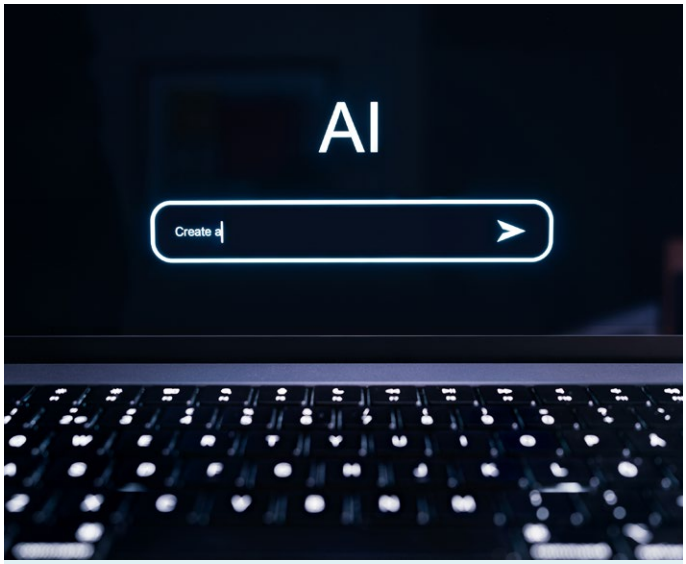
"We are seeing the first wave of litigation from Daniel's Law – there has been a lot of activity based on that initial law, and now we are seeing other states considering similar legislation," says **Ewing.**

Compliance is a moving goalpost, according to **Stephens:**

"Organizations are collecting data on individuals across multiple countries and states, each with its own data privacy laws and regulations. To keep pace with regulation in real time is a significant challenge, especially with advances in technology like artificial intelligence and biometrics."

By 2026, about half of the US population will be covered by a state comprehensive privacy law, according to law firm BakerHostetler[27]. US states continue to introduce or modify data privacy legislation in areas like data collection and use, biometrics, children's data protection and data brokers.

Complying with regulations, such as breach notification requirements, can be challenging for companies, especially in the midst of a cyber-attack. However, breach response and crisis management services that typically accompany cyber insurance can support organizations with experienced experts that can work quickly, explains **Stephens.**



terovesalainen / Adobe Stock

AI liability and litigation exposures

Artificial intelligence (AI) is a hot topic among insureds, as organizations come under competitive pressure to adopt AI tools in an evolving regulatory environment.

"AI is now an inescapable topic, and an interesting emerging area of risk and liability. Almost every company is looking to use AI to operate more efficiently. No-one wants to be left behind in the next phase of the technology revolution," says **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

"Underwriters will ask how companies are using AI, with a particular focus on higher risk use cases, such as consumer facing applications, or where AI is embedded into a service that is offered to customers. We want to know more about such use cases and what steps are being taken to mitigate the risks."

In addition to its role in cyber security, AI is also likely to drive future liability exposure and claims. For example, AI systems could facilitate breach of privacy regulation through unauthorized collection and use of data.

"There is exposure. Privacy litigation relating to the use of AI could be an area to watch as a potential source of cyber claims going forward," says **Caitlin Ewing, Complex Claims Analyst at Allianz Commercial.**

Detection, response and training

kaliel / Adobe Stock

DETECTION, RESPONSE AND TRAINING

Reducing the cost of a claim

Recent cyber-attacks have demonstrated the value of good cyber hygiene and detection and response capabilities, as well as the need for adequate training programs for employees in order to improve their awareness of potential threats. All have been shown to significantly limit the impact of an incident.

"A big take-away from this year's report is that while the importance of cyber hygiene is still critical, response preparedness for an event is equally as important. And this is where cyber insurance can really help. It gives customers access to a wide range of experts and services that can help prepare and manage an incident, which significantly mitigates the financial, business and reputational impact," says **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

> "Detection and response capabilities can reduce the cost of a claim by a factor of 1,000

Analysis of **Allianz Commercial** claims shows how basic controls – such as patching, segmentation, backups and the use of multi-factor authentication (MFA) can make all the difference preventing and mitigating cyber losses. In more than 80% of large claims (>€1mn) **Allianz Commercial** sees, the insured company's decisions significantly contributed to the size of the loss, and most incidents could have been easily avoided or contained.

Detection and response capabilities, in particular, can reduce the cost of a claim by a factor of 1,000. Their expansion is reflected in the growth of the global managed detection and response (MDR) market, which is predicted to more than quadruple in size from around US$3bn in 2024 to $12bn by 2034, according to Precedence Research[28].

€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).

Early detection and preparedness, in particular, is even more important with the growing reliance on technology and third-party service providers, says **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial.**

"It's not if, but when a cyber incident will happen, so resilience is key. Focus on detection and containment to control the cost of business interruption – be prepared, test regularly and retain incident response experts. Shortening periods of disruption and containing breaches quickly will result in significant cost savings."

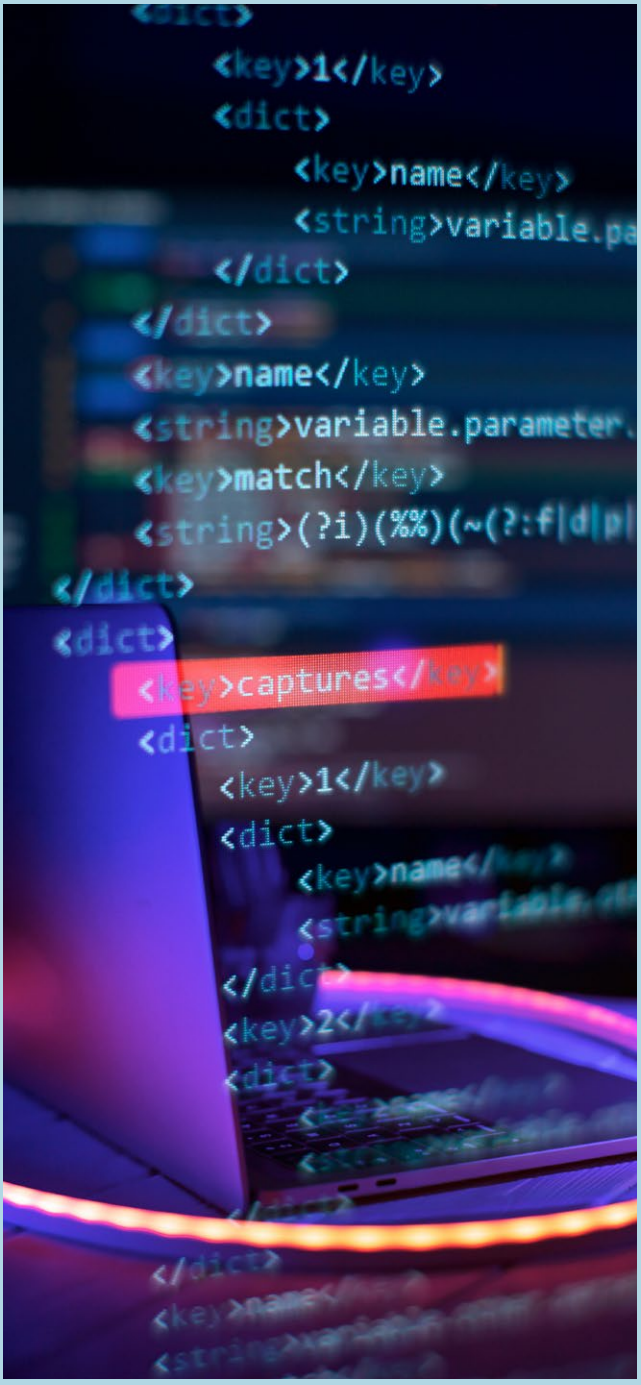
This positive trend should give companies the confidence to invest in cyber security in an evolving cyber risk landscape, says **Stephens:**

"The risk landscape keeps changing and we never know what new challenge is on the horizon. New technologies, like artificial intelligence (AI), the increasing reliance on IT supply chains and outsourced services, and a changing regulatory and legal environment can create new risks and loss scenarios in a relatively short time."

Advances in cyber security, including AI-powered detection technology, are creating new opportunities to get one step ahead of cyber criminals, according to **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**

"Until recently it was very difficult for an organization to build up their cyber defenses to a level that would result in a minimal chance of a successful attack. In the past, cyber criminals had the edge. Now there are the tools and processes for each company to better determine its fate," says **Daum.**

"We will never completely eliminate the risk, but there has never been a better time to invest in systems, controls and defenses. The ability for companies to influence and mitigate their cyber risk has never been greater."



Maximusdn / Adobe Stock

> In the past, cyber criminals had the edge. Now there are the tools and processes for each company to better determine its fate

DETECTION, RESPONSE AND TRAINING

Widening gap: Insureds grow more resilient

The stable trend in cyber claims frequency so far this year stands in contrast to the wider threat landscape. Ransomware attacks continued their upwards trend in 2024, with a 56% increase in active ransomware groups during the first six months, according to IBM[29]. Last year also saw a new record for internet crime losses reported to the FBI's Internet Crime Complaint Center (IC3) – US$16.6bn[30].

The cyber-resilience gap between uninsured and insured organizations continues to widen. In Germany, insurance industry figures show that the loss impact of cyber insureds increased by around 70% over four years, well below the 250% increase in the economic impact of cyber crime during the same period[31].

The widening gap between insured and non-insured companies reflects policyholders' heightened awareness of cyber risk and their actions to mitigate it, many of which are a condition of obtaining insurance. But it also reflects the effectiveness of risk prevention services, advice and incident response assistance provided by cyber insurers, explains **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

"Companies that purchase cyber insurance tend to be risk aware and are more likely to be willing to invest in cyber security. There is a clear value in cyber insurance that goes beyond risk transfer, and extends to threat intelligence, loss prevention, mitigation and response from a range of risk consulting and claims experts. Allianz, for example, provides clients with access to subsidized tabletop exercises, which are designed to test an organization's response to certain cyber event scenarios," says **Stephens.**

According to the World Economic Forum's Global Cybersecurity Outlook 2025[32], having some form of insurance helps organizations to become more cyber resilient: among organizations classed as highly resilient, only 7% claimed to not have cyber insurance.

Seventyfour / Adobe Stock

JonoErasmus / Adobe Stock

DETECTION, RESPONSE AND TRAINING

Be prepared with tabletop exercises

One recent cyber claim managed by **Allianz Commercial** demonstrated the value of tabletop exercises. The insured suffered a cyber-attack just weeks after taking part in an exercise, which meant the response team was well prepared to deal with the incident, ultimately helping to mitigate the cost of the claim, according to **Caitlin Ewing, Complex Claims Analyst at Allianz Commercial.**

"Tabletop exercises prepare companies for a cyber incident and give them confidence in their response plans. Businesses and the threat landscape are constantly changing, so regular resilience training and preparation will help people feel capable when something happens," says **Ewing.**

Tabletop exercises are a particularly useful tool to help companies prepare and mitigate the business interruption impact of a cyber incident, although not all companies routinely do so, according to **Tresa Stephens, Head of Cyber, North America, Allianz Commercial:**

"Everyone needs a playbook. People leave organizations, systems and suppliers change, so it's important to have a response plan and test, update and embed it in the culture of the company. This should be a priority."

> Everyone needs a playbook. People leave organizations, systems and suppliers change, so it's important to have a response plan and test, update and embed it in the culture of the company

DETECTION, RESPONSE AND TRAINING

Ransomware attacks highlight need for business interruption workarounds

Recent cyber-attacks against retailers in the UK and US in particular highlight the potentially catastrophic impact of business interruption (BI) on an organization, and the need for robust cyber business continuity planning.

BI remains the largest single driver for loss for cyber claims, accounting for over 50% of the value of losses, according to **Allianz Commercial** claims analysis. Cyber and business interruption were the top two risks of concern in this year's **Allianz Risk Barometer.**

The recent retail attacks, while similar in nature, resulted in varying degrees of disruption. Marks & Spencer indicated in its results statements that the April 2025 attack was expected to cost the UK retailer some £300mn in lost profit[33] after the firm suffered months of disruption to stock systems and online sales. The Co-operative attack[34] compromised the data of some six million customers and affected stock levels at some stores. However, the company reportedly stopped the attack before attackers were able to encrypt its systems.

BI losses are closely correlated to early detection, incidence response and business continuity planning. Early detection and containment will significantly reduce the cost of BI, but weak communication, coordination and indecision can prolong the impact of a ransomware attack, leading to a larger financial and reputational impact. Cyber BI is very different to a traditional property damage event, which, typically, can be limited to a single location. In contrast, a cyber-attack can quickly impact an entire organization and is likely to be met with less sympathy from customers and business partners than a natural catastrophe.

When preparing an incident response, organizations need to consider the potential impact from a loss of systems and disruption to supply or sales, as well as possible mitigating actions, according to **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**

"As part of their incidence response and business continuity plans companies should think through the mechanisms and workarounds that would enable the business to keep running and supplying customers in the event of a cyber incident. It helps to define these mechanisms in advance, and prepare, test and train for potential cyber business interruption events," says **Daum.**

"As part of response preparations, it helps to have good visibility of dependencies and have plans in place – or at least consider potential mitigating actions – should supply be disrupted. Preparing upfront for business interruption – and understanding any policy requirements – can help minimize disruption and control costs," adds **Caitlin Ewing, Complex Claims Analyst, Allianz Commercial.**

Many companies continue to struggle to quantify their cyber risk, particularly when it comes to business interruption.

"There are so many layers, moving parts and variables, it is sometimes hard to put a figure on it, but brokers and insurers and third-party service providers can help and share probable loss data and experience," says **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

The shortage of IT professionals and growing skills gap is also making it harder to understand and quantify the potential impact of a cyber incident. The IT skills shortage is expected to impact nine out of 10 organizations by 2026 with a cost of US$5.5trn, according to the International Data Corporation[35].

DETECTION, RESPONSE AND TRAINING

The transformative power of AI-powered detection

Artificial intelligence (AI) is helping to transform cyber security, speeding up and automating threat detection and response, as well as helping organizations identify vulnerabilities and increase resilience.

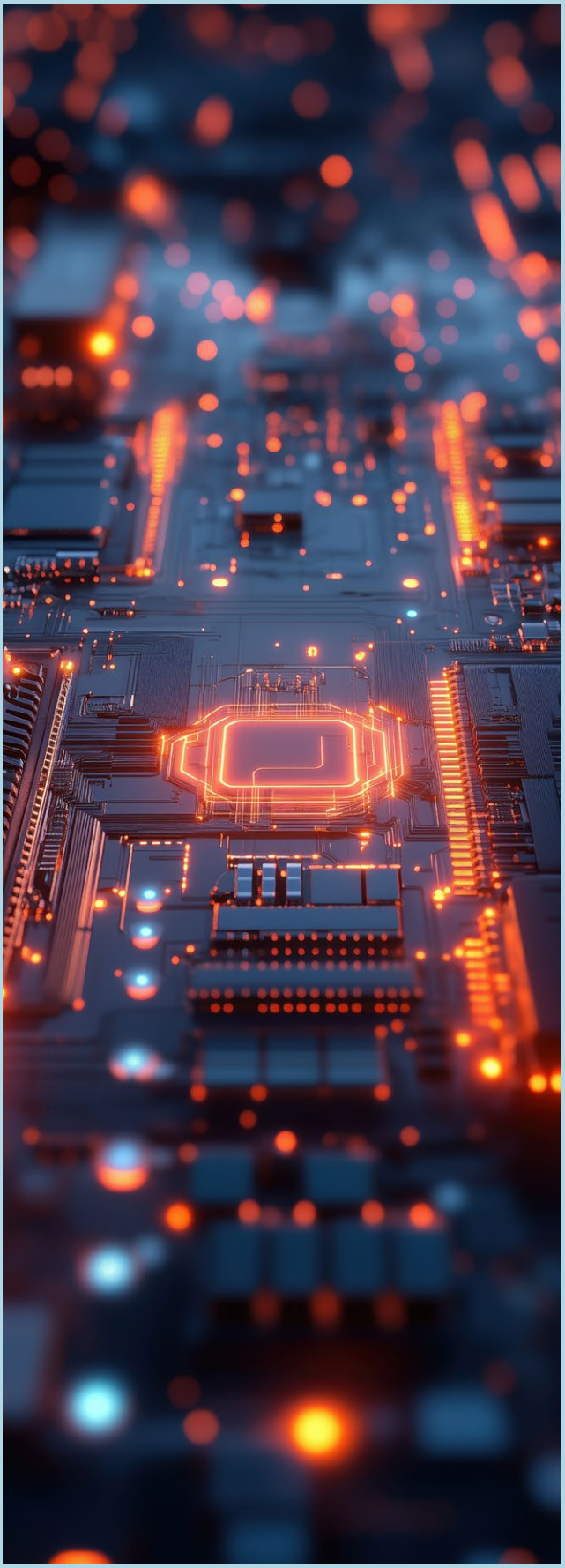
On average, organizations that used AI and automation in prevention saved US$2.2mn in breach costs, versus those that did not, according to IBM's Cost of a Data Breach Report 2024.[36] The survey found that two out of three organizations deployed security AI and automation for IT security in 2024.

"AI is creating an advantage for defenders currently, but you need to invest in AI-enabled detection tools. If you do not, then it is an advantage for attackers," warns **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**

AI plays an increasingly important role in cyber security, according to **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial:**

"Attackers are using AI to assist cyber-attacks, but companies are also increasingly using it to protect their businesses, analyzing the content of potential phishing emails and spotting patterns in code and meta data. AI can flag anomalies in software code and recognize potential malware, as well as identify unusual behavior.

"AI-enabled solutions like Security Orchestration, Automation, and Response (SOAR) tools enable organizations to respond to security threats more rapidly, reducing the time between detection and containment, and therefore reducing business interruption."



narin_nonthamand / Adobe Stock

DETECTION, RESPONSE AND TRAINING

Regulation set to raise the cyber resiliency bar

Incoming regulations are set to raise cyber resiliency, a move that should bolster supply chains and reduce the impact of ransomware attacks.

Data protection regulations, such as the EU's General Data Protection Regulation (GDPR), are now well established in most key markets, and organizations are generally on top of compliance. However, the EU is now looking to bolster its digital strategy with a focus on cyber security and emerging areas like artificial intelligence (AI).

Along with DORA (Digital Operational Resilience Act), which aims to strengthen the digital operational resilience of financial entities by mandating robust IT risk management, incident reporting, and resilience testing, the revamped Network and Information Security Directive (NIS2) is set to transform cyber security in the EU. The directive, which is currently being implemented by member states, establishes a common cyber security framework across 18 critical sectors, including their supply chains. Organizations covered by NIS2 will have to take appropriate cyber security risk management measures and notify relevant national authorities of significant incidents.

"NIS2 will be challenging for a lot of companies, but I consider it to be an opportunity. Like DORA, NIS2 is an excellent piece of legislation, and it represents a paradigm shift in the way EU governments treat cyber risks," says **Robin Kroha, Chief Information Security Officer & Head of Global Protection and Resilience at Allianz Services.**

NIS2 will raise cyber security standards for many companies, including mid-sized companies that currently lack adequate cyber security and risk management systems, according to **Kroha:**

"Many companies – particularly mid-sized companies– are woefully underprepared for such regulations. They do not have many of the risk management systems you would see in a large company, such as business continuity management, crisis management, information security and IT security management."

ImageFlow/Adobe Stock

The expansion of cyber security requirements under NIS2 should significantly boost cyber resilience in Europe, according to **Kroha.** NIS2 will require organizations to adopt many of the best practices that help mitigate the impact of a cyber-attack, such as backup strategies, detection and response services and business continuity planning.

"NIS2 will be immediately beneficial. The average mid-sized company lacks well established management systems in the cyber realm. Companies that bounce back are those that have strong cyber security and digital resilience baked into their culture," says **Kroha.**

DETECTION, RESPONSE AND TRAINING

Insurance market trends

The global cyber insurance market is predicted to more than double to close to US$30bn by the end of the decade.

"Cyber criminals will just keep moving to the next target, and as more and more organizations experience these attacks, it will drive demand for cyber insurance, especially among mid-sized companies and in parts of the world where investment in cyber risk mitigation has not been as prevalent. As companies digitalize it makes sense that they will want to manage and protect their digital risks and assets in much the same way as they do for physical assets," says **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

> The cyber insurance market is in a good position to grow and take on more risk

Insurance penetration remains relatively low, yet it plays an important role in helping build resilience at a time of rapid technological and regulatory change. Yet many companies remain unaware of the breadth of cover offered by cyber insurance, which can include costs associated with breach response, business interruption and regulatory fines and penalties, according to **Stephens.**

A World Economic Forum survey[37] found that 71% of large organizations are confident in their cyber insurance to adequately cover potential losses due to cyber events, as opposed to only 35% of small organizations.

"The cyber insurance market is in a good position to grow and take on more risk. Greater awareness and investment in cyber security has improved the underlying risks, while cyber risk modeling and reinsurance protection is helping insurers better manage aggregate exposures," says **Stephens.**

Photographee.eu / Adobe Stock

References

1 Qantas, Qantas cyber incident, July 2, 2025
2 Reuters, UK police arrest four over cyber-attacks on M&S, Co-op and Harrods, July 10, 2025
3 CrowdStrike, CrowdStrike 2025 Global Threat Report
4 BlackFog, BlackFog report reveals record number of ransomware attacks from January to March, April 9, 2025
5 Verizon, 2025 Data Breach Investigations Report
6 World Economic Forum, Global Cybersecurity Outlook 2025
7 IBM, IBM report: Escalating data breach disruption pushes costs to new highs, July 30, 2024
8 Sophos, The State of Ransomware 2025
9 CNN, AT&T says personal data from 73 million current and former account holders leaked onto dark web, March 30, 2024
10 CNN, AT&T may pay customers up to $7,500 in $177 million data breach settlement, August 16, 2025
11 Verizon, 2025 Data Breach Investigations Report
12 Cybereason, TTP Briefing: January - May 2025
13 Verizon, 2025 Data Breach Investigations Report
14 CrowdStrike, How to navigate the 2025 identity threat landscape, March 31, 2025
15 CrowdStrike, 2025 Threat Hunting Report
16 Crowdstrike, 2025 Global Threat Report
17 Cybereason TTP Briefing: January - May 2025
18 Fred Heiding, Simon Lermen, Andrew Kao, Bruce Schneier, Arun Vishwanath, Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects, November 30, 2024
19 Computer Weekly, Luxury retailer LVMH says UK customer data was stolen in cyber-attack, July 14, 2025
20 BBC, Jaguar Land Rover production severely hit by cyber-attack, September 2, 2025
21 World Economic Forum, Global Cybersecurity Outlook 2025
22 CrowdStrike, CrowdStrike 2025 Threat Hunting Report: AI Becomes a Weapon and a Target, August 4, 2025
23 RetailTechInnovationHub, H&M all apologies as fashion and homeware retailer reports major IT outage affecting payments in stores, June 4, 2025
24 European Parliament, Data leak affecting owners of Volkswagen Group electric vehicles, January 16, 2025
25 Reuters, How warning signs hinted at Spain's unprecedented power outage, May 2, 2025
26 Duane Morris, DMCAR Trend #7 – Data breaches gives rise to an unprecedented number of class action filings, January 21, 2025
27 BakerHostetler, Comprehensive State Privacy Laws
28 Precedence Research, Managed Detection and Response (MDR) Market Size, Share and Trends 2025 to 2034
29 IBM, Research finds 56% increase in active ransomware groups, November 18, 2024
30 FBI, Federal Bureau of Investigation Internet Crime Report 2024
31 Bitkom, Wirtschaftsschutz 2024, Berlin, August 28, 2024
32 World Economic Forum, Global Cybersecurity Outlook 2025
33 M&S, Full Year Results for the 52 Weeks Ended 29 March 2025
34 BBC, Co-op boss confirms all 6.5m members had data stolen, July 16, 2025
35 International Data Corporation, IT skills shortage expected to impact nine out of ten organizations by 2026 with a cost of $5.5 trillion in delays, quality issues and revenue loss, according to IDC, May 14, 2024
36 IBM, Cost of a Data Breach Report 2024
37 World Economic Forum, Global Cybersecurity Outlook 2025

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 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 us to provide 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 through our own teams or the Allianz Group network and partners. In 2023, the integrated business of Allianz Commercial generated around €18 billion in gross premium globally.

Further information and contacts

For more detailed information on cyber insurance, please contact your regional Allianz Commercial contacts.

commercial.allianz.com

Email: az.commercial.communications@allianz.com

Allianz Global Corporate & Specialty SE, Königinstraße 28, 80802 Munich, Germany.

Commercial Register: Munich, HRB 208312

September 2025