



COVERAGE INSIGHTS

Provided by Connor & Gallagher OneSource

How AI Is Changing Commercial Insurance

The past few years have seen a rapid expansion in artificial intelligence (AI), with many businesses leveraging this technology to automate workflows and administrative tasks, analyze vast amounts of corporate data, and enhance customer service offerings. However, as more businesses integrate AI-powered tools into their operations, this technology is also posing unique exposures.

Complicating matters, many standard commercial insurance policies were written before the widespread adoption of AI. In response, a growing number of insurers have begun updating policy language and, in some cases, introducing certain coverage exclusions for AI-related risks. Consequently, businesses that neglect to review these policy changes could face considerable coverage gaps and unanticipated out-of-pocket losses when claims arise.

This article provides more information on common AI-related exclusions in the commercial insurance landscape and offers associated guidelines for policyholders to keep in mind before renewal.

Common AI-related Exclusions

Exclusions for AI-related risks have emerged across several lines of coverage in the commercial insurance space, including the following:

- **Commercial general liability (CGL)**—In recent years, many liability policies were largely “silent” on AI-related exposures, making the extent and scope of coverage for such losses relatively ambiguous. Effective January 2026, the Insurance Services Office (ISO) introduced multiple

generative AI exclusion endorsements for its CGL coverage forms. Since most insurers utilize ISO-based forms, carrier adoption is expected to increase steadily throughout the CGL segment. In practice, these endorsements may exclude coverage for third-party bodily injury, property damage, and personal and advertising injury losses stemming from generative AI outputs.

- **Professional liability/errors and omissions (E&O)**—Alongside the rising prevalence of exclusion endorsements for AI-related risks in the CGL space, the E&O segment has demonstrated some of the most aggressive exclusion activity toward these exposures. In particular, some insurers have introduced broad exclusions that eliminate or significantly restrict coverage for losses tied to AI-powered professional services or advice. This is especially concerning for businesses that leverage AI tools (e.g., chatbots) in client-facing operations.
- **Directors and officers liability (D&O)**—In the D&O space, some insurers have started implementing exclusions for certain AI-related exposures and using more restrictive policy language regarding AI governance risks. One of the top concerns in this segment is claims stemming from AI-washing, in which companies are accused of overstating or otherwise misrepresenting their AI usage or the capabilities of this technology to investors and the general public. As a result, insurers are placing greater scrutiny on AI-related disclosures during the underwriting process, and policy language may continue to evolve to address these risks.



How AI Is Changing Commercial Insurance

- **Fidelity and crime**—Standard fidelity and crime policies generally exclude coverage for cyber fraud, particularly for social engineering attacks that involve honest employees being manipulated by cybercriminals into transferring company funds to external accounts. This exclusion also applies to AI-enabled fraud, namely deepfake plots and business email compromise scams, as these incidents usually don't qualify as "direct theft" under traditional policy terms. To combat these exposures in the fidelity and crime space, businesses may need to purchase social engineering or fraudulent instruction endorsements. Even then, specific coverage capabilities will depend on the nature of the incident and the type of fraud involved, with some insurers implementing strict sublimits and security requirements.
- **Cyber**—Unlike other lines of coverage, insurers in the cyber segment are largely affirming rather than excluding claims stemming from AI-driven losses. While businesses may still need to secure endorsements for certain events (e.g., social engineering schemes), standard cyber policies typically cover losses resulting from cybercriminals using malicious AI programs to penetrate corporate networks, expose confidential data or deploy automated ransomware attacks. Nevertheless, cyber insurance does not apply to bodily injury and property damage losses, which could leave businesses with ongoing coverage gaps if their other policies fully exclude AI-related risks.

Guidelines for Policyholders

In light of these evolving exclusions, it's critical for policyholders to review their coverage before renewal and take steps to prevent potential gaps. Here are some key guidelines to consider:

- **Document and disclose AI usage.** Businesses should conduct a detailed inventory of their AI usage across their operations, including standalone tools and those embedded within third-party software platforms. This inventory

should be well-documented and shared with insurers during the underwriting process. Failure to disclose the full extent of AI usage could give insurers grounds to deny associated claims or rescind coverage moving forward.

- **Review policy definitions and limitations.** Rather than focusing solely on the declarations page of their policies, businesses should carefully review these documents in full, especially the exclusions section, for AI-related restrictions that might otherwise be missed. Businesses should also note how AI is defined in their policies to determine whether this language is broad enough to cover losses stemming from routine or incidental AI use. When applicable, businesses should request copies of any AI-related endorsements for their CGL, E&O, D&O and other liability policies, thereby ensuring full comprehension of what is and isn't covered.
- **Explore additional coverage options.** Businesses should never assume they have sufficient coverage for AI-related exposures just because their cyber policies affirm these losses. Cyber insurance rarely fills other liability coverage gaps, especially for businesses with significant E&O exposures. Businesses struggling to secure adequate protection against AI-related risks under standard commercial policies should consider purchasing specialized AI liability coverage. Yet, it's worth noting that these offerings are still evolving and remain somewhat limited. In any case, businesses can consult trusted insurance professionals to discuss their unique coverage needs.

Conclusion

As AI continues reshaping business operations, its insurance implications grow increasingly complex. Policyholders must proactively review their coverage, disclose AI usage and work with insurance experts to remedy ongoing gaps before they become costly surprises. Staying informed and adaptive is the best defense against future AI-related claims. Contact us today for additional insurance guidance.