LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Insurance Policies Can Cover Generative AI Risks

By **Josianne El Antoury** (October 4, 2023, 12:14 PM BST)


Josianne El Antoury

The pace of artificial intelligence technology integration into U.K. businesses is rapidly increasing and providing unquestionable efficiency benefits to businesses.

In 2022, more than 3,000 AI companies were working in the U.K., which generated more than £10 billion ($12 billion) in AI-related revenue.[1]

On June 7, 2023, Prime Minister Rishi Sunak announced that the U.K. will host the first major global summit on AI safety — a step toward making the U.K. a "world leader for AI innovation" — and one of its focuses is mitigating AI risks.[2]

At the same time as embracing AI, U.K. authorities have warned of its potential risks, such as AI-facilitated hacking and intellectual property infringement.

This article summarizes some of the U.K.'s concerns as they relate to generative AI, a new category of AI tools, and some potential insurance coverage solutions for those risks.

The takeaways are that policyholders' existing insurance policies, such as cyber, property, professional liability — particularly technology errors and omissions, and directors and officers insurance — and crime are likely to provide coverage for these new risks.

AI risks might not fit neatly into the language of these policies, and insurers may argue that exclusions or gaps in policy wordings apply.

However, after careful analysis of their existing coverages and unique AI-related risks, policyholders should consider any gray areas, including exploring new AI-focused specialty insurance products.

Generative AI Risks

On June 14, Lindy Cameron, CEO of the U.K. National Cyber Security Centre, highlighted the NCSC's commitment to "realize the benefits provided by AI." However, the NCSC warned of risks around the security of AI, such as the increasing risk of novel forms of AI-facilitated hacking.

For example, generative AI, such as large language models, or LLMs, might be used to write more "convincing spear-phishing emails" to help penetrate a company's cybersecurity defenses and promulgate mass hacking campaigns.[3] This can also lead to business data being compromised.

Other risks identified by the NCSC include businesses' IP being at risk if their staff submit confidential information into LLM prompts. IP risks around ambiguity over who owns the content created by generative AI may result in claims of IP infringement.

The U.K. government has highlighted that increasingly sophisticated AI could displace workers, which in turn can lead to disgruntled employees sabotaging AI technology — a 21st-century version of the Luddite attacks on job-displacing textile machinery at the start of the industrial revolution.

A U.K. government report in May suggests that AI could replace around 7% of jobs, particularly low-paid jobs, during the five-year period of 2021-2026, rising to around 18% after 10 years, and to just under 30% after 20 years.[4]

The malfunction of innovative generative AI tools used by professionals, such as law firms, may also result in professional negligence claims, physical loss or damage to property, or personal injury to consumers.

Traditional Business Insurance Coverage for Generative AI Risks

What existing insurance coverage is available for the new risks that may arise from generative AI?

Some examples of likely responsive insurance policies are considered below.

Cyber Policies

Cyber risk or technology errors and omissions policies may be the best fit for AI risks if an AI system is hacked or its data is compromised.

There is no "one size fits all" cyber policy, but generally, it can cover certain first-party losses to the insured business. This includes business interruption due to digital asset loss following a cyber incident and the costs for breach response experts such as IT forensics and external legal counsel.

Such policies can also cover third-party liability for data breaches.

As previously reported, cyberinsurance premiums have risen exponentially, due predominantly to the increase in ransomware attacks. As a result, some companies have been priced out of purchasing cover.[5] This trend continues, even though it may be starting to level out at current high premium rates.

For example, in the legal sector, the Law Society of England and Wales confirmed in July that only seven in 10 law firms had cyberinsurance.[6]

In 2021, the Solicitors Regulatory Authority, the regulatory body of law firms in England and Wales, excluded cyber-related first-party loss from the minimum standard terms for professional indemnity cover, which may result in a potential gap in coverage for AI risks.

For businesses that have cyberinsurance coverage, AI risks may not fit neatly into the language of those policies, and insurers may argue that exclusions or gaps in policy wordings apply.

Insurers may dispute coverage under some cyber policy wordings for brand damage caused by an AI-based antivirus tool that has been tricked by threat actors into thinking a specific type of ransomware is benign.

Property Policies

Physical loss or damage caused by AI risks would likely be covered by traditional property policies.

Property policies are generally underwritten on an "all risks" basis, covering all loss or damage except what is expressly excluded. Such policies also provide a "time element" or business interruption and extra expense cover in response to physical damage that may be caused by AI.

However, property insurers, among others, have taken steps to introduce exclusions aimed at so-called silent cyber exposures and may assert that those exclusions apply to AI-related risks.[7]

Policyholders should check their cover for such exclusions and evaluate them carefully in light of the particular AI-related functions and applications they deploy.

Professional Liability Policies

Claims for breach of IP rights and AI-generated advice might be covered by liability policies, including professional indemnity, such as those covering lawyers, media liability, and technology error and omission.[8]

Directors and officers policies also might be triggered where a claim has been made against a director or officer — in some cases an entity — for AI-related loss.

Some English law-governed policies with a liability trigger may require the insured to prove that it would have been legally liable to the third party in order to recover for settlement of a claim.

This may create difficulties for policyholders where it is unclear whether they would have been legally liable, particularly in light of the uncertainty around the application of existing regulations over AI and the difficulty of proving evidentiary issues, such as causation for the underlying claimant.

Crime Policies

The sabotage of AI technology, including by disgruntled employees, and related financial losses could be covered under crime policies, also known as fidelity coverage.

Generally, a key requirement of these policies is to prove a criminal or dishonest act, which could be challenging where, for example, an AI system itself has been subtly manipulated to become the direct perpetrator of the sabotage, or where the complexity of the AI system otherwise impedes identifying a human perpetrator.

New Insurance Products for Generative AI Risks

The insurance industry is aware of the potential for inadequate protection under existing insurance products for the full range of novel risks posed by AI,[9] and some insurers have already started promoting new AI-specific insurance products.

While it is still unclear how broadly such products have actually been implemented in the marketplace, some AI-specific products currently promoted include American International Group Inc.'s robotics shield,[10] and Munich Re's aiSure, which is aimed at vendors of AI solutions,[11] and aiSelf, which is aimed at companies developing their own AI.[12]

Other insurers have promoted enhancements via endorsements for existing policies that might otherwise exclude silent cyber. This includes Marsh McLennan's cyber catalyst forms, including its "Silent Cyber Bridge" extension[13], and Lockton's "Silent Cyber Property Solution for Businesses."[14]

Before considering purchasing AI-specific insurance policies such as these, policyholders should evaluate their current policies to understand the amount and scope of coverage currently available, including any applicable exclusions, as applied to the generative AI risks presented by their operations.

After careful analysis of their existing coverages and their unique AI-related risks, policyholders should consider any gray areas. This should be done well before renewal, leaving adequate time to develop a thoughtful strategy to negotiate clarified wording for their existing lines of coverage, explore new AI-focused specialty insurance products or both.

Josianne El Antoury is special counsel at Covington & Burling LLP.

[1] "Artificial intelligence sector study 2022" published by the Office for Artificial Intelligence and the Department for Science, Innovation and Technology, dated March 29, 2023, https://www.gov.uk/government/publications/artificial-intelligence-sector-study-2022/artificial-intelligence-sector-study-2022-ministerial-foreword-and-executive-summary.

[2] UK to host first global summit on Artificial Intelligence - GOV.UK (www.gov.uk). Press Release by the UK Government, dated June 7, 2023, https://www.gov.uk/government/news/uk-to-host-first-global-summit-on-artificial-intelligence.

[3] Lindy Cameron at Cyber 2023, Chatham House - NCSC.GOV.UK, dated June 14, 2023, https://www.ncsc.gov.uk/speech/lindy-cameron-cyber-2023-chatham-house.

[4] Report commissioned by the UK Government from consultancy firm PWC in 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1023590/impact-of-ai-on-jobs.pdf. See also the World Economic Forum's Report: "These are the jobs most likely to be lost – and created – because of AI", dated May 4, 2023, which also expects that many clerical or secretarial roles are likely to decline quickly because of AI. https://www.weforum.org/agenda/2023/05/jobs-lost-created-ai-gpt/.

[5] Law360 "How The Rise In Ransomware Is Affecting Business Insurance" April 25, 2022, https://www.law360.co.uk/articles/1485332/how-the-rise-in-ransomware-is-affecting-business-insurance.

[6] Solicitors Journal, "Law Society: 7 in 10 firms lack cyber insurance" July 21, 2023, https://www.solicitorsjournal.com/sjarticle/law-society-7-in-10-firms-lack-cyber-insurance.

[7] Covington Alert: "The Noise About "Silent Cyber" Insurance Coverage," https://www.cov.com/-/media/files/corporate/publications/2020/01/the-noise-about-silent-cyber-insurance-coverage.pdf.

[8] For example, Lloyd's launched a Technology E&O Policy for the tech sector in 2014, which provides cover for technology companies for losses caused by the failure of the policyholder's technology products or services sold to third parties. (Lloyd's launches new E&O facility for the tech sector, June 10, 2014, https://www.lloyds.com/news-and-insights/news/lloyds-launches-new-eo-facility-for-tech-sector).

[9] R. S. S. Kumar & F. Nagle, "The Case for AI Insurance," Harvard Business Review (April 29, 2020), https://hbr.org/2020/04/the-case-for-ai-insurance.

[10] AIG Robotics Shield, "End-to-End Management for the Booming Robotics Industry," https://www.aig.com/content/dam/aig/america-canada/us/documents/business/professional-liability/aig-robotics-shield-hs.pdf.

[11] Munich Re, aiSure, "Insure the performance of your Artificial Intelligence Solutions," https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/MRE_aiSure_Infographic.pdf/_jcr_content/renditions/original./MRE_aiSure_Infographic.pdf.

[12] Munich Re, aiSelf, "Insure the performance of your Artificial Intelligence Solutions," https://www.munichre.com/en/solutions/for-industry-clients/insure-ai/ai-self.html.

[13] Marsh Cyber Catalyst, https://www.marsh.com/us/services/cyber-risk/products/cyber-catalyst.html.

[14] "Lockton Launches Silent Cyber Property Solution for Businesses", Insurance Journal (October 20, 2021), https://www.insurancejournal.com/news/international/2021/10/20/638002.htm.