Swiss Re Institute

May 2024

Tech-tonic shifts

How AI could change industry risk landscapes

Key findings

- This study contains original Swiss Re Institute analysis of the risk profile of artificial intelligence (AI) across industries. We combine text analysis of recent AI incidents with historic loss data and forward-looking patent applications. This provides us with frequency and severity weightings across different sectors. We ultimately provide risk ratings over a short- and medium-term duration.

- Risk is currently concentrated in a few sectors. The most notable is technology, which should be no surprise given its role as the developer of AI systems. In contrast, we expect risk probability in energy and utilities to be relatively low; but any incident is likely to have a high severity. Frequency will increase as AI becomes more widely deployed in smart grids.

- Media and communications has short-term exposure to intellectual property risk. This reflects the recent coming onstream of generative AI and the legal status of the use of copyrighted materials to train large language models (LLMs).

- As AI use becomes more common, the risks will be more disbursed over sectors. Most prominent will be healthcare and pharmaceuticals due to a combination of 1) high frequency of potential incidents, given a high number of applications across the health value chain that could use AI; and 2) potentially high-severity losses (eg, bodily injury, professional liability).

- Other sectors with higher risk distribution include energy and mobility. Both industries are undergoing transformation that should see AI-use become more common place, such as in smart grids and autonomous vehicles. Both will give rise to higher risk frequency, and both could have high loss severity.

- Risks such as ethics, bias and privacy will be more prominent in the short term. As AI models are established, the danger is that existing flaws in data storage and analysis become entrenched. Those industries holding sensitive personal data – such as healthcare, finance or law – are particularly vulnerable.

- Longer term, performance risk will grow in importance. Assuming teething pains in creating AI models can be solved, performance risk will become the dominant risk category. This will particularly be the case for closed-systems production such as agriculture or manufacturing.

- Insurers will approach AI with a mix of new ideas and old exposures. The first specific AI products have already come to market, covering performance risk. The scope for expansion of this line is considerable. Cyber risk will overlap AI exposures, potentially give rise to new covers. Insurers will also have to monitor established lines like property or liability for losses caused by AI failure, or IP risks in professional lines.

Introduction

The potential benefits of artificial intelligence (AI) are immense. One estimate suggests that generative AI, a sub-branch of AI, could alone add "between USD 2.6 trillion and USD 4.4 trillion" annually to the global economy.[1] Swiss Re has written extensively on how AI and generative AI will likely be transformative within the insurance industry.[2]

In one respect, however, AI is no different from other technologies: it can go wrong. AI may fail against performance benchmarks; it may inadvertently perpetuate discrimination; it could be subject to malicious attack; or it will perhaps cause real world damages. Wherever there are opportunities – and the opportunities are huge – there will be risk.

In this study we isolate six specific AI insurance risks. Drawing on data and anecdotal examples, we map these risks across industry sectors. These provide us with a helicopter view of sectors where AI risk is currently more concentrated, both by frequency and severity; and where it may become more prevalent with time.

The role of the insurance industry is to support our clients manage AI-related risks, in part with new risk protection products and partly through our existing lines of business. Providing AI risk solutions is a significant opportunity for the industry. It is also a potential vulnerability, particularly when AI risks accumulate unseen within insurers' portfolios.

This publication provides some early analysis and thoughts on AI risks, how these may play out across industry lines, and how re/insurers could shape their business offerings accordingly. We hope it makes for a stimulating read.

1 *Beyond the hype: Capturing the potential of AI and gen AI in tech, media and telecom,* McKinsey & Company, 22 February 2024.
2 *Generative AI in insurance: How should we see the AI machine?,* Swiss Re, 4 March 2024.

Industry, AI and risk: a modelling approach

What is AI: The OECD defines an Artificial Intelligence (AI) System as: A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[3]

AI, like any technology, comes with risk. We created a model to provide us with both a current view as to where, on an industry basis, that risk might be concentrated; and where it might be concentrated in the future.

Our model is based on text mining to assess past AI incidents combined with forward-looking patent data.[4, 5] We use this data to assess 10 industries for overall AI risk.[6] This data allows us to draw a near-term ranking of current AI risk; and where we expect risk to be in an 8–10 year period. Risk scoring is drawn from two components: (1) the probability, or frequency of an AI-related incident taking place; and (2) the loss potential, or severity of loss, of such incidents.

$AI\ risk_x = F(Probability_x, Severity_x)$

We subdivide risk into six categories most applicable for insurance (see Table 1).[7]

Table 1
Risk categories included in this study

Data bias or lack of fairness	Unintended discrimination by AI of groups by gender, race, age or other distinguishing characteristic such as geography
Cyber	Cyber vulnerabilities of AI systems; or malignant use of AI systems
Algorithmic and performance	Failure of AI to hit required performance metrics
Lack of ethics, accountability, and transparency	Failure of AI to adhere to a required code of ethics and accountability, obscured by lack of transparency
Intellectual property (IP)	Use of third-party IP in AI training purposes; and unintended IP violations by AI systems
Privacy	Exposure of personally sensitive data in training AI; and unintended disclosure or effective identification of individuals in AI output

Source: Swiss Re Institute.

This risk categorisation is largely consistent with the AI litigation database, which contained at the time of writing 179 cases of AI-related litigation.[8] The identification of AI incidents from litigation as well as studies and press reports, provides the basis of our **probability** occurrence.

We calculate **severity** scores based on historic data from five categories: (1) physical injury;[9] (2) property damage; (3) cyber incident; (4) reputational damage;[10] and (5) business interruption and other economic losses.[11] Each severity category is allocated a weight based on actual incurred loss data;[12] as well as a weighted average across the five severity categories. These are aggregated to a sectoral level.

The average of normalised probability and severity scores brings us to a final industry risk ranking assessment, for current and 8–10 year future time horizons.[13]

3 *Artificial Intelligence and Responsible Business Conduct*, OECD, Accessed 13 May 2024.
4 From PATENTSCOPE, World Intellectual Property Organisation (WIPO), see Appendix.
5 Using data from OECD AI Incidents Monitor (AIM), see Appendix.
6 For a detailed understanding of the sources and methodology driving the results in this paper, see Appendix.
7 For more detailed explanations, see Appendix.
8 *AI Litigation Database*, The George Washington University, accessed on May 6, 2024.
9 As proxied by personal accident and healthcare data from the US for 2022, as extracted from Axco.
10 As proxied by liability incurred losses data from the US for 2022, as extracted from Axco.
11 As proxied by the residue-difference between total non-life insurance and the other loss categories considered.
12 We use 2022 incurred loss data from US as a representative country. Weights are incurred losses for every loss category divided by total non-life losses.
13 Future time horizon is expected to have a gestation of 8–10 years.

Our model results produced the following risk rankings across industries (see Figure 1):

Figure 1
Current and future risk ranks for industries[14]

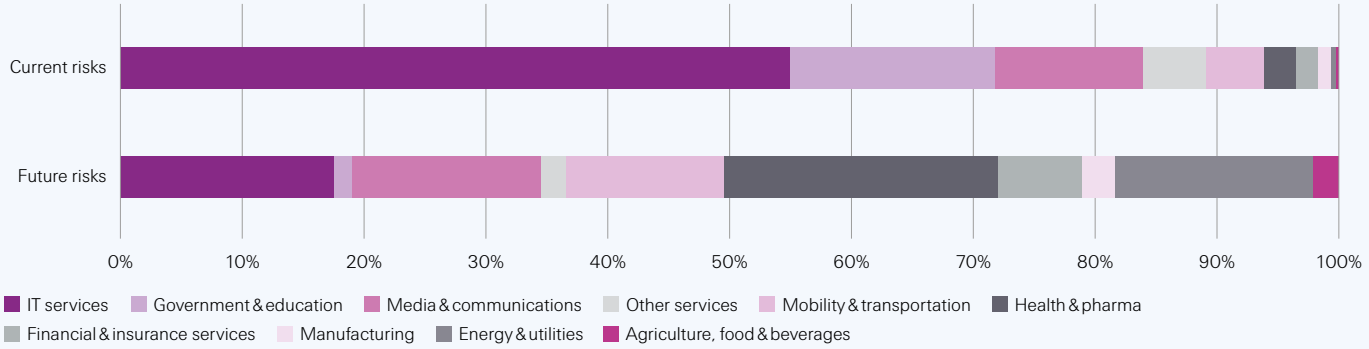
Current risks 2024–2025				Overall risks rank movement	Future risks 2032–2034			
Severity rank	Probability rank	Overall risk rank	Sector		Sector	Overall risk rank	Probability rank	Severity rank
5	1	**1**	IT services		Health & pharma	**1**	1	1
1	9	**2**	Energy & utilities		Mobility & transportation	**2**	5	2
2	6	**3**	Health & pharma		Energy & utilities	**3**	3	5
3	4	**4**	Other services		IT services	**4**	2	7
6	5	**5**	Mobility & transportation		Media & communications	**5**	4	10
4	7	**6**	Financial & insurance services		Government & education	**6**	10	3
8	2	**7**	Government & education		Financial & insurance services	**7**	6	8
7	8	**8**	Manufacturing		Manufacturing	**8**	7	4
9	3	**9**	Media & communications		Agriculture, food & beverages	**9**	8	6
10	10	**10**	Agriculture, food & beverages		Other services	**10**	9	9

Source: Swiss Re Institute[15].

[14] Normalized probability and severity scores are first calculated and both are given equal weightage in calculating final ranks.
[15] Other industries include retail, hospitality, real estate and legal services.

In the near term, the highest probability of risk by some distance (55% of total, see Figure 2) falls on the IT sector. This is reflective of the sector's 'first mover' status – the IT sector is, after all, developing AI technology, and is first to put it to wider use. We discuss the use of AI in coding later in this paper. Government and education is the second most frequent source of risk, reflecting the wide scope of use of AI technologies across public and educational sectors. Third comes media and communications, both as a result of the high use potential; and legacy intellectual property (IP) issues, which we will specifically discuss later in the paper. Severity of incidents is highest in the energy and utilities sector, reflecting the critical nature of infrastructure, even if frequency is low. Health and pharmaceuticals is the second most severely impacted sector, as a result of potential risk in this highly regulated industry.[16]

Figure 2
Current and future risk flow across industries

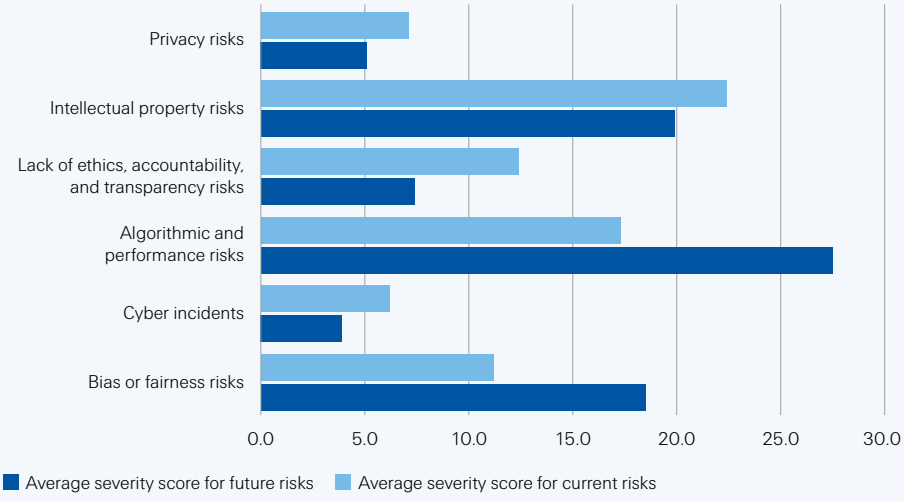


Source: Swiss Re Institute.

Fast forward 8–10 years, when AI is being used extensively across a range of industries, and risk frequency will be much more evenly distributed. The severity of risk in the health and pharmaceutical sector remains high; but will be exacerbated by a rise in frequency. This is because of the high number of processes in healthcare delivery that could be enhanced with AI (we highlight bias in pharma development as well as AI diagnoses later in this document). Second in our ranking, we have mobility and transport. This will be driven, literally and figuratively, by automation, most notably self-driving cars, as we will explore later. Also, growing in frequency will be energy and utilities, as smart grid technologies powered by AI increasingly come on stream to support net zero transition.

[16] Refer Figure 12 in *Additional data insights*.

Figure 3
Average loss severity score for different risk categories



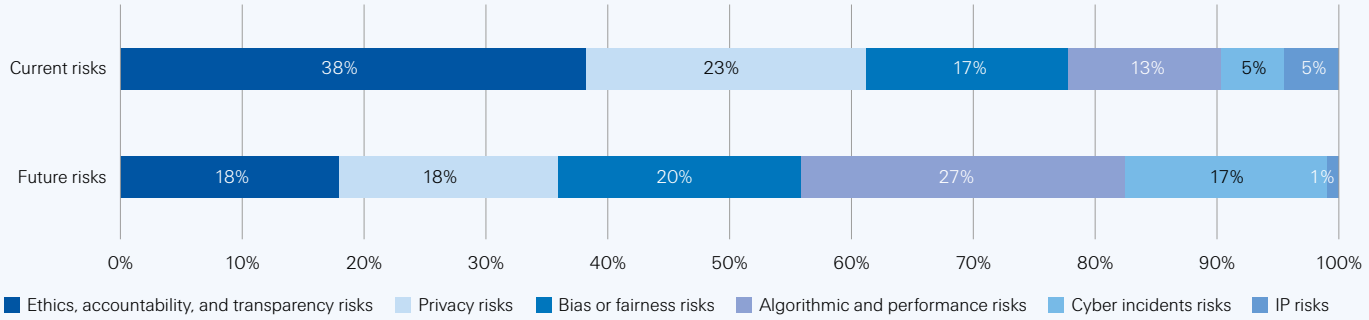
Source: Swiss Re Institute.

We can further transpose our results to focus on the risk drivers rather than industry (see Figure 3). In the near term, IP risks appear to be our most severe loss category, likely associated with the use of generative AI and copyright material, as we outline later in this paper. There is a danger of bias and discrimination becoming more severe over time if we do not take corrective measures. As we describe later, bias could affect everything from fair lending to pharmaceutical research. Over the longer term, however, as AI becomes embedded across a wide range of industries, we expect the single most severe risk to become one of performance, whether that is of vehicles, manufacturing plants, crop modelling, consumer chatbot interfaces or any manner of other uses.

Key sectoral analysis

IT services: first-mover risk

Figure 4
IT services current and future risks landscape
Overall current risks rank: 1
Overall future risks rank: 4
Spread of current and emerging risks across risk categories:



Source: Swiss Re Institute.

The tech sector is the primary sector developing and creating AI technologies. This exposes it to first mover risk, and hence, its position accounts for almost half current risks in our scoring chart. Over an 8–10 year time horizon, we expect the weight of the sector to diminish as AI becomes an established technology across other sectors.

Some of the more prominent near-term risks are:

- **Intellectual property**, which is primarily a problem of generative AI, in that there can be conflict between the learning needs of large language models (LLMs) and the rights of content producers (for greater detail, see section on *Media and Communications*).[17] Conflict between creation and learning exists within the industry too, in the form of code (see *Cracking the code: AI and software development* below).

Plagiarism: Gen AI platform warranties
Recognition of exposure to potential IP claims has seen a number of Big Tech companies proactively assure their users and clients that they will not be on the hook for any copyright infringements generated by their AI products. IBM, OpenAI and Microsoft among others, will offer legal protection from intellectual property claims that users of their AI tools/products may incur.[17,18,19]

[17] Gartner describes LLMs *thus*: "A large language model (LLM) is a specialized type of artificial intelligence (AI) that has been trained on vast amounts of text to understand existing content and generate original content." *Information Technology Glossary*, Gartner, accessed 13 May 2024.
[18] "IBM Announces Availability of watsonx Granite Model Series, Client Protections for IBM watsonx Models", *newsroom.ibm.com*, 28 September, 2023.
[19] "OpenAI offers to pay for ChatGPT customers' copyright lawsuits", *The Guardian*, 6 November 2023.
[20] "Microsoft announces new Copilot Copyright Commitment for customers", *blogs.microsoft.com*, 7 September, 2023.

- **Privacy:** LLMs are not only being trained on creative output with IP restrictions; they are also being trained on social media data that is in the public domain.[21,22,23,24] This is not a legal violation, it is mentioned in T&Cs, and individuals do have opt out opportunities, even if they are not always straightforward.[25] LLM creators will further argue all such data is already in the public realm and social media scrapers have been using data for marketing purposes for many years.[26] However, the novel danger could be of malicious agents mining LLMs to expose individual identities.

- **Cyber risk** has been around well before the mainstreaming of AI, and the insurance industry already offers protection against hacking and malicious actor risks (see Conclusion). However, AI does bring new vectors of online risk and attack surfaces that can be targeted by cyber criminals.[27]

- **Bias:** The most visible way to see bias expressed by LLMs is pictorially. One LLM, asked to create a secretary, created a female on 90% of occasions. For a CEO, a white male was the resulting image in 99% of cases.[28] Another example is an AI-empowered facial recognition tool that had a hard time with gender identification when it came to darker skin colours.[29] This is not just a problem in cyber space. It can also seep into real-life discrimination, such as in recruitment, persons being accused of shoplifting, and others.[30,31,32]

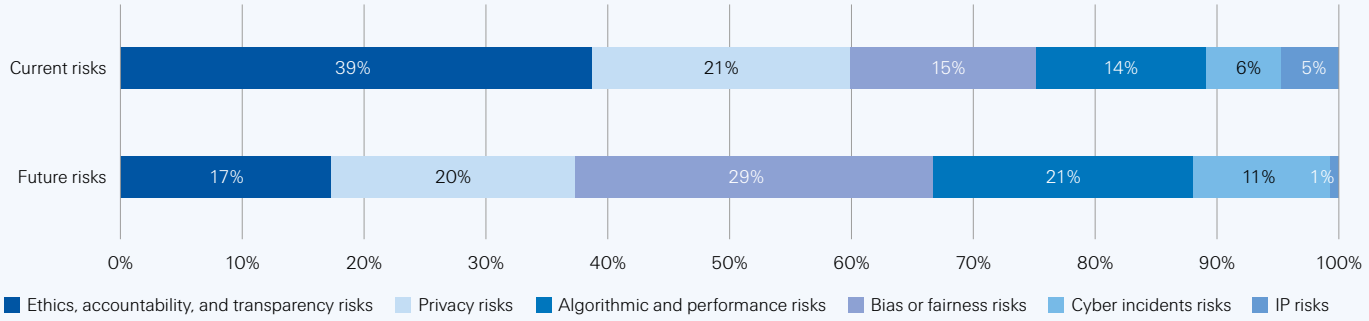
Cracking the code: AI and software development

Nowhere has AI been adopted more enthusiastically than in software development. Programming platform GitHub suggests that more than half of the programmers operating on its platform used AI to develop code in 2023, and that those who did so were 55% faster in their work. As a result, GitHub estimates, based on its own figures, that it will have added USD 1.5 trillion to the global economy by 2030.[32] This success is not without downside. Legal claims were issued against GitHub in 2022 for failure to acknowledge use of open source (OSS) code.[33] The claims were subsequently reduced, but the case remains unresolved at the time of writing.[34] Longer term, there are concerns that AI is facilitating copious quantities of code, some of insufficient quality. One researcher suggests that machine-written 'shoddy code' will create future issues that may cost a lot to correct.[35] Another study found that generative AI systems produced insecure code in lab environments, with the added danger that humans were less likely to question or examine the quality of AI code.[36]

21 "Privacy Matters: Meta's Generative AI Features", *about.fb.com*, 27 September, 2023.
22 "Google cut a deal with Reddit for AI training data", *theverge.com*, 22 February 2024.
23 "Tumblr is selling user data to train AI. Things could get weird", *businessinsider.in*, 28 February 2024.
24 "X confirms it will use public data to train AI models", *techradar.com*, 4 September 2023. X.ai announced the launch of *Grok-1.5* on 24 March 2024.
25 "AI Is Coming for Your Social Media Data: Can You Do Anything About It?", *makeuseof.com*, 5 March 2024.
26 "Social media scrapers", *apify.com*, accessed 22 April 2024.
27 "AI getting hacked – systemic vulnerabilities of a booming technology", *SONAR 2023*, Swiss Re.
28 "OpenAI's image generator shows gender bias in business roles", *newsbytes*, 29 April 2024.
29 "AI, ain't I a woman", *YouTube*, 2019.
30 "Rite Aid banned from using facial recognition software after falsely identifying shoplifters", *techcrunch.com*, 20 December 2023.
31 "Rite Aid facial recognition misidentified Black, Latino and Asian people as 'likely' shoplifters", *The Guardian*, 20 December 2023.
32 "AI hiring tools may be filtering out the best job applicants", *BBC*,16 February 2024.
33 "Sea change in software development: Economic and productivity analysis of the ai-powered developer lifecycle", *arXiv preprint*, 2023.
34 *GitHub Copilot litigation*, 3 November 2022.
35 "GitHub Copilot copyright case narrowed but not neutered", *theregister.com*, 12 January 2024.
36 "AI Is Writing Code Now. For Companies, That Is Good and Bad.", *The Wall Street Journal*, 31 May 2023.
37 "Do users write more insecure code with AI assistants?", In *Proceedings* of the 2023 ACM SIGSAC Conference on Computer and Communications Security.

Health and pharmaceuticals: skin in the game

Figure 5
Health and pharma current and future risks landscape
Overall current risks rank: 3
Overall future risks rank: 1
Spread of current and emerging risks across risk categories:



Source: Swiss Re Institute.

AI has been making its way into the health and pharmaceuticals sector for a few years, a process that is set to continue. The use cases for AI over the whole spectrum of health delivery are exhaustive, from improving and streamlining administration, to patient monitoring, to diagnosis, to drug development and many more. All told, with these numerous touch points, the potential frequency of adverse AI outcomes is high. The other half of the equation is that the risk potential is severe. With risk of bodily injury or even death, health care is a highly regulated sector with tightly controlled approval processes.

- **Cyber:** The US healthcare industry has the highest average sectoral cost of a cyber breach.[38] Causes include large attack surfaces; a high number of users; high levels of device interconnectivity; willingness to pay ransoms (high cost of downtime); and cost (and staff) required for cyber protection. AI may be able to play a role in enhancing cyber security.[39] Equally, it could create new vulnerabilities, for instance, if criminals specifically target AI-operating healthcare systems.[40]

- **Privacy:** Personal data utilised in healthcare is sensitive. More automation, including AI systems, will see more sharing of data between actors, greater vulnerability and regulators struggling to keep up.[41] However, excessively strict data privacy requirements will constrain the utility of AI systems: there needs to be a balance.[42]

- **Bias:** AI can only learn from its training data across the wide field that is medical research. If that data is (historically) biased, the results it produces will be biased.

38 "The Top 18 Healthcare Industry Cyber Attacks of the Past Decade", *Arctic Wolf*, 10 April 2024.
39 "The role of AI in Health Cyber Security", *Old National*, 20 February 2024.
40 "The Medical Industry at War Against AI Cybersecurity Attacks", *Techopedia*, 8 March 2024.
41 B. Murdoch, "Privacy and artificial intelligence: challenges for protecting health information in a new era", *BMC Medical Ethics*, 15 September 2021.
42 M. Bat et al., "You Can't Have AI Both Ways: Balancing Health Data Privacy and Access Fairly, Frontiers in Genetics", *Frontiers Journal*, 13 June 2022.

Gender bias, AI and pharmaceutical research

Health Canada concludes thus: "For many years, it was accepted that women did not differ from men except where their reproductive organs were concerned".[42] Historically, females have been underrepresented in medical trials, despite legislation.[43,44] Even animal trials have favoured males.[45] This is despite numerous studies suggesting women can and do react differently to drugs than men, along with presenting differing symptoms of illness, from mental health to cancer and many others.[46,47,48] The use of AI, particularly trained on historic data, could exacerbate bias within pharmaceutical research, particularly because AI can accelerate lengthy and costly drug development pipelines. One study in 2021 suggested that 126 of 130 medical AI devices approved by the FDA were developed using data collected prior to the development of the devices themselves.[49] To counteract gender and other biases, researchers are trying to build AI systems free of bias. At the same time, pressure groups seek to raise awareness of the issue.[50,51]

- **Performance:** Wherever deployed, AI performance failure in one stage of a value chain can have significant downstream effects in healthcare, including bodily injury or even death.

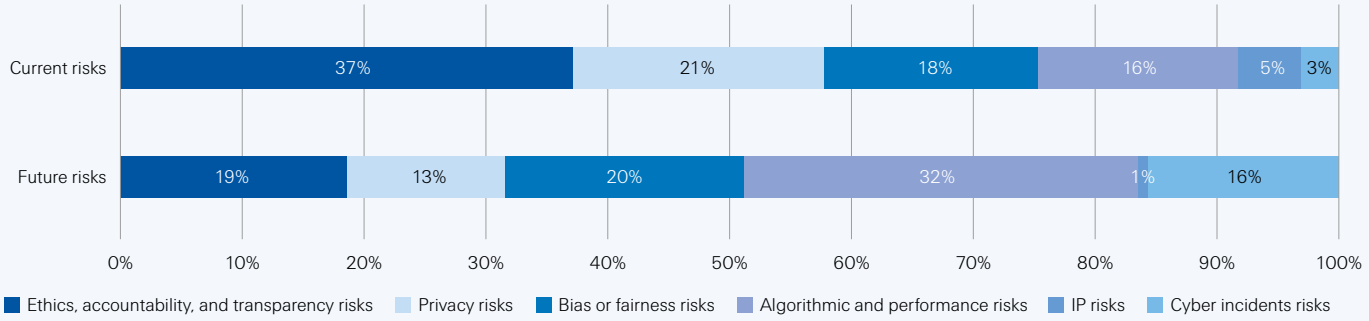
Robot doctors? AI and medical diagnoses

Despite warnings, Google has long been used for self-diagnosis.[52,53,54] Will ChatGPT replace Google? One paper found that ChatGPT 4 achieved a relative comparative score of 78.8%, describing it as exhibiting "high accuracy in symptom checking for a broad range of diseases."[55] A systematic literature review of ChatGPT's accuracy suggested it "achieved only moderate or passing performance in a variety of tests."[56] AI is further penetrating clinical diagnosis. Google's MedPaLM 540 billion parameter model scored 67.6% accuracy in a US Medical Licensing Examination, the first AI platform to pass the exam.[57] The score has since risen to 86.5%, according to Google.[58] Within radiology, studies suggest AI outperforms humans.[59, 60] However, there have also been cases of AI-driven technologies producing inaccurate or biased results,[61, 62, 63] leading one US Senator to warn against the premature deployments of AI technologies in healthcare.[64]

43 *Guidance Document: Considerations for Inclusion of Women in Clinical Trials and Analysis of Sex Differences*, Government of Canada, 2013.
44 S.E Geller, GW. Arends, A.R. Koch et. al., "The More Things Change, the More They Stay the Same: A Study to Evaluate Compliance With Inclusion and Assessment of Women and Minorities in Randomized Controlled Trials", *Academic medicine: journal of the Association of American Medical Colleges*, vol 93, no 4, 2018.
45 *Sex and gender in medicines regulation*, European Institute of Women's Health, 2017.
46 "Science experiments traditionally only used male mice – here's why that's a problem for women's health", *The Conversation*, 15 August 2013.
47 C. Kuehner, "Why is depression more common among women than among men?", *The Lancet Psychiatry*, 2017.
48 H.I. Kim, H. Lim and A. Moon, "Sex Differences in Cancer: Epidemiology, Genetics and Therapy", *Biomolecules & Therapeutics*, vol 26, no 4, 2018.
49 *Sex and gender in medicines regulation*, European Institute of Women's Health, 2017.
50 E. Wu, R. Daneshjou, D. Ouyang et. al., "How medical AI devices are evaluated: limitations and recommendations from an analysis of FDA approvals", *Nature Medicine*, vol 27, 2021.
51 "Researchers aim to ensure future AI healthcare monitoring systems are free of gender bias", *pharmatimes.com*, 6 March 2024.
52 See *Data2X*.
53 "More than half of Canadians use 'doctor Google' to self-diagnose", *Global News*, 31 July 2013.
54 "The rise of 'Dr. Google': The risks of self-diagnosis and searching symptoms online", *The Conversation*, 15 August 2022.
55 "Can this ad campaign get people in Belgium to stop Googling their symptoms?", *The Washington Post*, 2 Nov 2014.
56 A. Chen, D.O. Chen and L. Tian, "Benchmarking the symptom-checking capabilities of ChatGPT for a broad range of diseases", *Journal of the American Medical Informatics Association*, 2023.
57 J. Li, A. Dada, J. Kleesiek et. al., *ChatGPT in Healthcare: A Taxonomy and Systematic Review*, 2023.
58 K. Singhal, S. Azizi, T. Tu et. al., "Large language models encode clinical knowledge", *Nature*, vol 620, 2023.
59 MedPalm, *Google Research*, accessed 3 May 2024.
60 C.Brogan, *New AI tool detects up to 13% more breast cancers than humans alone*, Imperial, 17 November 2023.
61 "AI-Supported Mammogram Reading Detects 20% More Cancers", *breastcancer.org*, 3 August 2023.
62 "Eating disorder non-profit pulls chatbot for emitting 'harmful advice", *theregister.com*, 31 May 2023.
63 S. Jabbour, D. Fouhey and S. Shephard, "Measuring the Impact of AI in the Diagnosis of Hospitalized Patients: A Randomized Clinical Vignette Survey Study", *JAMA Network*, vol 330, no23 2023.
64 S. Rai, E.C Stade, S. Giorgi et. al., "Key language markers of depression on social media depend on race", *Psychological and Cognitive Sciences*, vol 121, no 14 2024.
65 *Letter to Google on Med-PaLM 2*, United States Senate, 8 August 2023.

Energy and utilities: Powering the AI age

Figure 6
Energy & utilities current and future risks landscape
Overall current risks rank: 2
Overall future risks rank: 3
Spread of current and emerging risks across risk categories:



Source: Swiss Re Institute.

Energy features highly in our AI risk rankings for two reasons. In the shorter run, energy incidents have potential for high severity and knock-on losses. And in the medium term, the energy sector faces radical transformation in the pursuit of net zero, with AI potentially playing a significant role.

Clean electricity is key for net zero. This requires a significant increase in the complexity of grid systems to manage intermittent renewables coming onto the grid and to allocate electricity to users efficiently. From demand management to predictive maintenance to smart forecasting, AI has the potential to significantly enhance grid performance.[66]

- **Cyber risk:** Like hospitals, energy companies have proved popular targets for cyber criminals. Possible explanations include 1) the vulnerability of energy firms to a variety of actors, from state security agencies to criminal gangs and hackers; 2) the firms present an expansive attack surface; and 3) the operational interdependency of physical and cyber assets that is characteristic of the sector.[67] Energy companies feature heavily in the "who's who" of victims to major cyber-attacks, including Colonial Pipeline, Solar Winds, and the Danish power sector.[68,69,70] The increasing use of AI will expand what the US Department of Energy describes as "novel vulnerabilities" to hostile cyber action, including poison, evasion and data extraction attacks.[71]

- **Performance risk:** AI presents two potential performance point risks: one critical and sudden, causing power outages; another gradual, causing sub-performance of electricity grids at a time when net zero requires greater efficiency. This is critical given the likely sharp increases in demand for electricity, both to facilitate the transition to net zero, and because of the energy needs of AI itself.

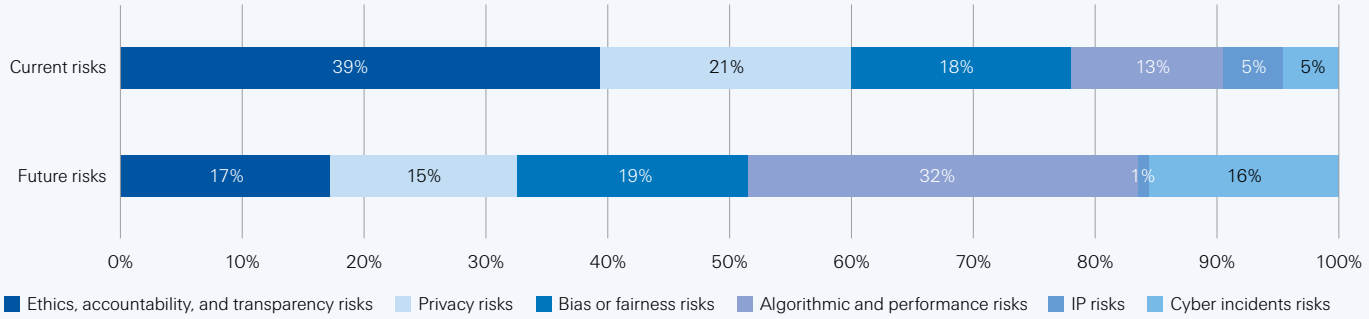
66 *Why AI and Energy are the new power couple*, International Energy Agency, 2 November 2023.
67 *The energy-sector threat: How to address cybersecurity vulnerabilities*, McKinsey & Company, 3 November 2020.
68 "What you need to know about the Colonial Pipeline hack", *Politico*, 5 October 2021.
69 "Solar Winds hack explained", *TechTarget*, 3 November 2023.
70 "Nearly two dozen Danish energy companies hacked through firewall bug in May", *The Record*, 15 November 2023.
71 *Potential Benefits and Risks of AI for Critical Infrastructure*, US Department of Energy, 26 April 2024.

Generative AI: energy monster

Whether in training or the provision of services, generative AI needs a lot of power. How much is difficult to determine, particularly because LLM administrators are reluctant to disclose associated data. The International Energy Agency suggests that data centres, AI and crypto-currencies will triple their electricity use annually by 2026 to consume the equivalent of Japan's annual electricity use.[71] One researcher estimates that by 2027, AI will consume around half a percent of total global electricity production, roughly equivalent to the Netherland's electricity use.[72] Another calculates that a generative AI enquiry can use 30–40 times more energy than a non-generative enquiry.[73] AI leaders have acknowledged this energy requirement, and some are investing in energy technology alongside AI.[74]

Mobility and transport: Risks of autonomy

Figure 7
Mobility and transport current and future risks landscape
Overall current risks rank: 5
Overall future risks rank: 2
Spread of current and emerging risks across risk categories:



Source: Swiss Re Institute.

Cars with autonomous functions are on roads across the world.[76] Further, trials of fully automotive vehicles are underway in select cities with remote human supervision – an average of 1.5 humans supervising each car, according to one report.[77] This level of human input is because the last mile is proving difficult to crack. Autonomous cars can function well in relatively closed systems such as motorways, but to date have proven less adept at the "edge" situations that can be thrown up by the open and unpredictable nature of towns and cities. There have been several well-publicised accidents and fatalities, which have shaken up the industry and led to the withdrawal of players from the sector.[78,79] In some cities, there has been a backlash against autonomous vehicles (which have proved remarkably easy to immobilise) and in some locations backtracking on the part of regulatory authorities.[80,81,82]

[72] *Electricity 2024, International Energy Agency,* January 2024.
[73] "How much electricity does AI consume?", *The Verge,* 16 February 2024.
[74] "AI already uses as much energy as a small country. It's only the beginning", *Vox*, 28 March 2024.
[75] "OpenAI CEO Altman says at Davos future AI depends on energy breakthrough", *Reuters,* 16 January 2024.
[76] *On the emerging risks of automation: the case for Autonomous Vehicles, Swiss Re,* 2021.
[77] "G.M.'s Cruise Moved Fast in the Driverless Race. It Got Ugly", *The New York Times,* 3 November 2023.
[78] D. Ingram, "Self-driving taxi startup Cruise freezes all operations after California revokes permits", *NBC News,* 27 October 2023.
[79] L. Smiley, "'I'm the Operator': The Aftermath of a Self-Driving Tragedy", *Wired,* 8 March 2022.
[80] R. Luscombe, "Driverless taxi vandalized and set on fire in San Francisco's Chinatown", *The Guardian,* 12 February 2024.
[81] D. Kerr, "Armed with traffic cones, protesters are immobilizing driverless cars» *npr.org*, 26 August 2023.
[82] A. Roy, "California lawmakers call for stricter regulation of autonomous vehicles", *Reuters,* 13 February 2024.

Autonomous vehicles: five AI performance challenges[83]

- **Coders are fallible** – Coding mistakes become amplified as systems become more complex.
- **Parameter changes** – Small alterations change learning and output parameters, such as the angle of the sun on the same stretch of road. Predictability is hard to establish.
- **Lack of information** – AI is bad at improvising if scenarios do not match training data.
- **Model drift** – If road conditions change from training data, AI may struggle and need constant updating.
- **System level challenges** – AI is programmed to stop where it can no longer resolve uncertainty. However, where it stops is unpredictable, inconvenient and potentially dangerous.[84]

Based on M.L.Cummings, "What self driving cars teach us about AI risk"

Safety authorities currently check hardware and driver behaviours. So far, no such checks exist for AI, suggesting new safety approaches are necessary.[85] Risk tolerance may also need to change given that while AI is not infallible, the reality is that US drivers contribute to over 40 000 road deaths per annum. A Swiss Re study with autonomous driving vehicle technology company Waymo showed a significant reduction in bodily injury and property damage claims in self-driving mode relative to expected baseline claims amongst the wider insured driving population.[86] Data was taken from benchmarked 3.8 million miles driven on US roads under rider-only conditions.

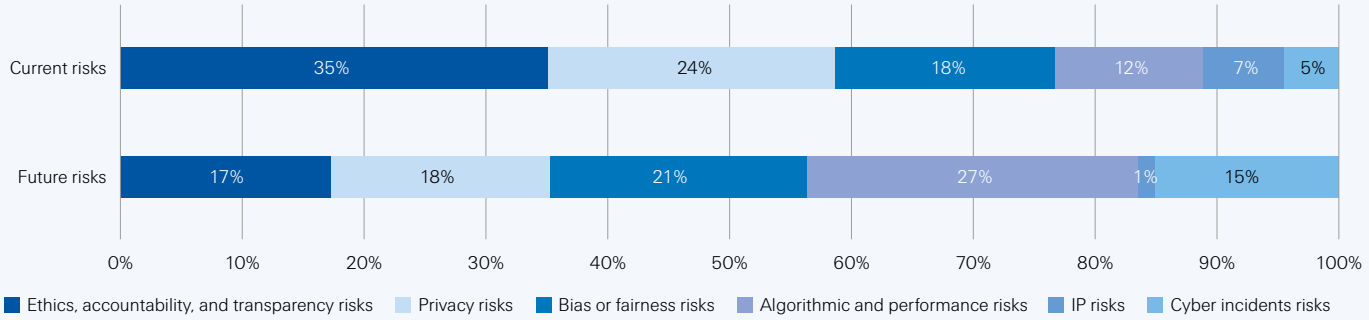
For insurers, autonomous vehicles will present many of the risks of conventional cars, such as theft, damage from weather and other natural catastrophe events, and hardware faults. However, there will also be some changes in business models:

- New risks: networked cars will be vulnerable to potential network outages or cyber-attacks
- Liability: self-driving cars will necessitate a shift of liability regimes from driver to software and ultimately the AI producer

[83] M.L. Cummings, "What self-driving cars teach us about AI risk", *IEE Spectrum,* 20 July 2023.
[84] S. Goodyear, "San Francisco robotaxi traffic jam is a warning to the world, says city official", *CBC Radio,* 16 August 2023.
[85] S. Atakishiyev, M. Salameh, H.Yao et. al., "Explainable Artificial Intelligence for Autonomous Driving: A Comprehensive Overview and Field Guide for Future Research Directions", *arxiv.org*, 2021.
[86] L.D. Lillo, T. Gode, X. Zhou et. al., "In over 3.8 million miles driven without a human being behind the steering wheel in rider-only (RO) mode, the Waymo Driver incurred zero bodily injury claims in comparison with the human driver baseline of 1.11 claims per million miles (cpmm). The Waymo Driver also significantly reduced property damage claims to 0.78 cpmm in comparison with the human driver baseline of 3.26 cpmm. "Comparative Safety Performance of Autonomous- and Human Drivers: A Real-World Case Study of the Waymo One Service", *arxiv.org*, 2023.

Media and communications: AI – intellectual property or intellectual piracy?

Figure 8
Media and communications current and future risks landscape
Overall current risks rank: 9
Overall future risks rank: 5
Spread of current and emerging risks across risk categories:



Source: Swiss Re Institute.

In media and communications, digital disruption has already transformed journalism, television, music, films and books.[87,88,89,90,91] The wave of disruption caused by generative AI could be the most significant yet and, around intellectual property, the most contentious.

Key to the debate is what constitutes "fair use" and, in a wider context, how robots learn.[92,93] Generative AI providers have scraped the internet for content citing fair use, a practice others have described as "daylight robbery".[94] Court cases are already lining up, most prominently the New York Times vs OpenAI/Microsoft, alongside others.[95,96,97,98,99] Some content providers are seeking deals with LLM hosts, which will increase the (significant) expense in training generative AI platforms.[100]

The unsolicited use of data is just one dimension of IP concerns. The output of generative AI has shown to be very close to original copyrighted materials.[101] One legal commentator suggests that if users prompt generative AI platforms to produce material close to the original, they should be liable for IP infringement.[102] If you ask an image generator for a black and white cartoon dog from the 1980s with a big nose that sleeps on top of a red kennel, you are likely to get Snoopy.

87 "The Decline of Newspapers, in Four Charts", *brookings.edu*, 23 October, 2014.
88 "The Digital Revolution Is Disrupting the TV Industry", *bcg.com*, 21 March, 2016.
89 "The Music Industry in an Age of Digital Distribution", in *Ch@nge: 19 Key Essays on How the Internet Is Changing Our Lives*, BBVA, 2013.
90 "How Netflix has changed the global entertainment industry", *businessinsider.in*, 17 April 2024.
91 *From publishers to self-publishing: The disruptive effects of digitalisation on the book industry*, *CREATe*, 2017.
92 A. Myers, "Reexamining "Fair Use" in the Age of AI", *hai.stanford.edu*, 5 June 2023.
93 M. Lemley, B. Casey, "Fair Learning", *Texas Law Review*, vol 99, 2021.
94 "Restrict AI Illustration from Publishing: An Open Letter", *artisticinquiry.org*, 2 May 2023.
95 "The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work", *nytimes.com*, 27 December 2023.
96 "Artists sue AI art generators over copyright infringement", *polygon.com*, 17 January 2023.
97 "Getty Images suing the makers of popular AI art tool for allegedly stealing photos", *cnn.com*, 18 January 2023.
98 "Universal Music Group calls AI music a 'fraud,' wants it banned from streaming platforms. Experts say it's not that easy", *cnn.com*, 18 April 2023.
99 *GitHub and Copilot Intellectual Property Litigation*, Joseph Saveri Law Firm, accessed 22 April 2024.
100 "OpenAI's news publisher deals reportedly top out at $5 million a year", *theverge.com*, 5 January 2024.
101 "Generative AI Has a Visual Plagiarism Problem", *spectrum.ieee.org*, 6 January 2024.
102 "OpenAI: 'Impossible to train today's leading AI models without using copyrighted materials'", *theregister.com*, 8 January 2024.

Accusations of plagiarism go beyond copying to also include imitation. There is (pre-digital) legal precedent that a specific style can be associated with an individual.[103] Ask an LLM to produce "in the style of" and it can create pictures, music or spoken word barely distinguishable from the real thing.[104] One US state is seeking to prevent or restrict such imitation through legislation dubbed the "Ensuring Likeness, Voice, and Image Security (ELVIS) Act".[105]

A new equilibrium is required. Generative AI can only work with massive banks of learning material and much of this will be copyrighted. The question will be what costs are incurred in reaching this equilibrium, how expensive court cases could be, and how legislators might react. AI-performance insurance currently does not cover claims relating to IP. However, it is possible that AI-driven IP claims appear in professional and cyber lines as a result of losses stemming from judicial settlements.[106]

Other sectors: Key findings

- **The more closed the AI system, the further it is from humans, the more risk is reduced.** Two examples stand out, from agriculture and manufacturing. In manufacturing, AI has the potential to replace humans in fields like inventory management and predictive maintenance. Up to 2023, the manufacturing sector worldwide had invested around USD 3.2 billion in AI.[107] AI also has the potential to increase automation in agriculture and provide analytics to enable "smarter" farming. AI risk in both these cases will focus largely on performance. Failure or underperformance can compromise output, with potentially significant downstream or upstream effects. Since the disruptions caused by the pandemic, supply chain risk has become a mainstream topic.[108] AI will likely increasingly be used in analysing and derisking supply chains.

- **Services with a high level of human interface will face scrutiny in their use of AI.** Financial services fall firmly into this category, including lending bias. One US report has suggested that with all other factors controlled, algorithms are 40–80% more likely to reject mortgage applications from persons of colour than from white applicants.[109] The Federal Reserve has warned of the dangers of such bias becoming entrenched in AI-driven lending decisions.[110] The legal profession also faces scrutiny on account of use of generative AI.[111, 112, 113] However, some suggest that *not* to use generative AI could be considered unethical, given that the American Bar Association insists members keep "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology".[114]

- **Human AI interfaces will be critical for any B2C business.** Social media has been busy making fun of how end users can manipulate automated chatbots into making poorly judged and ill-founded responses, such as agreeing to sell a car for a dollar.[115] As amusing as these cases might be, they highlight the vulnerability of LLM chatbots to opportunistic scammers or to simple mistakes. They will also raise questions as to liability. A customer dispute regarding flight prices following bereavement recently came to a US court, with the airline seeking to attribute a pricing fault provided by a chatbot to its underlying AI.[116] The court rejected the claim, insisting the airline was liable, rather than the AI provider.

[103] M. Samples, "Timbre and Legal Likeness: The Case of Tom Waits", *Oxford Academic*, 18 October 2018.
[104] "'Harry Potter' audiobook narrator Stephen Fry said AI was used to steal his voice, and warned that convincing deepfake videos of celebrities will be next", *businessinsider.com*, 18 September 2023.
[105] "Tennessee becomes first US state to protect musicians from threat of AI", *The Guardian*, 22 March 2024.
[106] "Insurers brace for claims from generative AI surge", *spglobal.com*, 12 December 2023.
[107] *6 ways to unleash the power of AI in manufacturing*, World Economic Forum, 4 January 2024,.
[108] *sigma* 6/2020: Derisking global supply chains, Swiss Re Institute, 11 September 2020.
[109] "Denied: The Secret Bias Hidden in Mortgage-Approval Algorithms", *The Markup*, 25 August 2021.
[110] "Fed's Barr Says AI Risks Amplifying Bias and Errors in Lending", *Bloomberg*, 18 July 2023.
[111] "Former Trump lawyer Michael Cohen accidentally cited fake court cases generated by AI", *theverge.com*, 30 December 2023.
[112] "New York lawyers sanctioned for using fake ChatGPT cases in legal brief", *Reuters*, 26 June 2023.
[113] "Fugees' Pras Michél says lawyer bungled his case by using AI to write arguments", *theverge.com*, 18 Oct 2023.
[114] "Could It Be Unethical Not To Use AI?" *relativity.com*, 5 January 2023.
[115] "A car dealership added an AI chatbot to its site. Then all hell broke loose", *Business Insider*, 18 December 2023.
[116] "Airline held liable for its chatbot giving passenger bad advice", *BBC*, 23 February 2024.

- **AI in the public sector has potential, but also raises challenges.** The sheer range of services provided by the state – education, defence, infrastructure, justice, public transport to name but a few – provides scale and scope for AI deployment.[117] Challenges include large (country-wide) rollout; large number of potential users and interfaces; competition with private sector for IT professionals; outsourcing and a lack of effective responsibility; a tendency to underbid and overpromise in public procurement; and the susceptibility of projects to changing political requirements. Public sector IT projects have not always been successfully implemented. For instance, the UK National Audit Office reported a "consistent pattern of underperformance" of government IT projects.[118] Moreover, the public sector is particularly vulnerable to hostile cyber actors, particularly those with state backing. This currently includes Ukraine, which has been described as a "living laboratory" of cyber conflict.[119]

[117] *The potential value of AI—and how governments could look to capture it*, McKinsey & Company, 25 July, 2022.
[118] "43 years of state IT project disasters – and they're still happening", *Campaign4Change*, 27 January 2022.
[119] What security pros can learn about AI from the Russia-Ukraine war, *SC Media*, 8 April 2024.

Conclusion: AI, risk and implications for insurers

The benefits of AI are considerable across swathes of industry. No technology, however, comes without risk. In this report, we have highlighted where vulnerabilities may exist. Providing risk protection products and services for those vulnerabilities is the business of insurers.

Swiss Re Life Guide Scout
Insurers often use AI themselves to improve operational efficiency. Very recently, Swiss Re launched the Swiss Re Life Guide Scout, a Generative AI-powered underwriting assistant, that integrates Microsoft Azure OpenAI Service to help increase the efficiency and quality of underwriting.[120]

Insurers can offer specific cover for some of the risks related to AI. One of the most rapidly growing insurance lines of recent years has been cyber risk. Swiss Re Institute estimates that USD 13 billion in cyber premiums were written in 2022, a threefold increase over five years.[121] The protection gap is nonetheless large, with cybercrime forecast to cost the global economy USD 10.5 trillion by 2025.[122] In our model, cybercrime specifically targeting AI scored somewhat lower than other risks. This is because 1) we only have limited past experience of AI-targeting attacks; and 2) our forward-looking data does not include illegal activity. If cyber criminals come to target AI systems in the same way they target non-AI digital systems, the risk could be significantly higher. One can imagine the damage that could be caused by, for example, hacking the AI of an autonomous car fleet, let alone the use of AI as a hostile attack weapon.[123, 124]

As AI becomes more widely adopted, performance risks will likely grow in severity. Though still in early steps phase, insurers have begun to offer specific coverage for AI (under)performance.

Insurance and algorithm failure
One of the latest product lines to be offered by insurers is cover for algorithmic or AI performance failures. Armilla Assurance is one such new provider.[125] Beyond AI model verification and assessment services for vendors, corporate clients and developers, in 2023, Swiss Re, Greenlight Re and Chaucer developed and supported Armilla in launching an innovative AI Performance Warranty product providing third-party coverage, indemnifying the performance of AI models.

Other risk categories may fall entirely or partly under existing insurance covers. Performance may spill over into property damage. IP infringements can fall under professional lines, which obliges insurers to follow current court cases between AI and media giants closely, a driver for our high near-term severity scores above. Data bias may lead to poor underwriting, not to mention potential regulatory and reputational risk, and the possibility of liability cases/claims. The same regulatory and reputational issues surround data privacy that may have specific coverage under cyber security policies.

Insurers can also play an important role in reducing risks associated with ethics, accountability and transparency. For instance, Swiss Re has launched Responsible Artificial Intelligence (RAI) as a service solution, an innovative approach to provide assessments of AI, machine learning and analytics models for trustworthiness, robustness, accuracy, transparency, ethical use and governance of data and AI. It can find application in multiple industries, including manufacturing (to optimise operations,

[120] *Swiss Re launches Swiss Re Life Guide Scout, a Generative AI-powered underwriting assistant,* Swiss Re, Apr 2024.
[121] *What you need to know about the cyber insurance market,* Swiss Re, 2023.
[122] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", *cybersecurityventures.com,* 13 November 2020.
[123] "AV framework advances, but what about cyber security?", *automotiveworld.com,* 19 January 2024.
[124] *The near-term impact of AI on the cyber threat,* UK National Cyber Security Centre, 2024.
[125] See *www.armilla.ai*

ensuring product quality, worker safety, and mitigating disruptions in the manufacturing process) and mobility (potential risks associated with self-driving vehicles).

A last word on insurance and AI: when we look at projections for AI growth, mentioned in the introduction as "between USD 2.6 trillion and USD 4.4 trillion" per annum, then AI will become ubiquitous across industry lines. This will bring AI into traditional insurance lines, which if it is not specifically included or excluded, could exacerbate losses. This has been described as 'silent AI risk' and has potentially serious consequences for accumulation risks in insurance portfolios. We will focus on silent AI risk in an upcoming Swiss Re Institute publication. AI may be revolutionary in many ways, but it will sometimes also be fallible. It is for insurers to consider to sustainably provide and create resilience for this emerging technology.

Additional data insights

1. Shift in the type of AI risks towards algorithmic and performance risks.

Currently, lack of ethics, accountability and transparency constitute obvious sources of risks (see Figure 9). With time, other kinds of risks will become more noticeable, driven by progression in AI capabilities as processing power and cloud computing technologies advance, and as data sets expand. For example, we expect algorithmic and performance risks to become a larger source of concern.

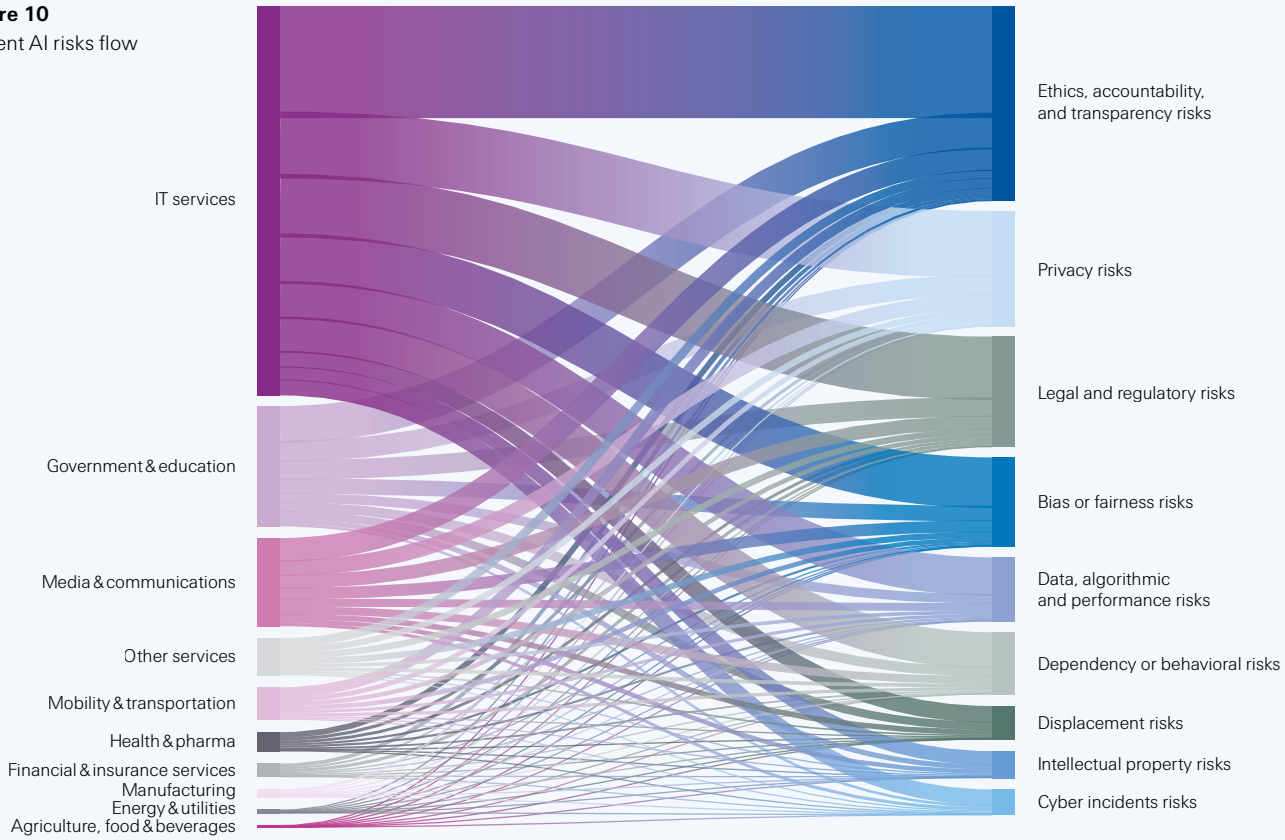
Figure 9
Risk across categories
Spread of current and emerging risks across risk categories:

Source: Swiss Re Institute.

2. Certain sectors, notably health and pharma, IT services and energy and utilities, will likely see a significant rise in the share of AI-related risks due to algorithmic and performance issues.

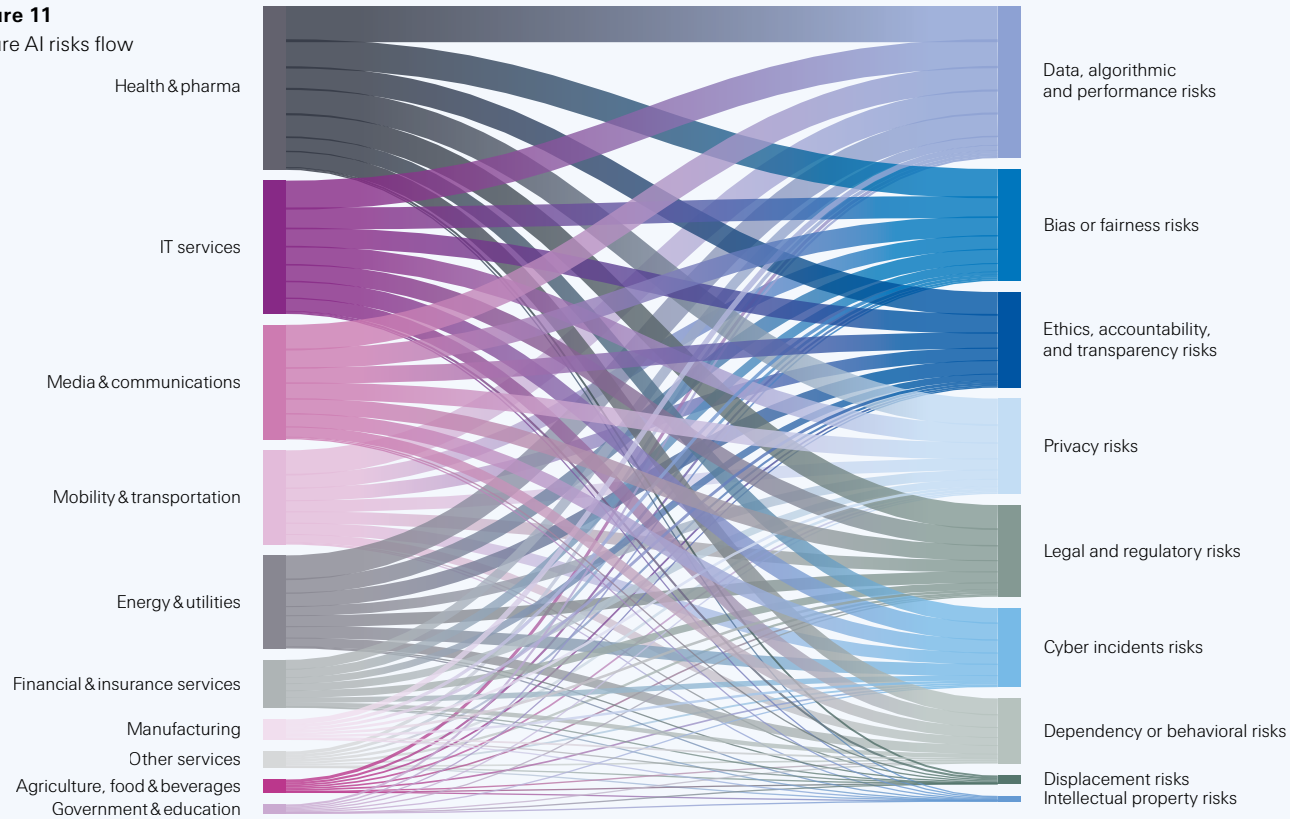
While Figure 9 provides an aggregated view of AI-related risks, Figures 10 and 11 show the current and anticipated future risk flows across industries and risk categories. The left column of both figures represents industry, and the right, risk categories. The height of the bars represents the relative risks. For example, historically IT services have had the highest AI risks, but we expect health and pharma to represent a significant portion of future risks. Why? Because rapidly expanding AI in healthcare has both potential as well as risks. Some of these emerging risks include injury to patients due to errors made by AI systems, misleading diagnosis by generative AI models, breach of patient privacy and data security, among others.

Figure 10
Current AI risks flow



Source: Swiss Re Institute.

Figure 11
Future AI risks flow

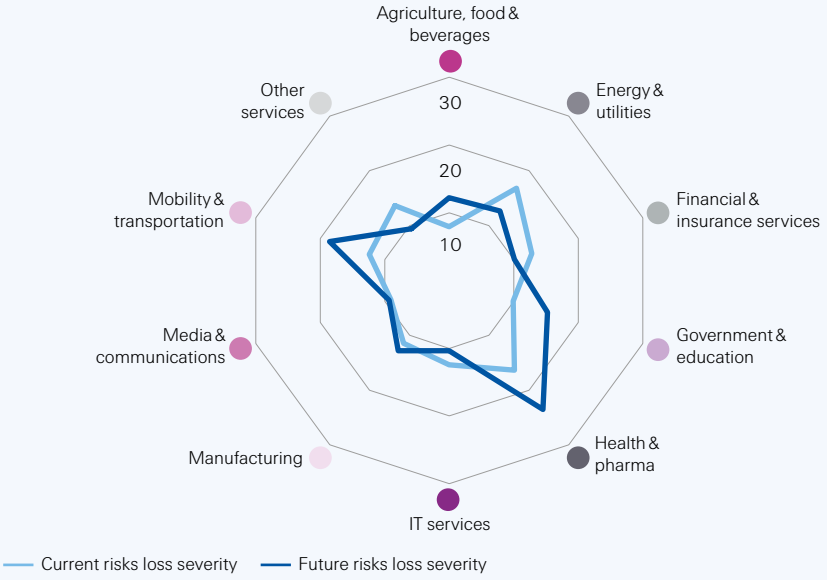


Source: Swiss Re Institute.

3. Health & pharma, and mobility & transport likely to see increases in severity scores.

Figure 12 represents potential loss severity scores. Health and pharma could have the highest loss severity in our future risks dataset (with a computed score of 23.6 as against a current score of 16.3). Mobility and transportation could likewise witness an increase in loss severity, with the sector score rising to 18.6 (future risks) from 12.4 (current risks).

Figure 12
Potential loss severity across industries



Source: Swiss Re Institute.

4. Energy and utilities severity scores could increase 10x due to cyber incidents; bias and fairness scores for health could jump 3x.

Figure 13 demonstrates the current and future loss severity matrix. Red indicates higher severity score for an industry-risk cell combination, while green indicates lower severity scores.

Some observations: there is a rise in severity for categories like bias & fairness risks and algorithmic & performance risks for health and pharma, algorithmic & performance risks in mobility, and transport & cyber incidents for the energy and utilities sector.

Figure 13
Loss severity matrix

Industry	Risk category	Bias or fairness risks	Cyber incidents	Algorithmic & performance risks	Ethics, accountability & transparency risks	IP risks	Privacy risks
Agriculture, food & beverages	Future severity score	15.7	2.4	22.2	6.8	20.5	4.1
	Current severity score	7.0	0.2	26.5	6.0	4.0	7.7
Energy & utilities	Future severity score	15.1	2.8	22.7	6.9	17.5	3.9
	Current severity score	15.8	0.2	20.4	15.4	41.2	13.8
Financial & insurance services	Future severity score	11.2	5.2	17.3	6.2	15.9	6.2
	Current severity score	11.4	7.0	23.0	12.7	19.3	8.9
Government & education	Future severity score	16.9	2.4	29.5	7.9	24.5	4.0
	Current severity score	10.6	6.1	13.0	10.9	13.0	6.2
Health & pharma	Future severity score	31.5	7.2	42.2	10.1	28.9	8.3
	Current severity score	11.4	6.8	23.1	17.9	45.9	7.7
IT services	Future severity score	13.5	1.8	20.6	6.1	16.6	3.6
	Current severity score	11.4	6.3	18.1	13.2	25.4	7.6
Manufacturing	Future severity score	14.4	2.5	23.6	6.7	20.3	4.1
	Current severity score	14.1	1.6	23.7	11.3	15.5	5.2
Media & communications	Future severity score	11.5	1.6	18.0	6.0	13.3	3.3
	Current severity score	9.3	4.0	12.8	9.2	15.2	6.3
Mobility & transportation	Future severity score	21.6	7.2	34.4	8.2	29.7	4.3
	Current severity score	11.3	9.3	20.7	12.4	29.5	4.9
Other services	Future severity score	10.8	1.2	19.2	5.8	16.6	3.5
	Current severity score	13.7	8.2	20.7	14.1	30.9	6.3

Source: Swiss Re Institute.

Appendix: data sources and methodology

Industries are heterogeneous and so are the AI risks they face. For the purpose of this report's analysis, we isolated risks into six buckets:

- **Data bias or lack of fairness**: The use of AI which results in disadvantage or differential treatment to individuals or groups of individuals, without proper justification. We further include issues related to selection or sampling, participation, geographical, confirmation and exclusion bias, among others.
- **Cyber incident risks**: In an increasingly digitally connected world, AI run models may be increasingly susceptible to adversarial attacks and data poisoning. This is a security risk where some actors can remotely force model behaviour to produce malicious results for their own benefit. Further cyber vulnerabilities could arise out of leakage of sensitive input data and information, black-box exploitation, model theft, inversion and data reconstruction. Moreover, AI could be used as an attack weapon by malicious actors.
- **Algorithmic and performance-related risks**: AI models are designed to yield a certain output and may fail to do so. Performance issues can arise from AI models when there are too many false positives or false negatives, reducing accuracy and precision of the model. Dedicated insurance products have been established to cover AI performance within specified terms and conditions.
- **Lack of ethics, accountability, and transparency risks**: An AI-driven decision may not adhere to appropriate ethical standards or codes of conducts. These risks exist in part because of the opacity and lack of explainability in many AI models; and the fact that AI has no inherent moral compass. The risk is manifested notably in (human) fields with high ethical requirements, such as law, medicine and finance.
- **Intellectual property (IP) risks**: Generative AI learning systems are hungry for training materials, and many have been fed with databases of copyrighted material. AI providers cite "fair use'", and that AI should learn as humans learn, by interpretation and impression. Lawsuits beckon, with potential insurance implications.
- **Privacy risks**: AI models can ingest large amounts of personal identifiable (PII) and sensitive personal information (SPI), and data privacy can swiftly become an issue. This could become a regulatory and reputational issue, particularly in sectors with stringent regulations. Even when data is anonymised for analysis, risk of re-identification remains. This requires consent, and should include models trained on social media. The benefits of better results using big data and smart analytics cannot be at the cost of privacy rights.[126]

Other risks exist, including legal and regulatory risks, human overdependence on AI and behavioural risks. However, we excluded these from our analysis on the grounds that they are independent and unpredictable variables, and have less direct relevance to insurance.

On these six risks, we have mapped the following 10 industry sectors:

Agriculture	**Mobility & transportation**
Energy and utilities	**Financial and insurance services**
Government and education	**Health and pharmaceuticals**
IT services	**Manufacturing**
Media and communications	**Other services (Retail, hospitality, legal)**

[126] Decoding digital trust – An insurance perspective, Swiss Re, 2022.

In order to populate the mapping of risks with industry sectors, we drew on the following historic data:

The AI Incidents Monitor (AIM), OECD	AIM identifies AI incidents reported in global media sources. The data is available from 2014 and post data cleaning, we had a database of total 13,398 incidents. An AI incident can be present in more than one risk category.

In order to better represent the fast-moving world of AI, we also take a forward data view, with our expectations guided by patent data:

PATENTSCOPE[127], World Intellectual Property Organization (WIPO)	We employed a combination of 22 AI technology terms along with industry specific keywords to classify the patents by relevant industries. A total of 41,742 AI-relevant patents (granted between January 2022 and March 2024) were used for this analysis. Text processing was used to classify AI-related risks relevant to these patents.

In preparing the model, we sought to maintain relevance for the insurance industry by capturing a view of both risk frequency/ flow and severity of incidents:

Risk flow[128]	% composition of the risk categories defined in the universe of AI incidents/patents.
Severity[129]	Potential for losses due to reasons such as physical injury, property damage, cyber breach, reputational damage and other economic factors.

To make the AI-related risks more relevant for re/insurance, we captured both risk frequency and severity of potential losses in the matrix of AI risks and industry. The risk flow mapped industry to AI risk categories. The purpose of creating these maps (as visualised in Figure 10 and Figure 11) was to check for interlinkages. We could thus, assess which industries have most risk concentration and how these risks might evolve.

[127] The World Intellectual Property Organization (WIPO) bears no responsibility for the integrity or accuracy of the data contained herein, in particular due, but not limited, to any deletion, manipulation, or reformatting of data that may have occurred beyond its control.
[128] Proxy for probability of AI related risks and frequency.
[129] As computed by loss potential.

Published by:
Swiss Re Management Ltd
Swiss Re Institute
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 2551
Email institute@swissre.com

Authors
Simon Woodward
Nikhilmon OU
Mitali Chatterjee

Contributors
Jonathan Anchen
Onur Yildrim
Luca Baldassarre
Michael Föhner
Matteo Vagnoli
Mark Muntwiler

Editor
Paul Ronke

Managing editor
Christoph Nabholz

The editorial deadline for this study was 28 April 2024.

The internet version may contain slightly updated information.

Graphic design and production:
Corporate Real Estate & Logistics / Media Production, Zurich

Swiss Re Management Ltd.
Swiss Re Institute
Mythenquai 50/60
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 3095
swissre.com/institute