Mahnoor/ Adobe Stock

ALLIANZ COMMERCIAL

Cyber security resilience 2024

Trends in data breach and privacy risk

Gorodenkoff/ Adobe Stock

Contents

Overview

Cyber claims have continued their upwards trend in 2024, driven in large part by the rise in data and privacy breach incidents. The frequency of large cyber claims (>€1mn) in the first six months of 2024 was up 14% while severity increased by 17%, according to Allianz Commercial claims analysis. This followed a 41% increase in frequency but just a 1% increase in severity during 2023. Data and privacy breach-related elements are present in two thirds of these large losses.

Key developments

- Data breach losses rise with (mass) ransomware exfiltration attacks, a consequence of the growing interdependencies between organizations, sharing ever more volumes of personal records.
- Litigation and regulation drive uptick in 'non-attack' privacy claims, such as wrongful collection and incorrect processing of personal data. Activity has tripled in value. Claims can be in the hundreds of millions of dollars.
- AI, digital interconnectivity, and the growing commercial value of data main factors shaping the future risk landscape.
- Chatbots and AI-generated content are likely to bring a higher degree of data privacy risk. However, AI is also an essential tool in fighting cyber attacks, potentially saving companies millions of dollars.
- Data breach risks are best mitigated through good cyber hygiene, breach and attack simulation tools, early response and detection capabilities and crisis management. Many companies need to improve oversight of cyber security in their supply chains.

Data breach is not a new risk in cyber insurance, but it is a threat that has been somewhat overshadowed in recent years by encryption-based ransomware attacks and resulting business interruption. Nevertheless, it ranks as the cyber risk exposure companies fear most, according to 59% of respondents in the **Allianz Risk Barometer 2024**.

The growing significance of data breach losses among cyber insurance claims is down to two notable trends. The shift by cyber criminals targeting personal data, and a jump in 'non-attack' data privacy related class action litigation, resulting from wrongful data collection and/or processing of personal data, for example. These two trends have been particularly evident in the US, which now accounts for 72% of large (>€1mn) cyber claims overall (in the first six months of 2024), up from 41% in 2023. The share of large claims in the US with data privacy violations in the first six months of 2024 was 100%, according to the value of claims analyzed. The share of 'non-attack' (privacy) data breaches tripled in value from 7% in 2022 to 21% during the first half of 2024.

Meanwhile, the past 18 months has seen several high-profile mass-data exfiltration cyber attacks – including MOVEit, MGM, T-Mobile, Change Healthcare and Snowflake – that have resulted in the theft of records belonging to hundreds of millions of individuals, triggering class action litigation and increasing pressure for companies to pay large extortion demands.

The underlying trends driving data breach and privacy exposure is a universal reliance on personal data, and the still evolving regulatory and legal environment. Digital supply chains are intensifying, with organizations collecting, storing, and sharing more personal and commercially sensitive data. Artificial intelligence (AI), particularly focused on consumer products and services, cloud-based services and 5G will only accelerate this trend.

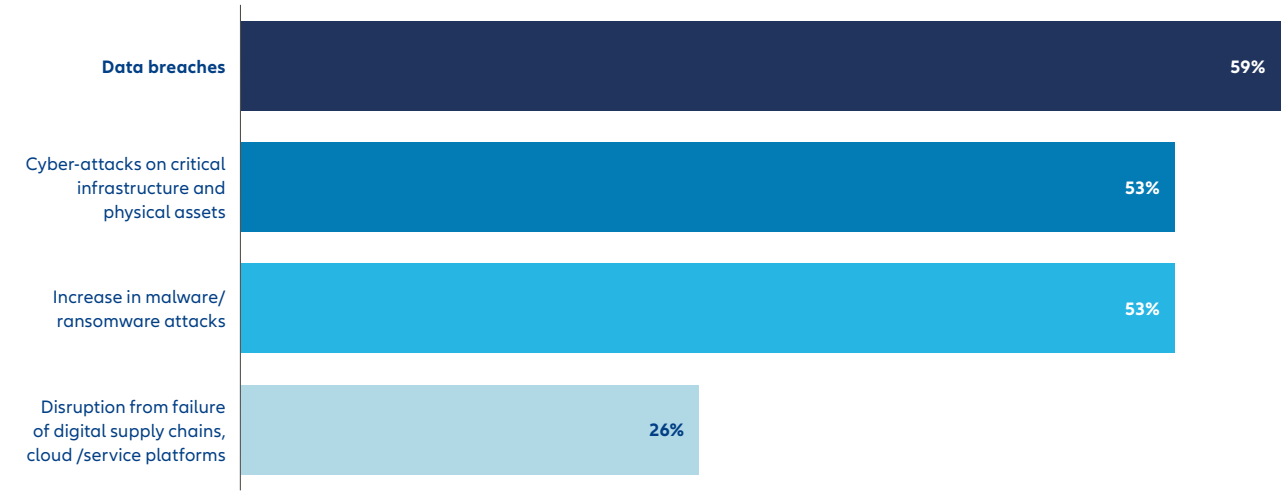
Against this backdrop, businesses large and small must redouble their efforts to protect data. Large data breaches continue to result from gaps or lapses in cyber security, particularly in digital supply chains. AI is becoming an essential tool in the fight against cyber attacks, as it can quickly identify a security breach and automatically isolate systems and databases, as well as having the potential to significantly reduce the cost and life cycle of a data breach claim by automating and speeding up tasks, such as forensics and notification. For example, the cost of postage for notifications can represent a significant component of damages, costing in excess of US$20mn in some cases.

> The share of 'non-attack' (privacy) data breaches, such as wrongful collection, has tripled in value from 7% to 21% in two years

The insurance industry must also step up its focus on data privacy, replicating recent successes in ransomware, providing loss prevention and mitigation advice, such as early detection and response to this increasingly important area of cyber exposure.

Which cyber exposures concern your company most over the next year?

Data breach is the cyber exposure of most concern, according to **Allianz Risk Barometer** respondents, followed by cyber attacks on critical infrastructure and physical assets and the increase in ransomware attacks.



Source: Allianz Risk Barometer 2024. Total number of respondents: 1,112. Respondents could select more than one risk. Top four answers.

MysteryShot / Adobe Stock

1. Claims trends

The rise of data and privacy breach claims

1. CLAIMS TRENDS

Ransomware: Slaying the Hydra

Ransomware continues to be the top cause of cyber insurance loss. During the first six months of 2024, it accounted for 58% of the value of large cyber claims (>€1mn). However, improved cyber security and backup strategies are helping insured companies better withstand attacks.

After a series of disruptive ransomware attacks, including the Colonial Pipeline attack in May 2021[1], which disrupted fuel supplies to the US Southeast, governments and enforcement agencies have moved to tackle ransomware gangs head on. Last year, law enforcement agencies from 10 countries[2] took out the LockBit ransomware group, one of the most prolific and harmful groups at that time, having caused billions of dollars' worth of damage.

Despite these successes, ransomware remains a significant and persistent threat, and a major cause of financial and reputational loss for organizations large and small. The February 2024 cyber attack against UnitedHealth Group's Change Healthcare will reportedly cost the US company up to US$1.6bn this year[3]. A ransomware attack in June 2024 against UK blood testing firm Synnovis[4] caused disruption to patient services and led to stolen personal and health data being published on the dark web.

"Ransomware is like the proverbial Hydra. Each time you cut off its head, another one grows back in its place. Each time a ransomware gang is taken down, you can be 100% sure that another will replace it, and that its members will reorganize and establish a new group," says **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**

Attacks are also becoming more sophisticated and targeted, with cyber criminals using artificial intelligence (AI) to automate attacks and encryption to avoid detection. Mirroring the wider digital economy, cyber criminals are also becoming more interconnected, outsourcing and sharing specialist skills and services.

While there have been welcome successes for law enforcement and from increased international collaboration, the threat of ransomware will not go away. The number of ransomware attacks increased by an average of 75% in 2023, according to Allianz Commercial analysis of cyber threat intelligence from tech providers. For the first time, total ransomware payments exceeded $1bn in 2023, according to Chainalysis[5].

Allianz Commercial has observed a stabilization of ransomware claims in 2024, after several years of increases. The positive trend is an indicator that insurers' recommendations and insureds' cyber security is working, according to **Daum.**

"During the first half of 2024, the impact of ransomware activity was quite stable. Due to the increase of 'non-attack' claims, the ransomware share among large losses has decreased by about 15%," says **Daum.** *"This positive trend in our portfolio reflects investments in cyber security, supported by risk assessments and our recommendations. So, while the ransomware threat persists, we appear to have stopped the upwards trend of recent years."*

Analysis of Allianz claims data shows that insured companies fared better than businesses as a whole, demonstrating the value of informed investment in cyber security.

Seventyfour/ Adobe Stock

"Organizations that purchase cyber insurance and follow the recommendations of insurers are responding better to ransomware than firms that do not," says **Marek Stanislawski, Global Cyber Underwriting Lead, Allianz Commercial.** *"This demonstrates that the value of cyber insurance goes well beyond the payment of claims. Insurance helps companies make the business case for cyber security investment and direct their resources to the most effective measures."*

"Ransomware losses are still significant, but are now relatively stable and under control, as today we know what it takes to successfully defend against the threat from ransomware, including investment in early detection and response, which is a key driver for the magnitude of loss."

In 2023, the number of ransomware attacks increased by an average of

75%

Total ransomware payments exceeded

US$1bn

1. CLAIMS TRENDS

Data exfiltration drives data breach claims

Data exfiltration is now a common feature of ransomware attacks as attackers continue to steal personal and commercially sensitive data to increase the chances of victims paying the ransom.

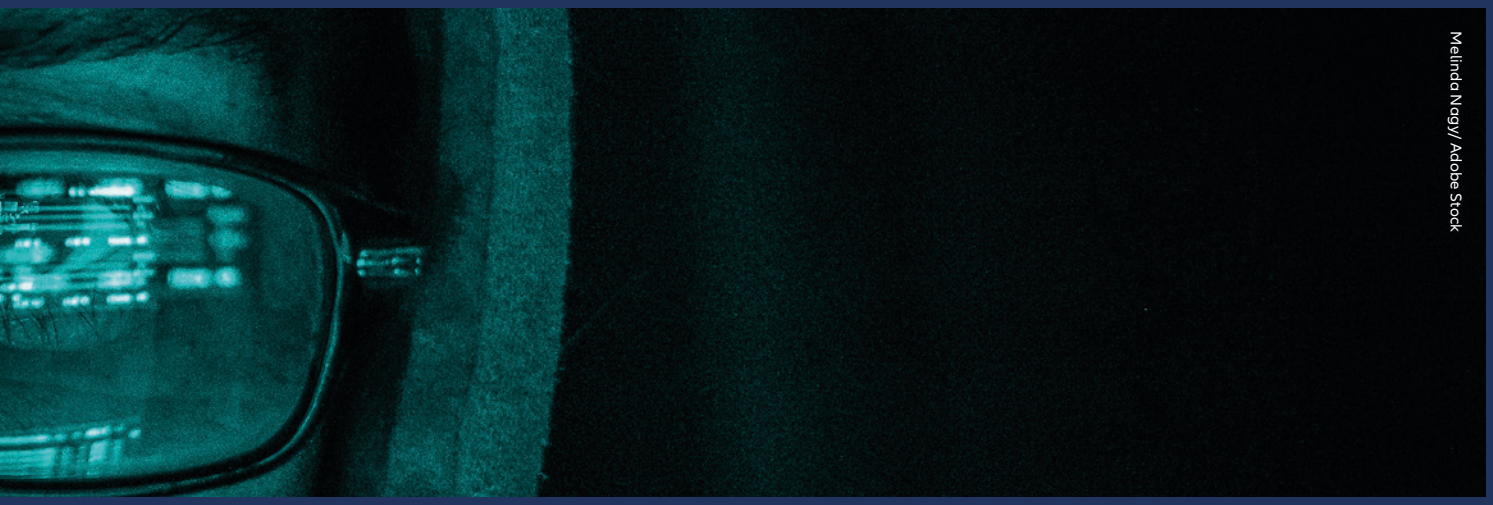
Cyber criminals continue to find ways to extort money from business, leveraging their reliance on IT systems, supply chains and data. Known as double or triple extortion, cyber criminals will look to exfiltrate data and encrypt files, creating multiple avenues for extortion.

"Data exfiltration is now a well-established method of cyber extortion. Even if you have a backup, your data is effectively lost as the attackers have a copy and will threaten to publish on the dark web," says **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**

In around a third of ransomware-related claims, data exfiltration is now the key loss driver, with some two-thirds being first party costs, business interruption, restoration, and incident response.

"The gap between business interruption (usually the most expensive cost driver of cyber-related losses) *and data breach claims has been closing with the increase in data exfiltration,"* explains **Marek Stanislawski, Global Cyber Underwriting Lead, Allianz Commercial.** *"Typically, what starts as a ransomware loss escalates into a data privacy event, once it is revealed that attackers have stolen personal data. This can lead to a large claim involving regulatory fines, notification costs and potentially third-party litigation, in addition to extortion demands, first party costs and any potential business interruption from the ransomware attack."*

Even a lesser discussed cost, such as the cost of postage for notifications can represent a significant component of damages. For example, the cost of mailing a paper letter to 50 million people alone, would be somewhere in the range of US$20mn+.



Melinda Nagy/ Adobe Stock

Data exfiltration has become the preferred method of attack for some ransomware groups, as it is typically easier to steal data than encrypt, which requires higher levels of administrative access rights. Cyber criminals have also turned their attention to data exfiltration as companies have implemented more effective backup strategies, which make it harder to carry out successful encryption-based ransomware attacks.

"Data exfiltration has been a real game changer. The theft of personal and sensitive corporate data puts organizations in the public eye, and ratchets up the pressure, leading to more successful extortion attempts for cyber criminals as companies are more likely to pay ransom demands to protect customers' personal data," says **Daum.**

High ransom payments are observed for attacks with data exfiltration, especially when sensitive data has been leaked, **Daum** adds.

Companies are two-and-a half times more likely to pay a ransom if data is exfiltrated, on top of the encryption, Allianz analysis of claims activity shows. However, paying a ransom for exfiltrated data does not necessarily resolve the issue. The company may still face third party litigation for the breach of data. Indeed, there are few cases where a company should believe that there is no other solution other than paying the ransom to be able to re-access its systems or data. Any impacted party should always inform and cooperate with the authorities.

Nevertheless, the average ransom payment increased 500% in the last year to $2mn, while almost a third (30%) of demands were for over $5mn, according to cyber security firm Sophos[6].

> Typically, what starts as a ransomware loss escalates into a data privacy event, once it is revealed that attackers have stolen personal data

Several cyber attacks in 2023 led to the loss of millions of personal records. In January, it was reported that a "bad actor" accessed personal data belonging to 37 million customers of US telecoms company T-Mobile after hackers exploited an Application Programming Interface (API) vulnerability[7]. In September, US hospitality and casino group MGM Resorts was hit by a ransomware attack that resulted in the loss of customer personal data and business interruption, at a cost to the company in excess of $100mn[8].

In one of the biggest data breaches of 2024, hackers stole personal data from UnitedHealth Group subsidiary Change Healthcare, which processes around 6% of all US medical claims[9]. The breach occurred after hackers used compromised credentials to access the company's Citrix portal. In exchange for patient data, UnitedHealth paid a ransom demand of $22m in Bitcoin, according to Reuters[10]. It was reported that the breach could potentially involve the data of up to one in three Americans[11].

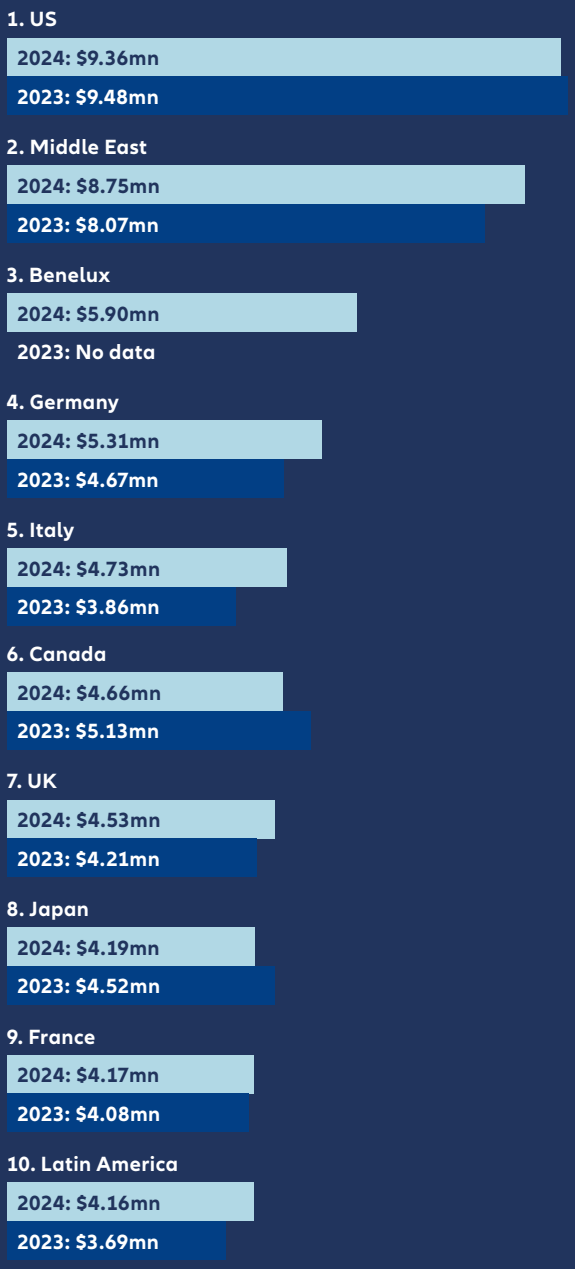
US companies alone recorded a record 3,205 data breaches in 2023 (78% more than in 2022), affecting 353 million known victims, according to the Identity Theft Resource Center (ITRC)[12]. The trend continued into 2024: The number of data breaches increased 14% in the first half, while the number of data breach victims increased 490% to over one billion.

"Companies now hold huge amounts of personal data. We have seen claims where attackers have exfiltrated huge volumes: as much as 50 terabytes, or the equivalent of 10,000 computer hard drives. And that data will have included personal and health data, trade secrets and sensitive confidential information on customers and suppliers," says **Daum.**

"Analyzing such huge volumes of data – to understand what data is affected and who is to be notified – is extremely time consuming and expensive," says **Tresa Stephens, Head of Cyber, North America, Allianz Commercial**. *"The greater the number of records, the higher the costs from data forensics, breach notification and class action litigation. For a large breach it can cost many millions of dollars and take weeks if not months."*

Even the average cost of a data breach reached an all-time high in 2024 of $4.9mn in 2024, up 10% year-on-year, and the highest increase since the pandemic according to IBM[13]. The US had the highest average cost— $9.36mn. Rounding out the top five regions and countries were the Middle East, Benelux, Germany, and Italy.

Cost of a data breach by country or region



Source: IBM, Cost of a Data Breach Report 2024

Worldwide, the average cost of a data breach reached an all-time high in 2024 of

US$4.9mn

The US had the highest average cost

US$9.4mn

1. CLAIMS TRENDS

‘Non-attack’ claims increase – privacy litigation ramps up

Breaches of data privacy regulation have emerged as a major driver for cyber insurance claims over the past two years. The share of ‘non-attack’ (privacy) data breaches, such as wrongful collection of data, increased from just 7% in 2022 to 14% in 2023, rising again to 21% in the first half of 2024, according to Allianz Commercial claims value analysis.

‘Non-attack’ data breaches are increasing in both frequency and severity, according to **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.** *“The latest development in cyber insurance has been a marked rise in ‘non-attack’ cyber claims, mostly related to data privacy breaches in the US. In the past these claims were rare but now they make up a significant proportion of claims.”*

The rise in ‘non-attack’ data privacy claims is the consequence of several ongoing trends, including developments in technology, the growing commercial value of personal data, and a developing regulatory and legal landscape. Unlike the EU’s General Data Protection Regulation (GDPR), privacy regulations in the US are less prescriptive and open to interpretation, while plaintiff lawyers are hungry for potential sources of revenue. This creates a grey area that is ripe for class action litigation, according to **Daum.**

“We are seeing more privacy data-related claims in the US where there is a growing trend for class action litigation related to privacy violations, such as around consent and data usage,” says **Marisa Anthony, Senior Complex Claims Analyst, Allianz Commercial.**

“Regulators and courts are interpreting data privacy laws and how they apply in the real world, as companies use personal and biometric data and technology in their day-to-day operations, and in products and services. Data has become extremely valuable, and companies can be tempted to push boundaries in pursuit of their commercial interests,” adds **Daum.**

On the rise: examples of ‘non-attack’ data breaches

- Perceived invasion of privacy when tracking consumer behavior.
- Improper data collection action.
- Sharing data without the consent of users.
- Incorrect processing of personal data.
- Incorrect / misuse of biometric information.

> We are seeing more privacy data-related claims in the US where there is a growing trend for class action litigation related to privacy violations

Large US and international corporations that hold huge amounts of personal data are now targets for privacy class action litigation. UK education and publishing group Pearson faced a potential class action lawsuit in the US for allegedly sharing Meta Pixel data without the consent of users[14]. In July 2023, Amazon reached a US$25mn settlement with the Federal Trade Commission over alleged privacy violations related to its voice assistant Alexa and doorbell camera Ring[15].

"There are many eyes on US data privacy cases, such as state attorneys and regulators, including the Federal Trade Commission and the Securities and Exchange Commission," says **Anthony.**

"We all desire better technology and the efficiencies and benefits it brings. But there is a tension between wanting more and better technology on the one hand, with the need to protect privacy on the other. This conflict, which is unlikely to go away in the foreseeable future, results in data privacy litigation and claims."

The increase in 'non-attack' claims is also a reflection of cyber insurance coverage. Most large companies will seek to include cover for 'non-attack' breaches of privacy regulation, which can be broad, depending on an individual insurer's wordings. In the US, hundreds of class action claims have been filed across a wide range of data privacy regulations, such as Illinois' Biometric Information Privacy Act (BIPA), the California Invasion of Privacy Act (CIPA), the Video Privacy Protection Act (VPPA), and federal wiretapping laws.

"In its early years, cyber insurance provided cover for data breaches arising from a cyber attack, but during periods of increased competition, terms and conditions and scope of cover have broadened to include 'non-attack' privacy events, such as wrongful collection of data," says **Marek Stanislawski, Global Cyber Underwriting Lead, Allianz Commercial.**

The cost of some data privacy breach claims is as large, or even larger, than a ransomware incident, according to **Daum.** *"A major data privacy breach can generate losses of a magnitude we are not used to in the cyber insurance market. We are now seeing claims for 'non-attack' data breaches in the hundreds of millions of dollars, while the total cost will be even higher as reputational damage is not insured."*

Data privacy regulations and court rulings in the US can result in a spiral of litigation, resulting in potentially large accumulations of losses for insurers. If a court rules that a certain practice or technology breaches data privacy laws, it opens multiple companies up to copycat and follow-on class action litigation.

"When you think of a systemic or large cyber loss event, we tend to talk about a zero-day vulnerability or contagious malware that leads to multiple claims, or a major internet infrastructure outage. But we can now see the possibility of similar claims from data privacy. This is a new element for the cyber market to consider, particularly outside of the US," says **Daum.**

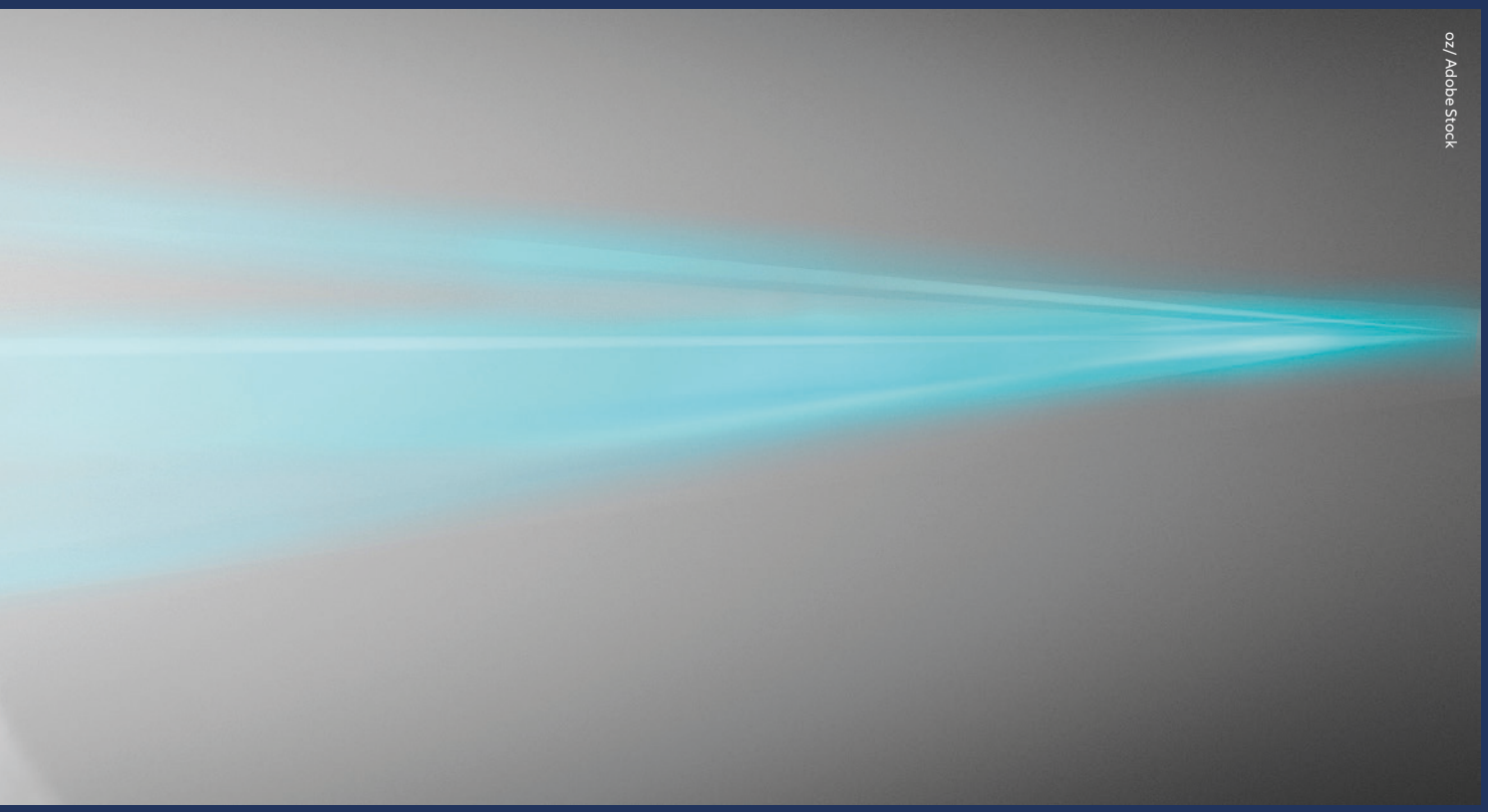
For example, multiple class action lawsuits have been launched against organizations using Meta Pixel tracking tools to track consumer behavior. Entertainment streaming platforms have been targeted with class action lawsuits alleging that they may have violated privacy protection rights.

"Hundreds of thousands of companies use tracking technology like Meta Pixel. Technology is not bulletproof, and plaintiff law firms in the US will test perceived breaches of data privacy. If successful, it follows that they will look for others to target, resulting in a cascade of class action litigation," says **Daum.**

'Non-attack' data privacy claims will remain a hot topic.

"As cyber insurers, we are having to shift focus. In discussions with clients, it is critical we understand their data governance standards and how transparent they are when it comes to their use of consumers' data, who they share it with, and their approach to vendor cyber security," says **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

"We are looking at better understanding the drivers for loss and advising companies on how best to prevent and mitigate against data privacy incidents. We need to replicate the success we have had in addressing ransomware in the data privacy space," adds **Stanislawski.**


ozz/ Adobe Stock

2. Emerging trends and loss drivers

Regulation, AI and connectivity

2. EMERGING TRENDS AND LOSS DRIVERS

Evolving regulation and cyber disclosure rules

Businesses large and small are operating in an evolving regulatory and legal environment, in which data privacy and cyber regulation lags behind developments in technology and business practices.

Organizations are finding new use cases for artificial intelligence (AI) and biometric data, yet regulations and legal interpretations are still a work in progress.

"We are currently in a holding pattern in terms of what the future holds for the application of regulation in areas like privacy, biometrics, and cyber incident disclosure rules. There is broad cover for breaches of data privacy regulation in the market, so it is important to keep on top of changes in regulation and as legal precedents are established by the courts," explains **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

At the start of 2023, California, Colorado, Virginia, Utah, and Connecticut were the only states with comprehensive data privacy laws[16] in the US, but that doubled last year, with Iowa, Indiana, Montana, Tennessee, Texas, Oregon, Delaware and Florida signing their own. While these laws shared the common goal of protecting consumers, they differed in scope, requirements, and definitions.

Since its enactment in 2008, Illinois' Biometric Information Privacy Act (BIPA) has provided a rich seam of litigation. There were hundreds of new cases filed in 2023, and several rulings that expanded the scope of liability[17] for companies handling biometric data in the state. A 2023 BIPA decision in the Illinois Supreme Court ruled that a BIPA violation – subject to a US$1,000 fine – should accrue each and every time an organization collects or discloses biometric information without consent. On August 5, 2024, Governor J.B. Pritzker signed into law a bill that overturned this 2023 decision, now holding that companies can be held liable for only one single violation per person[18].

tippapatt / Adobe Stock

In Europe, the General Data Protection Regulation (GDPR) has provided a harmonized and comprehensive framework for data protection and privacy since 2018. But while the law is relatively prescriptive, courts continue to clarify aspects. Last year, the EU's highest court – the Court of Justice – issued two separate landmark rulings on the interpretation of damages and regulatory fines for data breaches. In addition, the EU's upcoming AI Act in 2024 is intended to complement the GDPR and plug gaps in data privacy requirements for AI systems.

Meanwhile, the Asia Pacific region is also seeing significant developments in data privacy laws as countries strive to align with global standards, with Japan, South Korea, India, and China among those countries strengthening their frameworks.

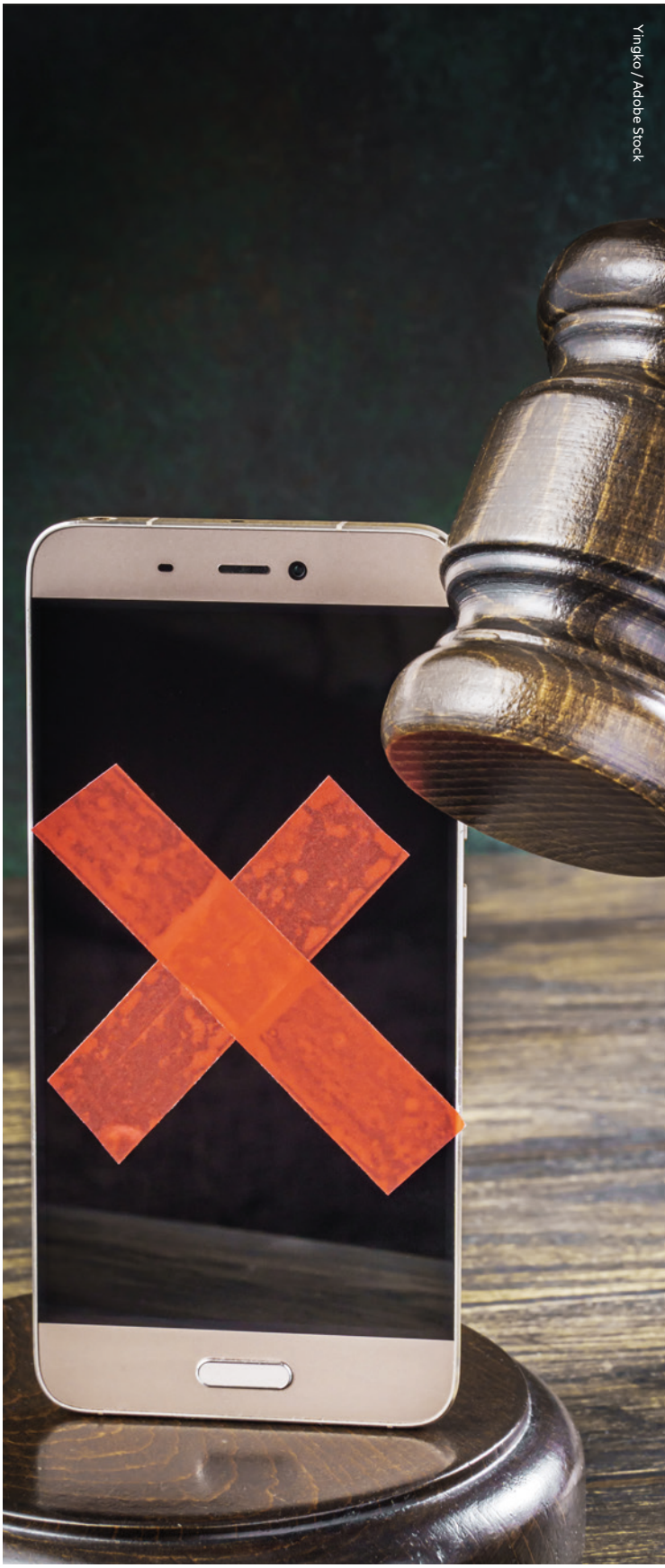
Another developing area of regulation is cyber security and reporting requirements, such as the US Securities and Exchange Commission's (SEC) new rules on cyber security risk management, governance, and incident disclosure for public companies. The rules require publicly traded companies to disclose cyber security incidents within four business days, in addition to annual reporting on their cyber security risk management and governance procedures.

While the SEC rules should encourage companies to take cyber security seriously, its implementation is not without challenges, according to **Marisa Anthony, Senior Complex Claims Analyst, Allianz Commercial.**

"Stringent SEC requirements to disclose material cyber security incidents within four days could lead to premature reporting, as it will be almost impossible for a company to know what it is dealing with within this timeframe. The risk is that we will see over-reporting of cyber incidents that lead to negative publicity, media attention and potential class actions," says **Anthony.**

The new cyber disclosure rules are also open to interpretation, for example, they do not define what constitutes a 'material' cyber security incident.

"It will be a challenge for some companies to disclose material deficiencies without communicating to threat actors the 'holes in the castle wall'," says **Stephens.** *"So far, organizations that have experienced breaches are erring on the side of caution, and setting a low bar for what is 'material'."*


Yingko / Adobe Stock

2. EMERGING TRENDS AND LOSS DRIVERS

A wave of class action litigation

Data breach class actions have surged in the US, creating additional costs and reputational risks for both US and multinational companies. And while Europe continues to favor strict regulation over the courts, collective data breach actions are on the horizon.

Almost every major data breach in the US is now accompanied by a wave of negative publicity and class action litigation. And while data breach litigation does not result in the nuclear verdicts seen in personal injury litigation, it has attracted the attention of plaintiff law firms and litigation funders. And with large numbers of claimants, there are incentives for parties on both sides to settle.

"In many jurisdictions, data breaches must be notified and communicated as soon as possible, which brings an incident to the attention of plaintiff attorneys, who are quick to raise enquiries and launch a class action. It's a double-edged sword. We need companies to be able to talk about what has happened, but transparency can also lead to explosive media attention and litigation," says **Marisa Anthony, Senior Complex Claims Analyst, Allianz Commercial.**

Data breaches have emerged as one of the fastest growing areas of US class action litigation. The number of data breach class actions in the US increased dramatically in volume in 2023 compared with 2022. There were 1,320 data breach class actions filed in the US last year, more than double the 604 filed in 2022 and the 310 in 2021, according to law firm Duane Morris[19]. The top 10 data breach class action settlements last year totaled $516mn, a significant increase over the $350mn recorded in 2022.

Large data breach events can evolve into hyper litigation, with one event triggering a slew of class actions. In October last year, more than 240 lawsuits[20] related to the 2023 MOVEit data breach were consolidated into a single Multidistrict Litigation. Plaintiffs are suing both Progress Software and organizations that used MOVEit for alleged failures to take adequate steps to secure customer data, maintain basic network safeguards and comply with industry standards of data and security.

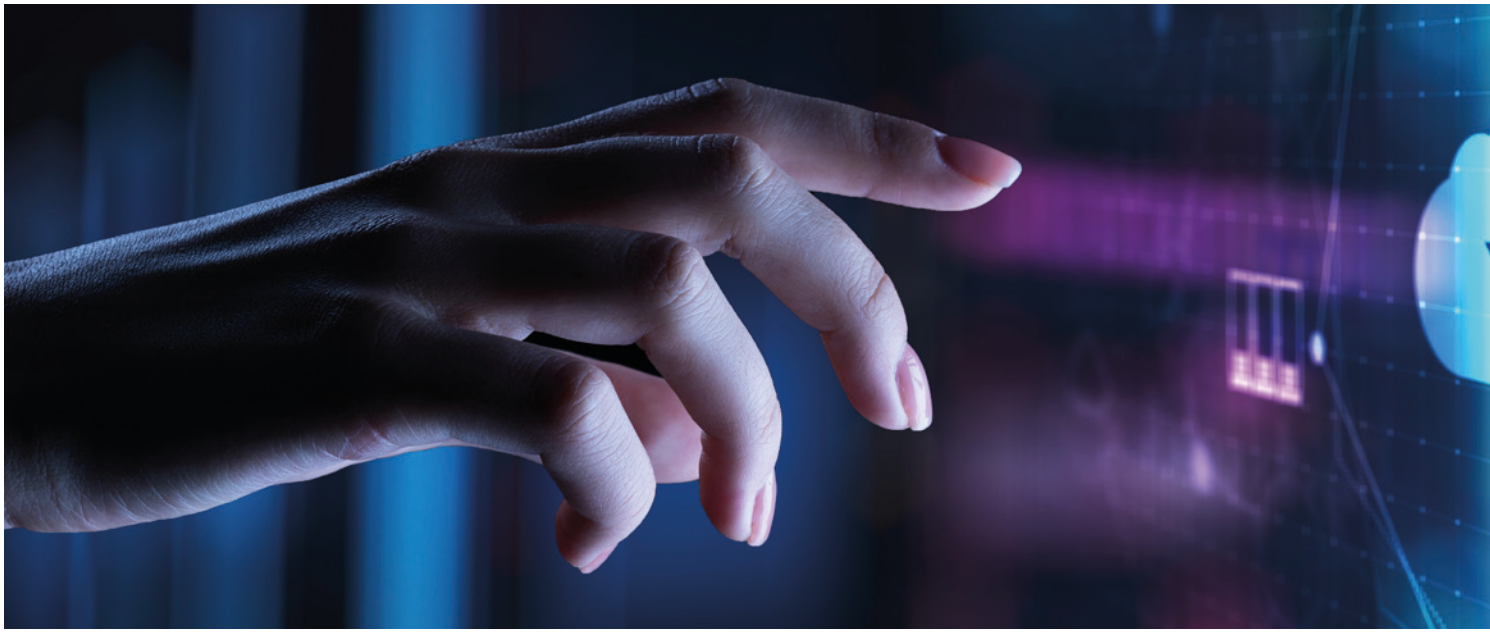
The rush to attribute blame and litigate takes the focus away from cyber criminals, according to **Anthony:** *"Data breach class actions only benefit plaintiff law firms and cyber criminals, focusing efforts on finger pointing, rather than the actions of threat actors, when it would be more beneficial to collaborate and communicate with each other in order to address these matters collectively.*

"Class actions are expensive, and ultimately that cost is born by consumers through the cost of products and services."

The risk of data breach litigation is also growing in Europe. Heightened awareness of data protection rights, a rise in the availability of third-party litigation funding, and a more consumer friendly litigation environment could make mass data privacy claims a reality, albeit not on the same scale as the US.

"While there have been collective data privacy actions in Europe, the courts have been reluctant to grant compensation for non-financial damages, such as emotional distress. It is harder to bring a successful class action in Europe for data privacy breaches, but it is an evolving situation and there may be a shift in favor of consumers in the future," says **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**

The EU's Collective Redress Directive provides consumer protection organizations and certain data privacy non-governmental organizations with a mechanism for collective redress of General Data Protection Regulation (GDPR) damage claims. Last year a consumer association in the Netherlands revealed that it was preparing a mass claim against Google[21] with the support of a large US plaintiff law firm.



2. EMERGING TRENDS AND LOSS DRIVERS

Connectivity fuels mass data breaches

The growing commercial value of personal data and exchange of data between organizations creates opportunities for criminals, eager to exploit lax cyber security and vulnerable personal data.

The collection, storage and sharing of personal data is increasingly central to the day-to-day activities of businesses, governments, and individuals. Around 200 zettabytes of data are expected to be stored by 2025, of which 50% is likely to be housed in the cloud, according to Cybersecurity Ventures[22]. The number of internet users is predicted to reach 7.5 billion by 2030 (90% of the projected world population over the age of six).

"Year on year, more and more personal data is being collected, stored and shared and this increases the attack surface and creates more opportunities for attackers, as well as the opportunities for errors," says **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.** *"Biometrics is a hot topic, with regulatory developments and litigation in the US. Biometric data is also more personal and sensitive: While it is possible to change a compromised password, a person's fingerprint, voice, or image cannot be changed.*

"At the same time, we are seeing the expansion of stricter data privacy regulation around the world, which enables attackers to increase the pressure on companies."

Companies are also becoming more and more connected, exchanging data and services within a complex web of customers, suppliers, and partners. Cyber criminals are now targeting these digital supply chains to exfiltrate personal data en masse.

A cyber attack against customers of cloud database hosting service provider Snowflake is on track to become one of the largest data breaches ever. In May, events company Ticketmaster suffered a data breach in which the personal data of 560 million customers worldwide[23] were reported stolen by a group known as ShinyHunters. It later transpired that more than 165 other companies had potentially been exposed, with it also being reported[24] that victims did not have multifactor authentication (MFA) in place.

The number of US companies impacted by supply chain attacks more than tripled in Q1 2024 compared to the same period in 2023, according to the Identify Theft Resource Center (ITRC)[25]. Cloud data environments are also popular targets of cyber attacks. Around 40% of breaches spanned multiple environments, such as public and private clouds. Data breaches solely involving public clouds were the most expensive type, US$5.17mn on average, up 13% in the year leading up to February 2024, according to IBM[26].

Mass data exfiltration attacks are a consequence of the growing interdependencies between organizations, which are increasingly reliant on third parties for software and services, according to **Marisa Anthony, Senior Complex Claims Analyst, Allianz Commercial.**

"Incidents like MOVEit and Change Healthcare are the poster children of digital interdependency and connectivity. They are a reminder that everyone in the data value chain plays a part, and is responsible for maintaining good cyber security, whether that be keeping passwords secure or using multifactor authentication. In too many cases a lack of basic cyber hygiene has led to a major data breach," says **Anthony.**

Around 40%

of data breaches spanned multiple environments, such as public and private clouds

Data breaches solely involving public clouds were the most expensive type, costing, on average

US$5.17mn

"You can't blindly trust in the cyber security of vendors and third-party suppliers. Vendor oversight is challenging – it is difficult to really go deep into the supply chain – but ultimately your firm will be responsible for protecting customers' and employees' personal data."

While outsourcing and cloud services are not new, interconnectivity is now on a mass scale, according to **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

"The network of risk is expanding. In the past, insureds' digital operations were largely isolated, but now they are more interconnected, with multiple organizations working together, sharing, and using information. This expands the network footprint, creating more points of entry," says **Stephens.**

These interdependencies are a challenge for insurers, who could face multiple claims linked to a single cyber attack, vulnerability, or an outage at a critical service provider. Some sectors and services are concentrated on a small number of suppliers, creating large potential accumulations of exposure for insurers. Examples of incidents in 2024 alone include: CDK Global, a software firm serving car dealerships across the US which was hit by a ransomware attack; hackers stealing data from Change Healthcare which processes US medical claims; and, of course, the software update from CrowdStrike, which caused a massive IT outage, crashing millions of Windows systems and disrupting critical services and business operations around the world *(see box)*.

"With today's complex web of interconnectivity and reliance on service providers, modeling has become critical. When we assess our customers' risks, we are not just modeling to the insured's exposure. We are modeling to the extended network, their cloud, software, and digital service providers," says **Stephens.**

"We are now at an inflection point in cyber. You really need to get the modeling right because the threat is advancing so quickly – and now we have artificial intelligence to add to the challenge."

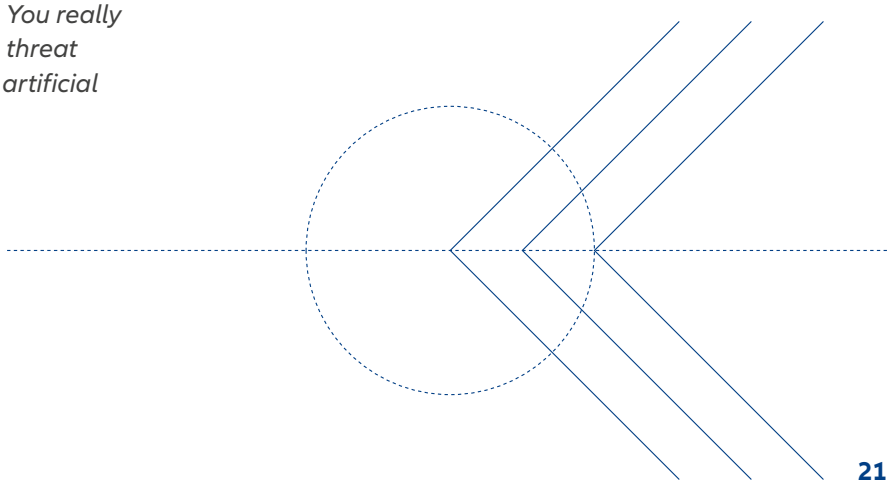
Cyber resilience after CrowdStrike

During July 2024, many critical services and businesses around the world experienced a widespread technical outage after cyber security firm CrowdStrike[27] pushed out a routine software update that inadvertently crashed Windows systems. It is believed to be one of the largest IT outages in history, if not the largest.

The incident once again underscores the critical importance of securing supply chains, given their global interconnectivity can cause significant ripple effects.

"Although not always feasible, the diversification of core business activities and services is a great approach to reduce the impact of impromptu incidents," says **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial.** *"Preparedness for worst-case scenarios in terms of planning and practicing resilience drills and updating the incident response strategy are crucial. This incident highlights the necessity of having rapid incident response, robust disaster recovery plans and business continuity strategies.*

"Finally, it also underpinned that clear communication with the stakeholders during and after an incident is critical. Maintaining the lines of communication throughout the incident handling, and being transparent about the steps that are being taken to resolve the issue, fosters trust."



2. EMERGING TRENDS AND LOSS DRIVERS

AI to power future data privacy breaches

Artificial intelligence (AI) has the potential to turbocharge data breach exposures in future, fueling greater processing of personal data and as a powerful tool for threat actors.

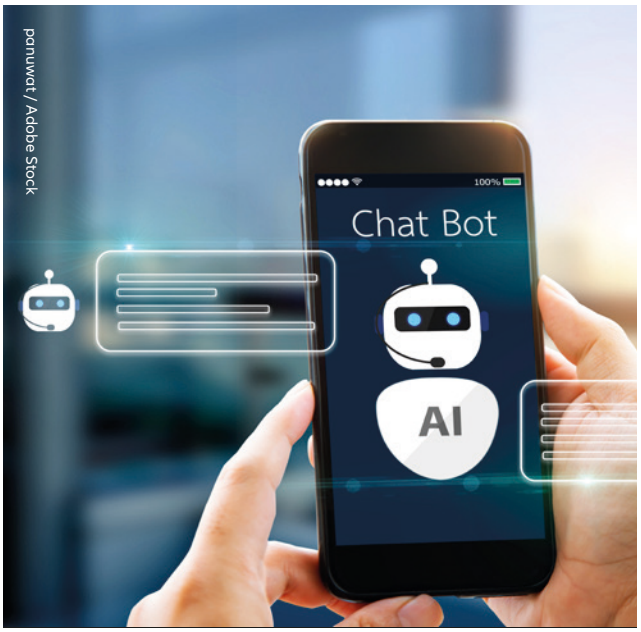
The use of AI by businesses and public bodies is growing day by day, with applications in technology, media, healthcare, finance, retail, and logistics. In a recent McKinsey[28] survey, almost two thirds (65%) of organizations say they regularly use AI, nearly double the number from a year ago.

AI relies on the collection and processing of vast amounts of data, including personal, health and biometric information, for training AI models and making accurate predictions or recommendations. AI is also integral to some technologies, such as personal assistants (like) Alexa and Siri, for surveillance, tracking and monitoring systems, chatbots and driverless vehicles.

Given the volumes of personal data involved, and its black-box nature, AI can create potential privacy and security risks if not properly managed. With so much data being collected and processed, there is a risk that it could fall into the wrong hands, either through hacking or other security breaches. There are also concerns around potential breaches of privacy laws, such as whether organizations have proper consent to process data through AI. In February 2024, Air Canada was ordered to pay compensation to a customer that had relied on incorrect information provided by one of the airline's chatbots[29].

AI technology and use cases are also developing in an evolving regulatory and legal environment. AI regulation is tightening – the EU is establishing a common framework for regulation under the AI Act and complementary AI Liability Directive – which will increase complexity and raise the compliance bar for companies.

"It will take years until AI regulation is well developed. Until then, organizations face a phase of elevated uncertainty, and the risk of data privacy related losses will be above normal levels," says **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**



Different AI applications, however, carry varying degrees of risk. AI use cases that focus on consumer products and services – such as chatbots or AI-generated content – are likely to bring a higher degree of data privacy risk than administrative AI applications, such as automation of internal processes.

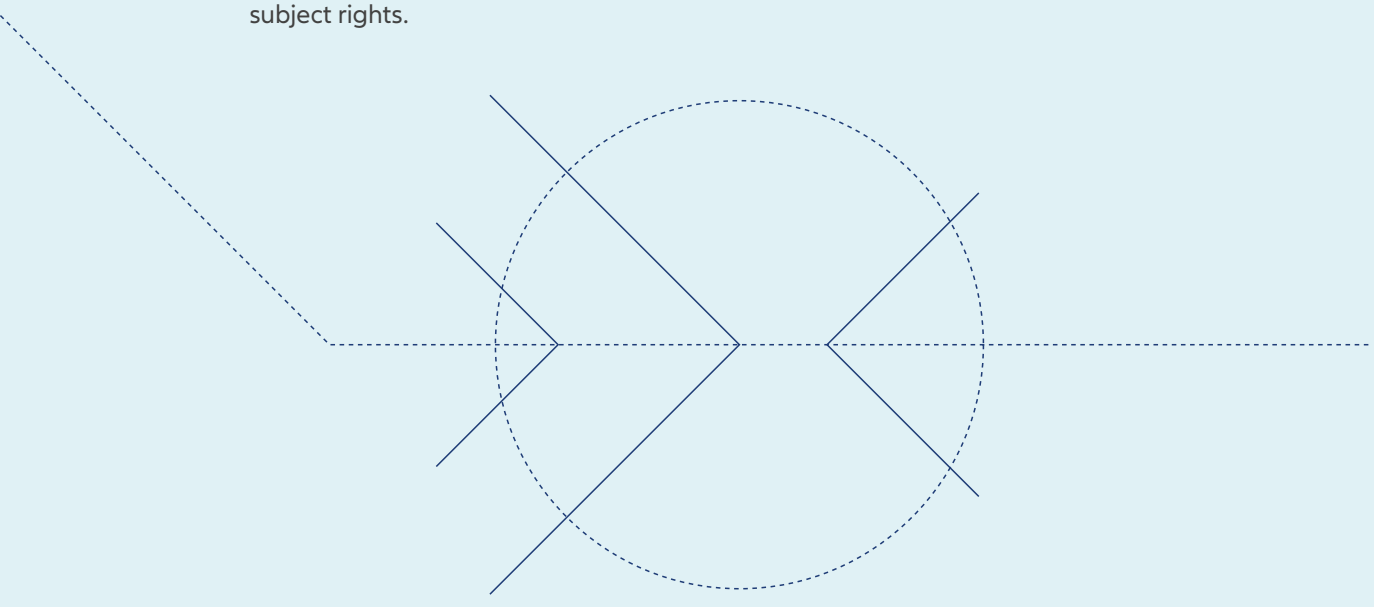
"Using AI and personal data for your own business purposes is one thing, but once you turn it into a product or service, the privacy element becomes more challenging," says **Tresa Stephens, Head of Cyber, North America, Allianz Commercial.**

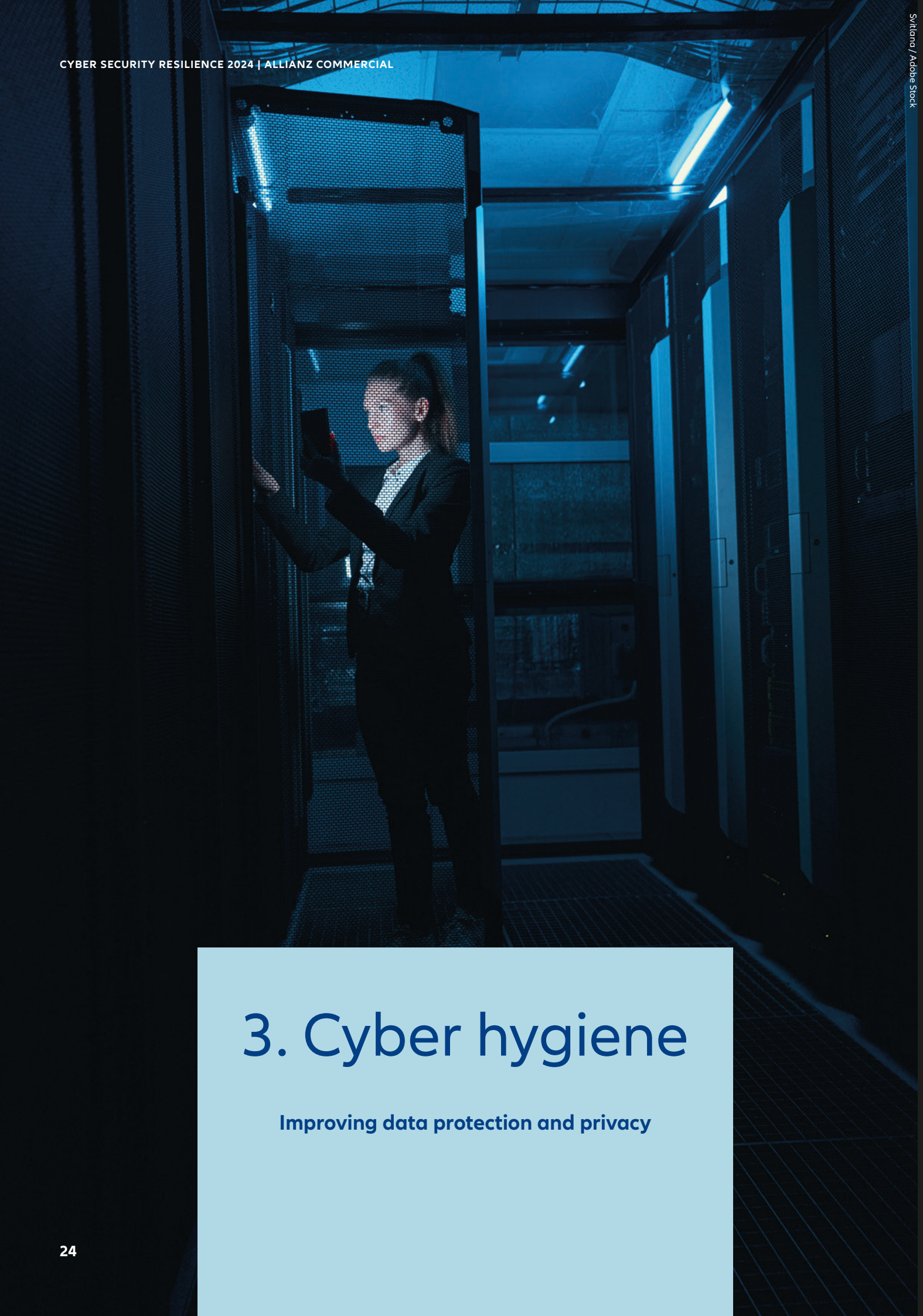
"AI is an interesting area to watch for cyber insurance. More and more customers are inquiring about AI coverage. At present, cyber insurance generally has broad definitions and does not exclude, or explicitly include. But insurance will need to adapt and respond to advances in technology like AI. We must keep pace with it in terms of underwriting and coverage."

AI: harness the benefits, mitigate the breaches

Companies should consider the following factors to harness the benefits of artificial intelligence (AI) while mitigating the risks of potential breaches, according to **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial.**

- **Data governance:** Establishing robust data governance practices is crucial for ensuring that data is collected, stored, and processed in compliance with privacy regulations and internal policies. This includes defining data ownership, implementing data classification, and setting clear guidelines for data access and usage.
- **Security measures:** Implementing strong security measures, such as encryption, access controls, and regular security audits, is essential for protecting the data used by AI systems. This helps prevent unauthorized access and data breaches that could compromise individuals' privacy.
- **Privacy regulations compliance**: Companies must ensure that their use of AI aligns with relevant privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe or the California Consumer Privacy Act (CCPA) in the US. This includes obtaining explicit consent for data collection and processing, providing individuals with control over their data, and honoring data subject rights.
- **Ethical AI practices:** Embracing ethical AI practices involves considering the potential impact of AI on individuals' privacy and well-being. This includes addressing bias and fairness in AI algorithms, being transparent about data usage, and incorporating privacy considerations into the design and deployment of AI systems.
- **Privacy-preserving AI techniques:** Companies can explore privacy-preserving AI techniques, such as federated learning and differential privacy, to minimize the risk of data privacy breaches. These techniques allow AI models to be trained on decentralized data sources without directly accessing sensitive information, thus reducing privacy concerns.





Svitlana / Adobe Stock

3. Cyber hygiene

Improving data protection and privacy

3. CYBER HYGIENE

Common mistakes

Despite a general trend for increased investment in cyber security in recent years, many data breaches, including some of the largest over the past 18 months, are the result of weak cyber security within organizations and/or their supply chains.

The compromise of cloud-based data storage and analytics platform Snowflake[30] in June 2024 for example, for example, highlights common security vulnerabilities, namely weak access controls and issues with cloud and third-party suppliers. According to cyber security firm Mandiant[31], which carried out an investigation into the attack, the hackers used compromised credentials stolen by infostealer malware to access companies. The investigation also revealed that some credentials were stolen from third party contractors' systems, which in a few instances had also been used for personal activities like gaming. Compromised accounts did not always have multifactor authentication enabled.

Phishing and stolen or compromised credentials were the two most common attack vectors in 2023, and were responsible for 16% and 15% of breaches, respectively, according to IBM[32]. Cloud misconfiguration was identified as the initial vector for 11% of attacks, followed by business email compromise (BEC) at 9%.

Phishing attacks have been a persistent threat since the early days of email and are an attractive method for cyber criminals to initiate attacks or carry out fraud, tricking users into downloading malware, revealing passwords, or transferring funds, according to **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial.**

"Phishing and BEC attacks, which are often the precursor for a data breach or ransomware attack, remain one of the top cyber risk concerns for businesses. These attacks have been on the rise and continue to evolve, becoming increasingly more sophisticated and targeted," says **Baviskar.**

Cyber security misconfiguration, caused by mistakes or oversights in the setup of applications, is another common cause of data breach. Hackers proactively search for unprotected databases and misconfigured systems, for example, the use of default configurations and passwords, improper access controls, unpatched systems and misconfigured network devices and Application Programming Interfaces (APIs), warns **Baviskar.**

"It's not a matter of what you spend on cyber security, at the end of the day, it is how a system is configured or hardened. With the complexity and scale of IT, cloud, and large numbers of devices and entry points, misconfiguration and a lack of visibility into the IT perimeter can be a real challenge for large companies. If it's not hardened, or you do not know about it, it's unprotected," adds **Alex Pabst, Deputy Group Chief Information Security Officer, Allianz.**

Similarly, digital transformation projects and mergers and acquisitions (M&As) can also open the door to hackers, as complex changes can have unforeseen consequences, or lead to security oversights. *"For example, in the haste to push through their digital transformation or transition to the cloud, organizations do not always put the right cyber security controls, policies, and processes in place. M&As can also lead to misconfiguration and the creation of cyber security loopholes,"* says **Baviskar.**

The most common attack vectors in 2023

Source: IBM, Cost of a Data Breach Report 2023


DC Studio / Adobe Stock

3. CYBER HYGIENE

Doubling down on cyber security

Data breach risks are best mitigated through good cyber hygiene, including strong access controls, database segregation, backups, patching and training.

Further measures that help protect personal data include breach and attack simulation tools, which can identify gaps and weaknesses in cyber security, breach response and crisis management.

"The best way to protect against data breaches is to ensure you have a good level of cyber hygiene. Be vigilant and understand your risks before they become an incident. Data loss prevention technology is also a good way to deepen security and flag up potential issues," says **Marek Stanislawski, Global Cyber Underwriting Lead, Allianz Commercial.**

Vendor cyber security oversight, including regular audits, is an increasingly important aspect of good cyber security, and is an area where many companies need to do more, according to **Michael Daum, Global Head of Cyber Claims, Allianz Commercial,** who recommends that companies should try to mirror their own information security standards into vendor contracts to ensure the same level of security across all parties is involved.

Early detection and response capabilities are also key. Around two thirds (67%) of breaches are reported by a third party or by the attackers themselves, according to IBM[33]. Cyber breaches that are not detected and contained early can be as much as 1,000 times more expensive than those that are, Allianz Commercial analysis shows. Early detection and response can stop a €20,000 loss turning into a €20mn one.

"It is a universal concept in cyber: The quicker you detect and react to an incident, the less the economic and reputational impact," says **Stanislawski.**

Companies are investing in early detection and response tools and capabilities, which are improving with artificial intelligence (AI), according to **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial:** *"AI is becoming an essential tool in the fight against cyber attacks. For example, it can quickly identify a security breach and automatically isolate systems and databases. It can also significantly reduce the cost and life cycle of a data breach claim by automating and speeding up tasks, such as forensics, assessing potentially compromised personal data and notification."*

Organizations that deployed cyber security AI and automation reduced the cost of a data breach by around US$2mn on average, compared with organizations that do not, according to IBM[34].

"If you are not using AI for cyber security then you are now lagging behind," says **Baviskar.** *"Threat actors are using AI for more effective social engineering, to identify vulnerabilities and to automate attacks. So, if your organization is not investing in AI cyber security and response, then you will be more vulnerable."*

3. CYBER HYGIENE

Data privacy resilience

In addition to cyber security and data breach response capabilities, organizations must also focus more attention on preventing and mitigating data privacy breaches.

Data breach and privacy risks can be mitigated in large part by good data governance and housekeeping, explains **Marisa Anthony, Senior Complex Claims Analyst, Allianz Commercial.**

"Be mindful of what data you are collecting. Only collect and store personal data that is needed for business purposes, not what you think you need, and have a process in place to dispose of that data when you no longer need it. This is a simple measure companies – large and small – can take that is low cost and doable today," says **Anthony.**

Organizations need to adopt a risk-based approach to protecting data, advises **Rishi Baviskar, Global Head of Cyber Risk Consulting, Allianz Commercial:** *"Limit access to those people with a business requirement, and use encryption and monitoring for third parties. Data leak prevention tools and user behavior analytics can also help flag up any unusual access or movement of data."*

More sensitive private data, like biometric, genetic or health data, should be held to the highest level of cyber security, according to **Baviskar.** Organizations that collect biometric data should hold it locally, keep it segregated and encrypted, with tightly controlled access rights, and not shared with third parties.

Companies should also make sure that their terms of service are clear and understandable, according to **Anthony:** *"Often, privacy claims come back to the terms of service: Does the company's use of data match what was marketed and what the consumer agreed to?*

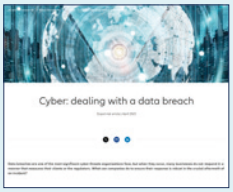
"With advancements in technology and developments in regulation, it's hard to see a time when data privacy will not be a dynamic in society. So how should an organization position itself? It comes back to being transparent, being clear in communication about what data you are capturing, explaining why and what you are doing with it."

> Be mindful of what data you are collecting. Only collect and store personal data that is needed for business purposes

Allianz Commercial risk assessment already includes data processing elements today, but going forward the scope will increase further, with meaningful advice offered to insureds on how to best avoid data breach losses.

"With the growing relevance of AI, risks around consent and unauthorized use of data are increasing. Companies need to make sure that data privacy governance is embedded going forward," says **Michael Daum, Global Head of Cyber Claims, Allianz Commercial.**

"By working with our customers, we have been successful in improving the level of cyber security and response, and we now see the positive results in the stabilization of ransomware claims. But as an industry, we need to focus on the data privacy side of cyber insurance and risk, supporting businesses and helping them be better prepared for the data privacy issues that are coming down the line."



Data breaches are one of the most significant cyber threats organizations face, but when they occur, many businesses do not respond in a manner that reassures their clients or the regulators. What can companies do to ensure their response is robust in the crucial aftermath of an incident?

Find out more Cyber: dealing with a data breach | AGCS (allianz.com)

References

1 Cybersecurity and Infrastructure Security Agency, The attack on Colonial Pipeline: What we've learned and what we've done over the past two years, May 7, 2023

2 Europol, Law enforcement disrupt world's biggest ransomware operation, February 20, 2024

3 Reuters, UnitedHealth to take up to $1.6 billion hit this year from Change hack, April 16, 2024

4 Financial Times, NHS England probes data leak after cyber attack on Synnovis blood-test provider, June 21, 2024

5 Chainalysis, Ransomware payments exceed $1 billion in 2023, hitting record high after 2022 decline, February 7, 2024

6 Sophos, Ransomware payments increase 500% in the last year, finds Sophos State of Ransomware report, April 30, 2024

7 CNN, 37 million T-Mobile customers were hacked, January 20, 2023

8 Reuters, Casino giant MGM expects $100 million hit from hack that led to data breach, October 6, 2023

9 UnitedHealthGroup, UnitedHealth Group updates on Change Healthcare cyberattack, April 22, 2024

10 Reuters, UnitedHealth issues breach notification on Change Healthcare hack, June 20, 2024

11 The HIPPA Journal, Change Healthcare Reports Ransomware Data Breach to HHS, July 31, 2024

12 Identity Theft Resource Center, Identity Theft Resource Center 2023 Annual Data Breach Report reveals record number of compromises; 72 percent increase over previous high, January 25, 2024

13 IBM, Cost of a Data Breach Report 2024

14 Bloomberg Law, Facebook 'pixel' video-sharing lawsuit advances against Pearson, March 4, 2024

15 Variety, Amazon agrees to pay $25 million fine to settle allegations Alexa voice assistant violated children's privacy law, July 20, 2023

16 WilmerHale, Year in review: The top 10 US data privacy developments From 2023, January 5, 2024

17 WilmerHale, Year In review: 2023 BIPA litigation takeaways, January 31, 2024

18 Reuters, Illinois governor approves business-friendly overhaul of biometric privacy law, August 5, 2024

19 Duane Morris, Duane Morris LLP publishes Its Duane Morris Data Breach Class Action Review - 2024, February 22, 2024

20 Clyde & Co, Understanding the MOVEit data breach: Navigating long tail liability risks in the wake of cyber incidents, April 30, 2024

21 Reuters, Dutch groups sue Google over alleged privacy violations, September 12, 2023

22 Cybersecurity Ventures, 2024 Data Attack Surface Report

23 BBC, Ticketmaster confirms hack which could affect 560m, June 2, 2024

24 The Register, Snowflake customers not using MFA are not unique – over 165 of them have been compromised, June 11 2024

25 Identify Theft Resource Center, Identity Theft Resource Center Q1 2024 Data Breach Analysis: Compromises Up 90 Percent Over Q1 2023, April 10, 2024

26 IBM, Cost Of a Data Breach Report 2024

27 The Guardian, The Microsoft/CrowdStrike outage shows the danger of monopolization, July 20, 2024

28 McKinsey, The state of AI in early 2024: Gen AI adoption spikes and starts to generate value, May 30, 2024

29 BBC, Airline held liable for its chatbot giving passenger bad advice - what this means for travellers, February 23, 2024

30 CNBC, AT&T's massive data breach deepens crisis for Snowflake seven weeks after hack was disclosed, July 12, 2024

31 Mandiant, UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion, June 10, 2024

32 IBM, Cost of a Data Breach Report 2024

33 IBM, Cost of a Data Breach Report 2023

34 IBM, Cost of a Data Breach Report 2024

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 information contact az.commercial.communications@allianz.com

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 2024