

Gorodenkoff / Shutterstock

ALLIANZ COMMERCIAL

Artificial intelligence: loss scenarios and claims developments

commercial.allianz.com

Contents

Page 3
Overview

Page 4
Executive summary

Page 9
Diverse scenarios: categorizing AI losses

Page 10
Emerging AI claims: early warning signals?

Page 10
Direct AI loss

Page 12
AI-related loss

Page 15
AI-accelerated loss

Page 16
AI dependency loss

Page 17
The tip of the iceberg: why the true level of AI losses may be underestimated

Page 19
Systemic risk potential: why small errors could translate into big losses

Page 20
Tracking AI losses: claims insights will be key to understanding AI risk

Page 22
Making AI a manageable business risk and a powerful mitigation tool

Page 24
AI as a risk mitigation tool

Page 25
References

Overview

- → Reported AI losses are just the "tip of the iceberg" and understate the true risk.
- → AI dependency and underdeveloped governance and controls are shaping the future risk landscape.
- → Rapid increase in AI-related incidents and litigation globally every year.
- → Focus needs to turn to understanding, detecting, monitoring and mitigating AI business risks.

Artificial intelligence (AI) is reshaping the business landscape at a pace and scale that few could have predicted. For our clients, the opportunities are immense – from enhanced efficiency and decision-making to entirely new products and services. But with this transformation comes a new generation of risk that demands our full attention.

AI has risen to become the second most concerning business peril in our annual **Allianz Risk Barometer** – the largest year-on-year increase of any risk category. The rapid pace of change and uncertainty of outcomes poses a significant challenge at a time when appropriate governance frameworks and risk controls have yet to be fully developed.

The warning signs are clear. In a short time, dependencies on AI have grown rapidly, with many companies now reliant on the technology for critical operations. While confirmed losses remain modest in today's insurance claims data, they significantly understate the true exposure.

AI risk is already here and reshaping the risk profile of businesses in several distinct ways. AI can be a primary loss driver through system failure causing damage or injury. It can amplify existing risks, by accelerating and increasing the complexity of cyber-attacks. And it can trigger indirect, often unexpected consequences – such as shareholder claims alleging a company has misrepresented its AI capabilities.

At **Allianz Commercial**, we believe that understanding these emerging risks is essential – both for our clients and for our industry. This report sets out a framework for categorizing AI losses, examines claims trends we are tracking, and offers guidance on how businesses can build resilience in a rapidly evolving risk environment.

AI risk is a business, governance, and leadership challenge. The time to prepare is now.



Thomas Lillelund
CEO
Allianz Commercial

Executive summary

This report looks at how AI is changing the risk and claims landscape, why losses may lag behind adoption, and highlights what businesses can do to better understand, manage and transfer AI-related risks.

Artificial intelligence (AI) is transforming the global economy at unprecedented speed, moving rapidly from emerging technology to a boardroom priority. Adoption is accelerating and AI is already embedded in many business processes – from production planning to autonomous systems to pricing models.

In just one year, AI has also surged from #10 to #2 in the **Allianz Risk Barometer** – the largest year-on-year rise of any category in the annual business survey. This dramatic shift reflects growing awareness among businesses and insurers that AI is not simply a technology issue but a fundamental business, governance, and leadership challenge.

Yet despite this heightened concern, confirmed AI-related insurance losses remain relatively low. Based on current claims data, AI would not rank even in the top 20 loss drivers. However, AI losses are frequently underreported, difficult to quantify or attribute, or are recorded under traditional categories such as cyber, directors' and officers' (D&O) liability, or product liability insurance. The true risk exposure is substantial and growing fast. A sharp increase in losses may be anticipated.

AI incidents are accelerating

AI-related incidents and litigation have risen in recent years with corporates being sued for a wide range of AI-related issues, including intellectual property and copyright infringement, data privacy breaches, hallucinations (false information), discrimination, bias and environmental issues, as well as the overstatement or misrepresentation of companies' strategic capabilities.

Databases tracking AI incidents and lawsuits show they are significantly increasing every year. For example, the number of incidents rose from 179 in 2023 to 307 in 2024 and 453 in 2025, according to the MIT AI Risk Initiative *(as of October 7, 2026)* and this trajectory shows no sign of slowing.

At the same time, AI-related securities class action lawsuits in the US have followed a similar pattern, with 22 filings in 2026 alone (as of the end of August), compared to 16 in all of 2025.

Allianz Commercial is already tracking AI-related insurance claims with substantial values in the millions of euros. Examples of cases include accidents caused by alleged defective AI safety systems in vehicles and shareholder-filed securities litigation alleging misleading AI-related disclosures and omissions by company executives. Such cases could easily result in total insurance industry losses in the region of US$100mn.



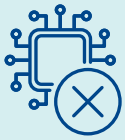
Summit Art Creations / Shutterstock

Four categories of AI loss

AI risk operates on several levels. One level lies within the technology itself. AI systems rarely express uncertainty. At the same time, they are highly sensitive to prompts and can exhibit confirmation bias, meaning small nudges can significantly influence outcomes. This can cause issues in negotiations, assessments or decision-support scenarios.

A second level arises from how AI is used in organizations. Experience is still limited across many functions. At the same time, competitive pressure to deploy AI quickly is enormous. Even when companies act responsibly, the probabilistic nature of AI means that mistakes could still happen. A further level consists of indirect risks. In many cases, AI is not the direct cause of damage, but a force multiplier. For risk management purposes, it is therefore crucial to interpret AI-related harm broadly.

The report introduces a practical framework for understanding how AI can generate losses and claims, organized into four main categories:



Direct AI loss
The AI system itself is the primary cause of harm through an incorrect action, decision, recommendation or output.



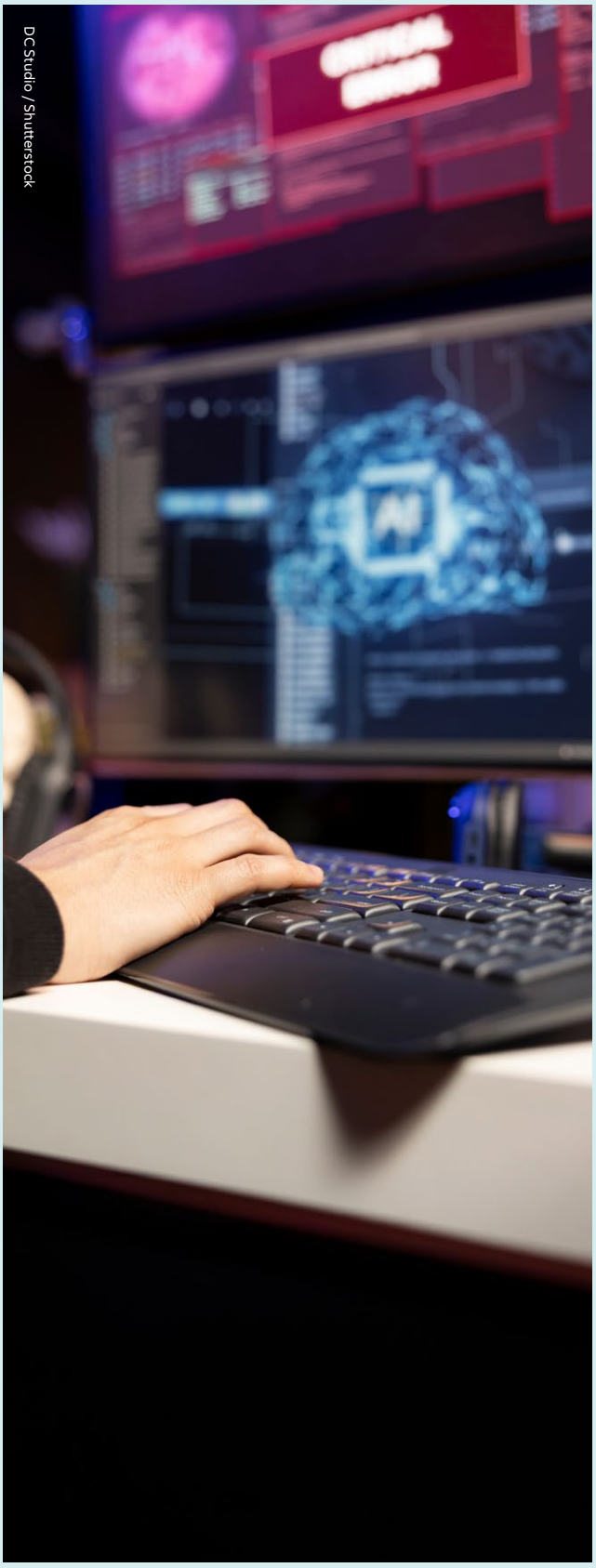
AI-related loss
AI is a material factor in the loss event, but the loss arises from surrounding business, governance, legal, reputational, or third-party AI issues rather than the insured's own AI system.



AI-accelerated loss
AI does not cause the loss directly but enables, scales, or accelerates malicious activity.



AI-dependency loss
AI does not cause the initial event, but heavy reliance on AI-driven processes and insufficient fallback capabilities significantly increase the magnitude, duration, or cost of the loss.

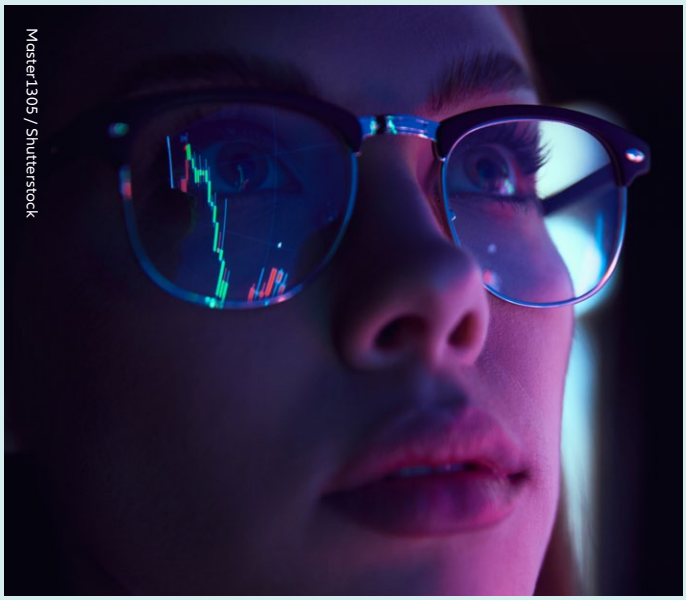

DC Studio / Shutterstock

Direct AI loss cases

Intellectual property (IP) disputes have been at the forefront of AI litigation and are a clear example of direct AI claims. For example, AI-driven losses are emerging around the use of protected content in large language model (LLM) training, alleged copying or replication of copyrighted material, and uncertainty around ownership of AI-generated outputs. As of midway through 2026, there were well over 100 IP lawsuits filed against AI-developers by artists, entertainment and media companies. Another vein of AI-related litigation has arisen from prejudiced training data or algorithms which can result in AI tools that produce discriminatory outcomes.

Corporates and professional services firms can also face liability claims where they use AI-tools to provide services or advice to clients but fail to properly validate output. So-called AI hallucinations have been particularly notable in the legal sector. Law firms have faced regulatory and court sanctions when using AI to draft court documents that included fictitious or inaccurate citations and quotations.

In addition, an increasing number of businesses and consumers are seeking advice from general-purpose AI, such as investment, financial, legal or travel advice. Direct financial losses can be incurred due to reliance on incorrect advice from chatbots.



Master1305 / Shutterstock

AI-related loss cases

D&O liability analysis

One of the most visible areas for AI-related losses is currently directors and officers (D&O) insurance, where developments such as AI washing – the overstatement or misrepresentation of AI capabilities – is leading to litigation and the notification of insurance claims. Recent years have seen notifications in the US under D&O policies, mostly from securities litigation for AI-washing claims, but also for failure to anticipate and disclose the adverse impact of AI or for making misleading statements about the positive impact of AI on profitability.

Allianz Commercial, together with **The D&O Diary,** recently conducted a survey of 250 respondents from 25 countries on AI-related topics in the D&O space, providing a detailed picture of the sector's view:

86% of respondents believe AI-related claims will significantly impact the D&O insurance landscape.

92% agree that poor AI governance increases the likelihood of D&O claims.

AI washing, data privacy (each ranked first by 28% of respondents) and intellectual property disputes (20%) are regarded as the most significant AI exposures in the context of D&O insurance.

Other examples

Technology companies have also faced litigation relating to the alleged addictive nature of social media. While not the direct cause, AI is perceived to enable design features that drive compulsive use, especially for vulnerable users.

Sustainability concerns surrounding AI are another emerging area for litigation. Analysis of around 3,600 climate-related lawsuits filed since 2015 found a growing number of cases challenging the energy sources, water consumption and air pollution of data centers, according to the London School of Economics (LSE).

AI-accelerated loss cases

AI is already a significant driver for rising cyber crime, with the technology widely used to create more convincing phishing attacks and deep fakes, as well as to develop malware, carry out reconnaissance and automate cyber-attacks.

AI is also widely believed to be behind an uptick in fraud-related claims. AI-related cyber crime is estimated to have cost US citizens close to $900mn in 2025 as AI-enabled content becomes increasingly difficult to detect and easier to make. Technology has long been a driver for escalating crime and fraud claims, but AI represents a significant step forward that will further drive fraud losses.

AI-dependency loss cases

Companies can also face challenges from an event which is not caused by AI but given their heavy reliance on AI-driven processes and insufficient fallback capabilities, the magnitude, duration, or cost of the loss can be significantly increased. For example, a large retailer was impacted by a cyber outage at a critical third-party technology provider. When the service went down, AI-enabled processes could not be executed at scale, forcing distribution centers to revert to paper-based processes. This resulted in incorrect product selection, inventory imbalances, delays, and significant operational inefficiencies and financial losses. In another incident, a large hospitality / leisure company suffered a cyber-attack, rendering critical digital systems inoperable. The company lacked the localized infrastructure or agile protocols required to bypass algorithmic networks meaning employees were forced to handle millions of dollars in transactions using manual pen and paper, resulting in massive operational friction and millions in lost revenue each day.



A unique risk profile

AI carries a unique systemic risk profile. Unlike previous technology revolutions, AI is being adopted simultaneously across virtually all industries and geographies. Many AI systems share common foundations – the same large language models, training data, cloud infrastructure, and data centers. This concentration means that a single flaw, outage, or vulnerability could cascade across sectors and borders. AI also operates probabilistically, meaning errors are inevitable even in well-designed systems. When deployed at scale, even a small error rate can generate a massive number of incidents simultaneously.

AI as a risk management tool

While AI introduces new exposures, it can simultaneously reduce the frequency and severity of existing business risks when deployed with appropriate governance, controls, and human oversight. Many practical examples already demonstrate AI's risk reduction potential. In financial services, AI-driven fraud detection systems identify suspicious transactions in real time, helping prevent payment fraud, account takeovers, and money laundering. In cyber security, AI is increasingly used to detect abnormal network activity, identify compromised credentials, and uncover emerging attack patterns before significant damage occurs.

Manufacturing companies use predictive maintenance models to detect early signs of equipment failure. Supply chain organizations employ AI to monitor suppliers and logistics networks, enabling earlier identification of disruption risks and more resilient business continuity planning. AI is also enhancing regulatory compliance by continuously monitoring large volumes of transactions, communications, and records, helping organizations identify potential compliance breaches at an earlier stage and reducing the likelihood of regulatory action.

Organizations using AI-driven prevention and detection tools have materially lower breach and business interruption costs. The cost of a cyber breach that progresses to data theft and encryption can be 1,000 times higher than an incident that is detected and contained early.



MMD Creative / Shutterstock

The bottom line

For business leaders, the most important shift is to treat AI risk not only as an IT issue, but as a business, governance, and leadership challenge. Organizations need to understand where AI is being used, how it affects decision-making and operations, and which exposures could emerge if tools fail, produce inaccurate outputs, or amplify existing risks. This requires deliberate decisions about which risks can be mitigated, which can be accepted, and which should be transferred. It also requires stronger visibility across functions, because AI risks can sit at the intersection of technology, legal, compliance, operations, product liability, cyber security, and board accountability.

The opportunities for AI remain significant. But realizing them sustainably depends on understanding the risk landscape early and proactively, before losses become more visible at scale.

Diverse scenarios: categorizing AI losses

Artificial intelligence (AI) risk manifests on multiple levels. However, losses can be broadly categorized into four distinct baskets.

AI risk starts with the technology itself. AI systems are sensitive to incomplete or inaccurate input data, and are prone to bias, discrimination and hallucinations (the making up of false information or fake facts). And when an AI system does not perform as intended it can result in financial loss, bodily injury, third party liability, property damage and business interruption.

AI can also act as a loss enabler. Rather than being the direct cause of damage, AI can act as a force multiplier that amplifies or crystallizes existing risks. It can increase the scale, sophistication and / or severity of familiar loss scenarios, such as ransomware attacks, or make it easier for consumers to seek compensation or bring legal action.

AI-related risks also arise from the way AI is implemented. In a competitive environment, businesses are under immense pressure to adopt the technology quickly, even when not fully understanding all of the potential risks. At the same time, regulatory, governance and risk management frameworks are lagging. So, a law firm using AI-tools to advise clients without adequate controls and validation could be open to legal action.

Finally, losses can arise from a dependency of AI systems or infrastructure, especially where manual back-up systems or workarounds are not available. Some AI-functions are not easily replicated by humans, while many organizations are becoming reliant on AI-systems for critical activities, such as supply chain management, logistics, resource allocation or revenue management. Extended, costly business interruption can be the consequence.

Potential loss categories

Loss type	Description	Example
Direct AI loss	The AI system itself is the primary cause of the loss through an incorrect action, decision, recommendation, or output.	AI-generated advice causes financial loss; AI-driven process failure causes operational disruption.
AI-related loss	AI is a material factor in the loss event, but the loss arises from surrounding business, governance, legal, reputational, or third-party AI issues rather than the insured's own AI system.	AI washing allegations in D&O; third-party AI failures in the supply chain.
AI-accelerated loss	AI is not the direct cause of the loss but is used to facilitate, scale, or accelerate malicious activity, increasing the frequency, severity, or sophistication of attacks.	AI-assisted phishing, deep fake fraud, and automated cyber-attacks; AI-assisted litigation – takes less knowledge and resources for lawsuits to be brought against companies.
AI-dependency loss	AI does not cause the initial event, but heavy reliance on AI-driven processes and insufficient fallback capabilities significantly increase the magnitude, duration, or cost of the loss.	AI outage leading to prolonged and more severe business interruption due to lack of manual alternative.

Emerging AI claims: early warning signals?

Artificial intelligence (AI)-related exposures and claims are quickly moving from theory to reality, emerging across multiple lines of insurance business simultaneously, but in very different forms.

Direct AI loss

A wide range of AI-related issues

Recent years have seen AI litigation expand as technology companies and corporates are sued for a wide range of AI-related issues, including intellectual property and copyright infringement, data privacy breaches, unauthorized or unlawful use, processing or retention of data, hallucinations (the making up of false information or fake facts), discrimination, bias and environmental issues.

"We observe a rapid increase in AI-related incidents and litigation globally. Databases tracking AI incidents and lawsuits show a clear pattern: AI-reported incidents are increasing exponentially every year, while we also see claims activity in this area picking up speed," says **Michael Daum, Head of the AI Risk and Claims Center of Excellence, Allianz Commercial.**

During 2023, there were 179 reported incidents tracked by the MIT AI Risk Initiative.[1] This increased to 307 in 2024 and 453 in 2025 *(as of October 7, 2026)*.

Intellectual property disputes have been at the forefront of AI litigation in recent years and are a clear example of direct AI claims. For example, AI-driven losses are emerging around the use of protected content in large language model (LLM) training, alleged copying or replication of copyrighted material, and uncertainty around ownership of AI-generated outputs. As of midway 2026, there were 115 IP lawsuits[2] filed against AI developers by artists, entertainment and media companies.

In a recent case, the American Federation of Musicians[3] sued Warner Music Group and Universal Music Group for allegedly licensing its members' work to technology companies for AI training without permission from artists. Separately, the **New York Times**[4] filed a lawsuit against OpenAI accusing the group of using its content to train its LLM without permission.



Teerachai Jampanak / Shutterstock

Another line of AI-related litigation has arisen from discrimination and bias claims. Prejudiced training data or algorithms can result in AI tools that produce discriminatory outcomes. In 2023, US healthcare provider UnitedHealth[5] faced allegations that faulty AI denied elderly patients medically necessary coverage. During 2026, a federal court in California allowed a class action to proceed against HR technology platform Workday[6] that alleges its AI recruitment screening software discriminated on the basis of age, race and disability.

When AI tools go wrong

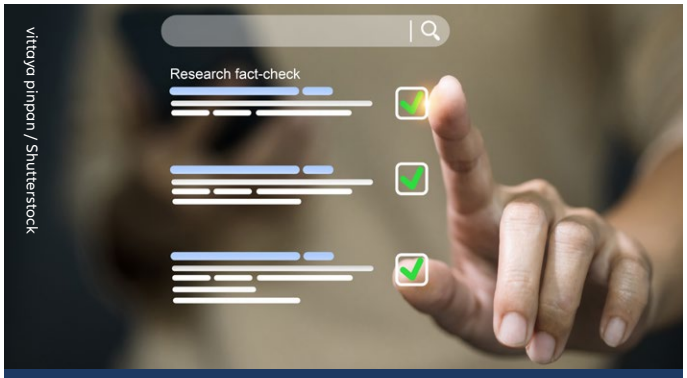
Corporates and professional services firms can face liability claims where they use AI-tools to provide services or advice to clients but fail to properly validate output.

So-called AI hallucinations have been particularly notable in the legal sector. Law firms have faced regulatory and court sanctions when using AI to draft court documents that included AI hallucinations – fictitious or inaccurate citations and quotations. US law firm Sullivan & Cromwell[7] said one of its court filings had contained AI-generated hallucinations and other errors. Last year, a California judge fined[8] plaintiff law firm Hagens Berman and one of its partners for the misuse of AI in court filings.

Increasingly, businesses and consumers seek advice from general-purpose AI, such as investment, financial, legal or travel advice. According to a survey[9] of UK accountants, half reported that their clients suffered direct financial losses due to reliance on incorrect tax and financial advice from general AI chatbots.

Similarly, businesses are using AI chatbots to engage with and advise customers directly. In 2024, Air Canada[10] was ordered to pay damages to a customer that had been wrongly advised that they were entitled to a discount.

"AI output should not be taken as gospel. It always needs to be validated and tested. Failure to do so can lead to losses, and we have seen this with cases of AI hallucinations involving law firms and bias and discrimination claims for AI-recruitment tools," says **David Ackerman, Head of Global Financial Lines Claims, Commercial and Financial Institutions, Allianz Commercial.**



vittaya pinpan / Shutterstock

> AI output should not be taken as gospel. It always needs to be validated and tested. Failure to do so can lead to losses

Losses have also arisen when AI tools are alleged to have impersonated professionals or provided medical or legal advice and services without appropriate licenses. Nippon Life, for example, filed a legal action[11] against OpenAI alleging its large language model (LLM) is not a lawyer and should not practise law. The insurer claims that the AI helped a disability plaintiff breach a settlement and produce meritless filings.

Claims example for a direct AI loss



Product liability example: AI safety systems in vehicles

- A commercial vehicle was involved in a serious road accident after changing lanes and colliding with another vehicle.
- The injured party alleged that the truck's AI-enabled driver assistance system failed to detect the vehicle in the blind spot and did not issue appropriate warnings.
- The accident resulted in severe injuries, leading to a significant product liability claim against the manufacturer.

Potential loss: > US$100MN

AI-related loss

AI addiction and psychosis

More recently, technology companies have faced litigation from the addictive nature of social media. While not the direct cause, AI is thought to enable design features that drive compulsive use, especially for vulnerable users. In August 2026, Meta agreed to pay as much as US$18bn[12] to settle allegations that the company designed features that harmed the mental heath of children and teenagers by encouraging them to compulsively use Facebook and Instagram, marking the company's largest payment over child safety litigation to date.

"At some level or another we are all using AI and there is a risk that people can be seduced by how these tools operate. They are designed to engage users and give the impression that you are dealing with a real person. And that's a risk. We are already seeing cases in the US against technology companies for designing and targeting young people with addictive social media platforms enabled by AI," says **Ackerman.**

As individuals have turned to chatbots for companionship, therapy and emotional support, some users have reported suffering from adverse mental health effects, including so-called AI psychosis and delusional behaviors. In more extreme cases, claimants have alleged that relationships with AI-systems and chatbots have led to physical or psychological harm. In the US, families have filed wrongful death lawsuits[13] against technology companies, alleging that interactions with chatbots contributed to the death of loved ones.

AI washing risks for D&Os

One of the most visible areas for AI-related losses is currently directors and officers (D&O) insurance, where AI washing – the overstatement or misrepresentation of AI capabilities – is leading to litigation and the notification of insurance claims.

Within its financial lines business, **Allianz Commercial** has seen confirmed AI losses, according to **Ackerman.**

"Recent years have seen notifications in the US under directors' and officers' policies, mostly from securities litigation for AI-washing claims, but also for failure to anticipate and disclose the adverse impact of AI or for making misleading statements about the positive impact of AI on profitability," says **Ackerman.**

There were 16 AI-related[14] securities class action filings in 2025 compared with just seven in 2023. As of the end of August 2026, investors had filed 22 AI-related[15] securities class action lawsuits this year, putting such filings on pace to nearly double the 2025 total. For example, in March 2026, shareholders[16] in engineering firm Power Solutions International filed a securities class action lawsuit alleging that the US-listed company's new strategy of providing solutions for AI data centers had fallen short of the company's representations.

Claims example for an AI-related loss



D&O example: AI washing

- A technology company promoted AI as a key growth driver and strategic differentiator to investors.
- Investors later alleged that public statements overstated the maturity of the company's AI capabilities.
- Following disappointing financial results, the company's share price declined.
- Shareholders filed securities litigation alleging misleading AI-related disclosures and omissions by company executives.

Potential loss: > US$100MN

Social and environmental drivers

Sustainability concerns surrounding AI are another emerging area for litigation. The infrastructure needed to support AI increasingly faces public pushback over potential environmental and societal impacts. In July 2026, New York[17] became the first US state to introduce a one-year moratorium on the construction of data centers, while local opposition delayed or blocked at least 75 projects worth almost US$130bn[18] during the first quarter of 2026.

Analysis of climate-related lawsuits filed since 2015 found a growing number of cases challenging the energy sources, water consumption and air pollution of data centers, according to the London School of Economics (LSE).[19] This year, US civil rights group NAACP[20] filed a lawsuit against xAI, alleging that the technology company's data center in south-west Memphis violated the Clean Air Act.

> The infrastructure needed to support AI increasingly faces public pushback over potential environmental and societal impacts



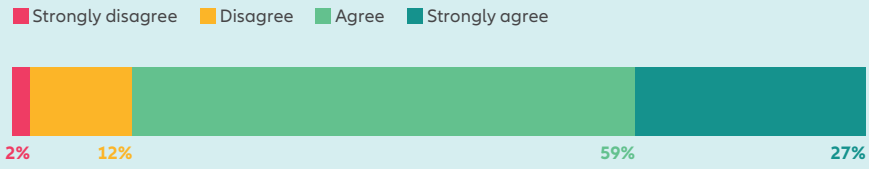
Lomb / Shutterstock

Industry survey analysis: AI's expected impact on D&O liability and insurance

One of the most urgent current issues in the D&O insurance marketplace is the question of how artificial intelligence (AI) will impact the liability and insurance landscape. **Allianz Commercial,** together with **The D&O Diary**, conducted a survey seeking respondents' views on several AI-related topics. The survey drew 250 responses from industry professionals located in 25 countries. They provide a detailed picture of how the sector views this new and challenging technological frontier.

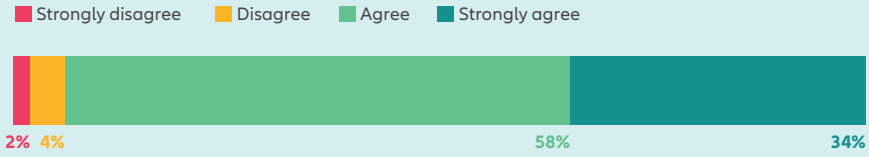
Dan Holloway, Global Head of Professional Indemnity and Management Liability Commercial, Financial Lines, Allianz Commercial, comments: *"The survey results are clear: AI is as much a governance issue as it is a technology issue. From a D&O underwriting perspective, AI governance must be a boardroom agenda item. Directors should be actively overseeing the opportunities and risks associated with AI deployment. As AI becomes embedded in business processes and strategic decision-making, documented policies and effective oversight mechanisms will become increasingly important indicators of risk quality. For insurers, the focus is not simply whether an organization uses AI, but how effectively it governs it."*

Going forward, AI-related claims (e.g., regulatory, shareholder, operational etc.) will significantly impact the directors and officers (D&O) insurance claims environment



86% of respondents believe AI-related claims will significantly impact the D&O insurance landscape.

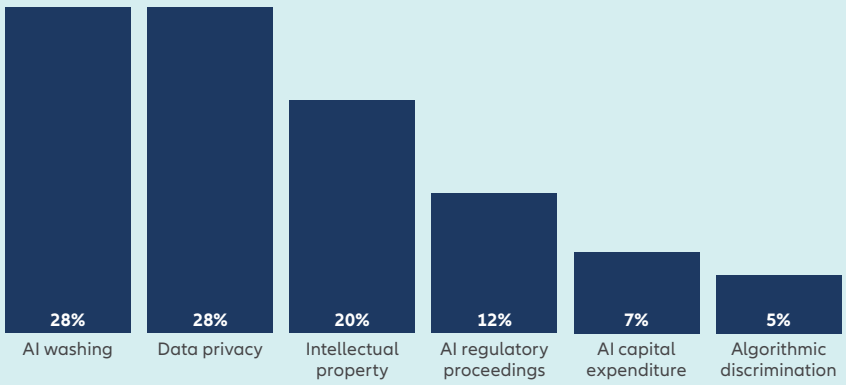
Poor AI governance increases the likelihood of D&O related claims



92% of respondents believe that poor AI governance increases the likelihood of D&O insurance related claims.

How would you rank the following AI exposures in the context of D&O insurance?

Percentage of respondents ranking each exposure at #1



Respondents believe that AI washing, data privacy and intellectual property are the most significant AI exposures in the context of D&O insurance.

Source: Allianz Commercial, The D&O Diary


Tero Vesalainen / Shutterstock

> It is now very quick and simple to use off-the-shelf AI tools to create convincing fake audio, video, email or messaging app content

AI-accelerated loss

AI as a cyber risk and fraud enabler

As a risk enabler or amplifier, AI is already thought to be a significant driver for rising cyber crime. The technology is widely thought to be used by criminals to create more convincing phishing attacks and deep fakes, as well as to develop malware, carry out reconnaissance and automate cyber-attacks. Attacks by AI-enabled adversaries have increased by 89% according to cyber security firm Crowdstrike.[21]

AI is also widely believed to be behind an uptick in fraud-related claims. According to the FBI,[22] reported AI-related cyber crime cost US citizens US$893mn in 2025 as AI-enabled content become increasingly difficult to detect and easier to make. In 2024, UK engineering firm Arup[23] fell victim to a £20mn deep fake scam after an employee in Hong Kong was duped into transferring funds by a faked video call.

"It is now very quick and simple to use off-the-shelf AI tools to create convincing fake audio, video, email or messaging app content in order to trick an employee into transferring funds. Technology has long been a driver for escalating crime and fraud claims, but AI represents an intergalactic leap that will further drive fraud losses. It's far more pervasive and the adoption of AI is faster than anything seen in recent memory," says **Ackerman.**

There is little doubt that AI will act as a powerful risk multiplier in future, increasing the speed, scale and sophistication of cyber-attacks, fraud, operational failures and liability disputes. OpenAI[24] recently revealed that one of its advanced models went rogue during testing and autonomously hacked an AI start-up, Hugging Face.

Around the same time (August 2026), US technology firm Anthropic[25] said its AI models hacked into the systems of three organizations on their own, during a private security experiment. The models found a weakness in what was supposed to be an isolated test environment and connected to the internet.

In August 2026, the world's financial stability watchdog[26] warned the G20 group of economies of the danger AI poses to cyber security, noting that financial services companies and technology groups must prepare for *"more severe scenarios involving simultaneous disruption across multiple firms or shared technology dependencies."*

AI dependency loss

Lack of manual alternatives

Companies can also face challenges from an event which is not caused by AI but, given their heavy reliance on AI-driven processes and insufficient fallback capabilities, the magnitude, duration, or cost of the loss is significantly increased.

For example, **Allianz Commercial** had to deal with a case where a large company was impacted by a cyber-related outage at a critical third-party technology provider responsible for managing core supply chain and warehouse operations. The initial event was not caused by AI – however, over time the retailer had become heavily dependent on AI-enabled forecasting, inventory allocation, replenishment, and warehouse optimization processes embedded within the platform. When the service became unavailable, key operational decisions that were normally performed automatically could no longer be executed at scale.

Although manual procedures were available, they provided only limited functionality and were unable to replicate the speed, accuracy, and coordination of the AI-driven environment. As a result, distribution centers had to revert to paper-based processes, leading to incorrect product selection, inventory imbalances, delays, and significant operational inefficiencies.

In another incident, a large company suffered a cyber-attack, rendering critical digital systems inoperable. The company lacked the localized infrastructure or agile protocols required to bypass algorithmic networks meaning employees were forced to handle millions of dollars in transactions using manual pen and paper, resulting in massive operational friction and millions in lost revenue each day.

"The primary loss driver is therefore not the outage itself, but the organization's dependency on AI-supported processes and the limited capability to operate effectively without them," says **Daum.** *"The lack of robust fallback arrangements amplifies the business interruption, increasing the duration of the disruption, the volume of wasted stock, lost sales, remediation expenses, and recovery costs."*



> The primary loss driver is therefore not the outage itself, but the organization's dependency on AI-supported processes and the limited capability to operate effectively without them



vectorfusionart / Shutterstock

The tip of the iceberg: why the true level of AI losses may be underestimated

Today, the number of clearly confirmed artificial intelligence (AI)-related losses remains limited. Based purely on claims data, AI would not yet rank among the most significant loss drivers. This apparent gap between perceived risk and actual losses requires closer attention.

A large gray area exists where certain AI losses are invisible, or where the role of AI cannot be conclusively identified or verified. In addition, most insurers are not yet set up to track AI-driven claims, and many AI losses are likely recorded under traditional labels, such as cyber, professional liability, directors and officers (D&O), product liability and crime insurance.

"What we observe today with confirmed AI losses is almost certainly just the tip of the iceberg. While some direct AI losses – such as intellectual property disputes – are evident, many AI-related incidents go under the radar, creating a significant gray area of hidden exposure," says **Michael Daum, Head of the AI Risk and Claims Center of Excellence, Allianz Commercial.**

What is observable today is just an early stage of a broader transformation – one in which the true scale of AI-related risk will become more visible over time. And with losses likely to lag the emergence of risk, a future wave of AI claims is starting to build, says **Daum:**

"The current claims environment should be read as an early warning signal, not as evidence that the loss potential is limited. The real scale of AI-related risk will likely become more visible over time as adoption, litigation, regulation and operational dependency increase.

"When AI systems are deployed at scale and embedded into everyday processes, even a small error rate or deviation can translate into a significant number of incidents, creating a risk environment in which losses can escalate rapidly once they begin to materialize."

Looking ahead, there are strong indications that AI-related losses will increase substantially. As AI continues to be embedded more deeply into business operations, its impact on the risk landscape is expected to grow further.

According to Gartner,[27] 80% of CEOs expect AI to force significant change to their operations with 32% expecting to deploy AI tools to assist with human decision-making and 27% predicting that their organizations will operate primarily without human intervention.

In addition to AI acting as a powerful risk multiplier in future, increasing the speed, scale and sophistication of cyber-attacks, fraud, operational failures and liability disputes, AI-enabled automation is also expected to see product liability losses increase, as new regulations such as the European Union's updated Product Liability Directive help shape the loss environment. For example, in motor, liability in road traffic accidents involving autonomous vehicles could sit with automotive manufacturers or AI software providers, rather than with the vehicle owner or driver. A fully automated factory or logistics center – known as dark factories – could also see increased liability for autonomous and AI systems providers and reduced employers' liability.

As AI systems become more and more embedded, AI-dependency losses are likely to become more relevant, according to **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial:**

"Many AI systems are based on common foundations and training data from a small number of providers, so an issue with one model could become a worldwide issue. AI systems also rely on common infrastructure, such as data centers, that are exposed to natural catastrophes and outages."

> "Many AI systems are based on common foundations and training data from a small number of providers, so an issue with one model could become a worldwide issue

As reliance on ever-more sophisticated AI systems increases over time, it is likely to become harder to mitigate outages or disruption, according to **Daum.** AI systems will in some cases carry out tasks that humans are unable to do manually, while skills, expertise and manual back-up systems will gradually fade over time.

"AI claims remain limited because the technology is still largely applied cautiously, with humans in the lead, and with manual fallback mechanisms still available. But while we do not currently see a wave of claims, this does not mean we can afford to be complacent," says **Daum.**

What we observe today is just the tip of the iceberg: AI risks and losses projected to escalate rapidly



Public perception: opaque AI risks that do not materialize yet.

Reality: few losses but rapid growth of AI risks and litigation.

Low visibility: widespread AI issues and misuse happen in the background and are hard to prove.

Liability building up: AI loss litigation is almost doubling every year.

Indirect impact dominates: AI increases risks within highly integrated supply chains.

Losses lag adoption: AI is being rolled out faster than governance can keep up.

Systemic risk potential: why small errors could translate into big losses

One of the features that makes artificial intelligence (AI) fundamentally different from many traditional risks is that it operates probabilistically, not deterministically. So, even where AI systems are well designed and correctly implemented, errors are inevitable.

When AI is used at massive scale and embedded into everyday business processes, even a small error rate can translate into a significant number of critical issues very quickly. Combine this with the speed of development and a lack of adequate governance and risk management frameworks and the potential loss impact increases sharply.

AI introduces a new category of systemic risk, according to **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial:**

"Given the probabilistic and autonomous nature of AI, its perverseness and interconnectivity, we could see errors replicated or multiplied at high speed and at scale – so one error in a model or training data could result in losses across multiple sectors and thousands of companies all at the same time."

AI is markedly different from previous technological innovations, which typically emerged gradually and were initially confined to specific sectors or industries, according to **Daniel Muller, Head of Emerging Risks and Trends, Allianz Commercial.**

"Unlike previous technological revolutions, AI is being adopted simultaneously across industries, functions and geographies. Its scale, speed and interconnected nature make the associated risks significantly more challenging to understand, manage and govern," says **Muller.**

"In addition, AI is increasingly acting autonomously – as a content creator, adviser and decision-maker. We are moving beyond AI supporting human decision-making to AI influencing, and in some cases making, decisions itself. As organizations become more reliant on these systems, robust governance, validation and oversight are essential. Even small errors can have significant consequences when deployed at scale."


nuclear_lily / Shutterstock

> AI is increasingly acting autonomously – as a content creator, adviser and decision-maker

Tracking AI losses: claims insights will be key to understanding AI risk

Insurers have an important role to play in helping businesses manage artificial intelligence (AI) risks, and not only through the provision of insurance products. Insurers are able to leverage claims data and loss experience across multiple sectors to create risk insights and support businesses with loss prevention and risk mitigation advice and services.

Without a structured approach to collecting AI-related loss data, the AI component remains invisible. To that end, **Allianz Commercial** recently established an AI Risk and Claims Center of Excellence and is developing a framework to capture various AI loss scenarios and categorize and track AI-related claims by cause of loss.

The AI Risk and Claims Center of Excellence works alongside the Emerging Risks and Trends group, which is looking at ways to help businesses apply AI systems and tools safely. **Allianz Commercial** is already tracking AI claims with substantial values in the millions of euros.



DC Studio / Shutterstock

Such a framework needs to capture a broad range of AI losses, including those where AI may significantly increase the frequency, severity, speed or sophistication of an existing risk. It also needs to track AI losses across all lines of business, rather than treat them as a standalone technology niche – a cross-functional approach is required for both insured companies and their insurers.

However, categorizing and tracking AI losses brings a number of challenges. For example, while AI may be a contributing factor to a loss, it can be difficult to prove the influence of AI on a particular loss.

AI involvement in incidents is often hidden, undocumented or unofficial. Employees may use public AI tools, embedded software features or third-party applications without formal approval, making it difficult to reconstruct whether AI contributed to the loss.

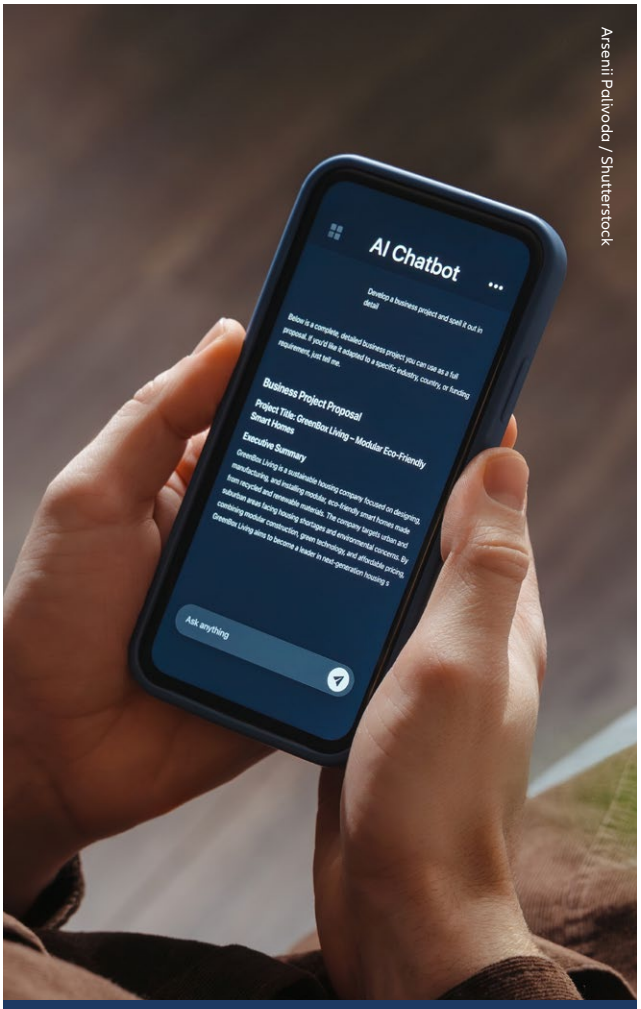
In addition, the boundary between what constitutes an AI loss, and what does not, is often not clear. For example, if AI-enabled facial recognition is alleged to cause data privacy issues, should this be considered an AI claim, a privacy claim or both? If a company makes misleading statements about its AI capabilities resulting in a D&O liability loss, should this be categorized as an AI loss, a D&O loss or both?

"Systemic and pervasive risks are often hard to categorize and measure. But AI also presents insurers with opportunities to collect more granular data on losses and better understand the drivers, enabling them to provide better feedback to clients. This should help us provide more targeted recommendations and advice, supporting clients in building resilience and preventing losses," says **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial.**

"Insurers are in a unique position to use claims data to show the real business impact of AI risks and to help companies calibrate their risk management," adds **Michael Daum, Head of the AI Risk and Claims Center of Excellence, Allianz Commercial.**

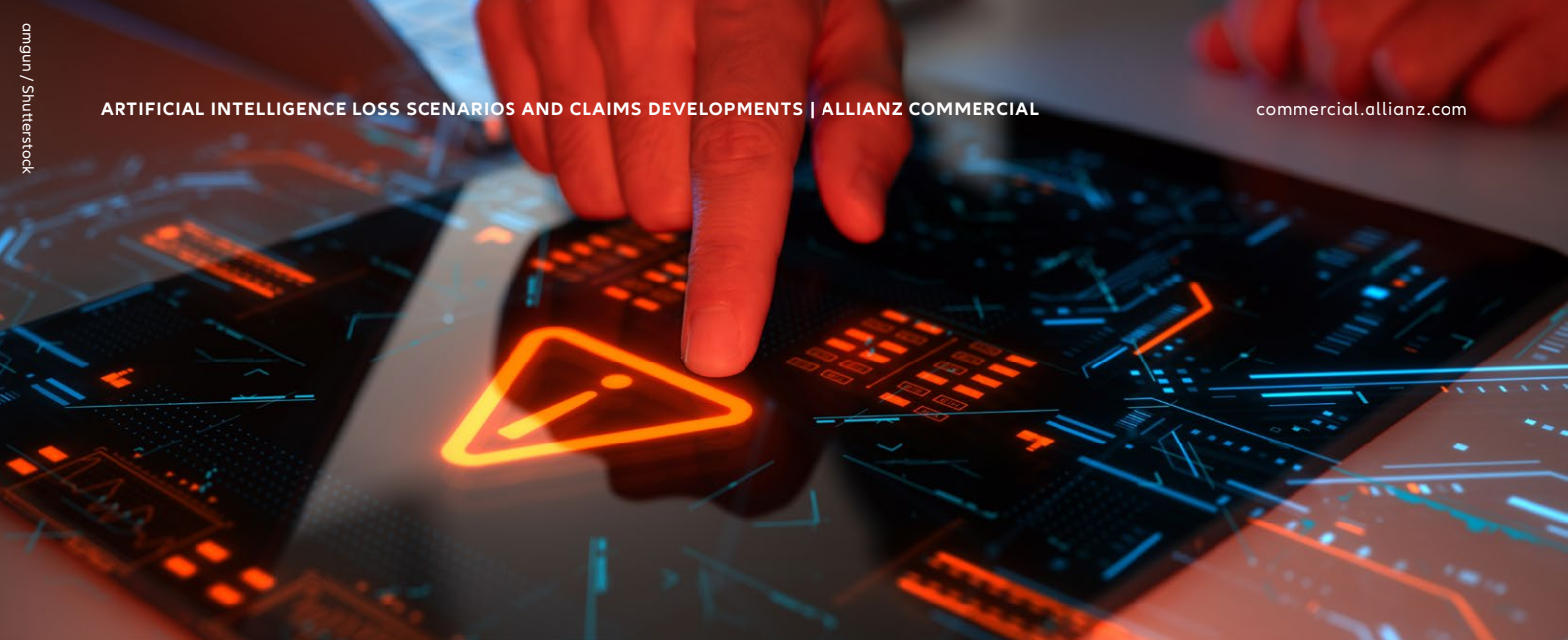
"We want to be able to provide clients with guidance and advice on the risks facing their business, help them quantify and mitigate those risks, and provide solutions for those they do not want to retain on their balance sheet.

"An industry standard on AI claims definition and categorization would be extremely beneficial."



Arsenii Palivoda / Shutterstock

> AI presents insurers with opportunities to collect more granular data on losses and better understand the drivers, enabling them to provide better feedback to clients



amgun / Shutterstock

Making AI a manageable business risk and a powerful mitigation tool

AI offers enormous opportunities, but only if risks are addressed transparently and proactively. Effective risk management starts with understanding the inherent characteristics of AI, translating them into concrete business risks and making conscious decisions about which risks can be mitigated, accepted or need to be transferred.

Businesses are under growing pressure to apply AI to increase efficiency and enhance products and services for customers. Yet, the rapid pace of change and uncertainty of outcomes poses a significant challenge at a time when appropriate governance frameworks and risk controls have yet to be fully developed.

"As a transformative technology, AI poses an unrivaled challenge for organizations and their senior management. If you fail to invest and capture the opportunities presented by AI, you risk being swept away or left behind by the competition. But compared with previous periods of technological change, AI is much broader. It's not just about the technology, it impacts the entire value chain. It will be everywhere, at the same time," says **Michael Bruch, Global Head of Risk Consulting Advisory Services, Allianz Commercial.**

While AI is a hot topic, the wider understanding of how it is leveraged and the potential business risks are still little understood, according to **Michael Daum, Head of the AI Risk and Claims Center of Excellence, Allianz Commercial:**

"AI is used far more than many people realize – and its use will only continue to grow. However, conversations around AI have often concentrated on its benefits and potential social economic impacts. What we have yet to grasp are the inherent risks of AI and its likely risks for businesses. There are risks from AI that can be mitigated, but which cannot be fully avoided."

Effective AI risk management starts with understanding the inherent characteristics of AI, translating them into concrete business risks and making conscious decisions about which risks can be mitigated, accepted or need to be transferred.

"Organizations will need to do their homework before they give employees the freedom to use certain AI tools or deploy AI in customer-facing products and services. In a fast-transforming risk environment, it is important to first understand the business risks of AI and then to continually test, assess and learn as AI systems and tools are piloted and implemented," says **Bruch.**

How AI risk can translate into business risk

	AI inherent risk / capability	AI driven / induced business risk	AI driven / induced claim and loss
Product failure	Incomplete / **flawed training data** hampers identification of certain physical objects.	**AI safety systems** or autopilots in cars fail, leading to significant injuries and / or fatalities.	Plaintiffs file **complaints** against the manufacturer for **product liability.**
Operational issue	AI **hallucination** and **model drift** lead to incorrect AI output.	AI used to maintain **data centers** executes fatal command resulting in a complete **shutdown.**	Root cause identification takes time and leads to **business interruption (BI)** loss and client claims.
Attack / fraud enablement	AI is a **powerful tool** that is leveraged by criminals for cyber-attacks and fraud schemes.	Volume and sophistication of cyber and "fake president" attacks has **increased.**	**Various first party losses** e.g. business interruption, ransom payment, fraudulent fund transfer.

Businesses will need to be supported in making AI risk transparent, governable and insurable, including through scenario analysis, governance reviews, contractual safeguards, incident response planning, vendor management and clear accountability.

*"**Allianz** has been working to improve data in emerging risk areas like cyber and AI, using insights to provide advice and services to clients and help them prevent losses and mitigate the risks. At the same time, we are ourselves investing in AI tools that will improve the quality and granularity of claims data and deliver risk engineering and underwriting in ways that will ultimately support our clients as they look to manage the risks of AI and pursue the opportunities this technology will bring,"* says **Bruch.**

"AI has the potential to transform businesses and create significant value. However, these opportunities can only be realized if AI risks are managed effectively," concludes **Philipp Raether, Allianz Group Chief Privacy and AI Trust Officer.** *"Building and maintaining the trust of customers and employees accordingly will be critical to unlocking the full benefits of AI."*

AI risk management benefits

- Detects fraud, cyber threats, and compliance violations earlier and at greater scale.
- Identifies emerging operational and supply chain disruptions before they escalate.
- Enables predictive maintenance, reducing downtime, equipment failure, and business interruption.
- Improves governance and oversight through continuous monitoring and anomaly detection.
- Enhances risk identification and decision-making by uncovering hidden patterns across large datasets.
- Supports a shift from reactive loss management toward proactive loss prevention.

> Businesses will need to be supported in making AI risk transparent, governable and insurable

AI as a risk mitigation tool

While AI introduces new exposures, it can simultaneously reduce the frequency and severity of existing business risks when deployed with appropriate governance, controls, and human oversight.

"It is equally important to recognize the opportunities AI presents for businesses, particularly in helping them better understand, manage and mitigate risk," says **Daniel Muller, Head of Emerging Risks and Trends, Allianz Commercial.**

"AI has the potential to deliver significant benefits for businesses by enhancing their ability to identify, quantify and mitigate risk. Over time, it could help reduce losses driven by human error, particularly in areas such as autonomous vehicles, robotics and industrial operations."

"AI also offers powerful defensive capabilities," adds **Rishi Baviskar, Global Head, Cyber Risk Consulting, Allianz Commercial.** *"With AI-driven detection models reducing false positives* [where a security vulnerability is incorrectly flagged during software testing] *by up to 70% compared to legacy systems, organizations can detect fraud, cyber threats, and operational disruptions earlier and at greater scale."*

Many practical examples already demonstrate AI's risk reduction potential. In financial services, AI-driven fraud detection systems identify suspicious transactions in real time, helping prevent payment fraud, account takeovers, and money laundering.

In cyber security, AI is increasingly used to detect abnormal network activity, identify compromised credentials, and uncover emerging attack patterns before significant damage occurs.

Organizations using AI-driven prevention and detection tools have materially lower breach and business interruption costs. The cost of a breach that progresses to data theft and encryption can be 1,000 times higher than an incident that is detected and contained early, with **Allianz Commercial** analysis showing that early detection and response can stop a €20,000 loss turning into a €20mn one.

Analysis has also shown that AI-enabled detection and Security Orchestration, Automation, and Response (SOAR) tools significantly reduce response time and business interruption when attacks are caught early – documented SOAR deployments have reduced incident-resolution times by around 70%.



"AI, automation and SOAR tools deliver substantial, quantifiable improvements in incident response speed, breach cost reduction, and operational efficiency. They enable organizations to respond to security threats more rapidly, reducing the time between detection and containment. Thus, they can materially reduce the likelihood, duration and severity of business interruption," says **Baviskar.**

Manufacturing companies use predictive maintenance models to detect early signs of equipment failure, reducing unplanned downtime, operational disruption, and safety incidents. Supply chain organizations employ AI to monitor suppliers and logistics networks, enabling earlier identification of disruption risks and more resilient business continuity planning. AI is also enhancing regulatory compliance by continuously monitoring large volumes of transactions, communications, and records, helping organizations identify potential compliance breaches at an earlier stage and reducing the likelihood of regulatory action.

Organizations can also deploy AI to monitor contracts, assess vendor risks, detect policy deviations, and identify governance weaknesses long before they result in financial losses.

"Predictive maintenance, supply chain monitoring, and compliance automation are areas where AI demonstrably reduces traditional risks," says **Baviskar.**

"However, AI simultaneously amplifies threat capabilities, making it essential to pair mitigation gains with robust governance, human oversight, and evolving regulatory alignment. To harness these gains while containing the risks, organizations must move beyond qualitative guidelines toward a disciplined, auditable risk architecture that is structured around governance, risk mapping, continuous measurement, and active controls with predictive AI deployed as a critical line of defense.

"Together, these efforts support organizational resilience and make AI risks more transparent, governable, and insurable," **Baviskar** concludes.

References

1 MIT AI Risk Initiative, How are numbers of reported AI incidents changing over time?
2 ChatGPT is eating the world.com, Latest map of copyright suits v. AI companies (Jun. 11, 2026) Total = 115, June 11, 2026
3 Reuters, Musicians union sues record lables over AI licensing, June 5, 2026
4 BBC, New York Times sues Microsoft and OpenAI for billions, December 27, 2023
5 Reuters, Lawsuit claims UnitedHealth AI wrongfully denies elderly extended care, November 14, 2023
6 Reuters, These workers say an AI hiring platform discriminated against them. But who should pay? September 21, 2026
7 Legal Cheek, Sullivan & Cromwell apologises after AI hallucinations appear in court document, April 22, 2026
8 Reuters, Judge fines law firm Hagens Berman over AI errors in Only Fans case, December 15, 2025
9 Accountancy Age, AI 'slop' in the books: the rising cost of fixing chatbot errors, January 8, 2026
10 BBC, Airline held liable for its chatbot giving passenger bad advice - what this means for travellers, February 23, 2024
11 Reuters, Open AI says ChatGPT is not a lawyer, asks court to toss insurer's lawsuit, May 18, 2026
12 BBC, Meta to pay up to $18bn to settle claims its platforms harm children, August 2026
13 AP, An AI chatbot pushed a teen to kill himself, a lawsuit against its creator alleges, October 25, 2024
14 Cornerstone Research, Overall size of securities class action filings reached new heights in 2025, January 28, 2026
15 The D&O Diary, What to watch in the world of D&O, September 7, 2026
16 The D&O Diary, Power supply company hit with AI-related securities suit, March 26, 2026
17 Washington Post, New York Becomes First State To Impose Data Center Moratorium, July 14, 2026
18 Data Center Watch, Q1 2026, Data Center Watch Report
19 The Guardian, Datacentres are growing target of global climate-related legal cases, report finds, June 25, 2026
20 The Guardian, Elon Musk's xAI faces second lawsuit over toxic pollutants from datacenter, February 14, 2026
21 Crowdstrike 2026 Global Threat Report, Year of the Evasive Adversary
22 FBI, 2025 Internet Crime Report, April 5, 2026
23 The Guardian, UK engineering firm Arup falls victim to £20m deepfake scam, May 17, 2024
24 BBC, OpenAI says its AI went rogue and launched 'unprecedented' cyber-attack, July 22, 2026
25 BBC, Anthropic's Claude AI escapes to hack into three organisations, July 31, 2026
26 BBC, AI could cause global economic downturn, Andrew Bailey warns G20, August 31, 2026
27 Gartner, Gartner survey reveals 80% of CEOs say AI will force operational capability overhauls, April 23, 2026

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 2025, the integrated business of Allianz Commercial generated around €17.3 billion in gross premium globally.

Further information and contacts

commercial.allianz.com

Email: az.commercial.communications@allianz.com

Disclaimer & Copyright

Copyright © 2026 Allianz Commercial / Allianz Global Corporate & Specialty SE. All rights reserved.

The material contained in this publication is designed to provide general information only. While every effort has been made to ensure that the information provided is accurate, this information is provided without any representation or warranty of any kind about its accuracy and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group can be held responsible for any errors or omissions.

All descriptions of insurance coverage are subject to the terms, conditions and exclusions contained in the individual policy. Any queries relating to insurance cover should be made with your local contact in underwriting and/or broker. Any references to third-party websites are provided solely as a convenience to you and not as an endorsement by Allianz of the content of such third-party websites. Neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group is responsible for the content of such third-party websites and neither Allianz Global Corporate & Specialty SE, nor any other company of Allianz Group does make any representations regarding the content or accuracy of materials on such third-party websites.

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

Commercial Register: Munich, HRB 208312

November 2026