A GUIDE TO AI RISK & INSURANCE

ASSESSING CLAIMS, COVERAGE AND THE INSURANCE MARKET

GB&A

White Paper
October 2026

Navigating A Challenging Risk Environment

The large-scale implementation of artificial systems has created a challenging risk environment. In addition to risk uncertainty, potential unrecognized liabilities and confusion pertaining to best practices regarding controls and oversight, policyholders must navigate a complicated insurance marketplace which can be equally daunting, especially as reactions from insurers diverge.

Some carriers have filed AI exclusions, others have remained silent, and a growing number have affirmed coverage, either through endorsements, or stand-alone AI policies. Understanding the true scope of coverage under each of these approaches, and where the liability lines are being drawn however, is proving equally challenging.

Disclaimer: The data, figures and policy terms cited in the below report are based on insurer responses, surveys, policy assessments, and interpretations of public databases as of October 2026. Accordingly they are subject to change, and may contain errors. None of the below should be construed as legal advice – please refer to any applicable policy and/or review with your appointed broker or counsel.

Contents

I	AI Claim Frequency & Coverage Under Existing Policies	p 04
II	Assessing Coverages	p 06
III	Coverage Under Legacy Policies	p 11
IV	Policy Exclusions and Insurer Response	p 14
V	Additional Coverage Considerations	p 16
VI	Exclusions & Problematic Terms in AI Policies	p 17
VII	About GB&A	p 19

2026 At A Glance

Risk Statistics

88%

of organizations regularly use AI in at least one business function, according to Stanford HAI's 2026 AI Index

36%

of companies report an AI incident or failure causing a material negative impact, according to a recent EY study

150%

increase in AI policy exclusions filed by admitted insurers from 2025 to 2026

38

states enacted AI laws across 2025–26, with 28 laws in California alone

23

enacted state laws focus on disclosure (chatbots and AI labels), the most common category

4 of 8

endorsed tech E&O / cyber policies contained LLM jacking endorsements, but only 2 provided meaningful coverage

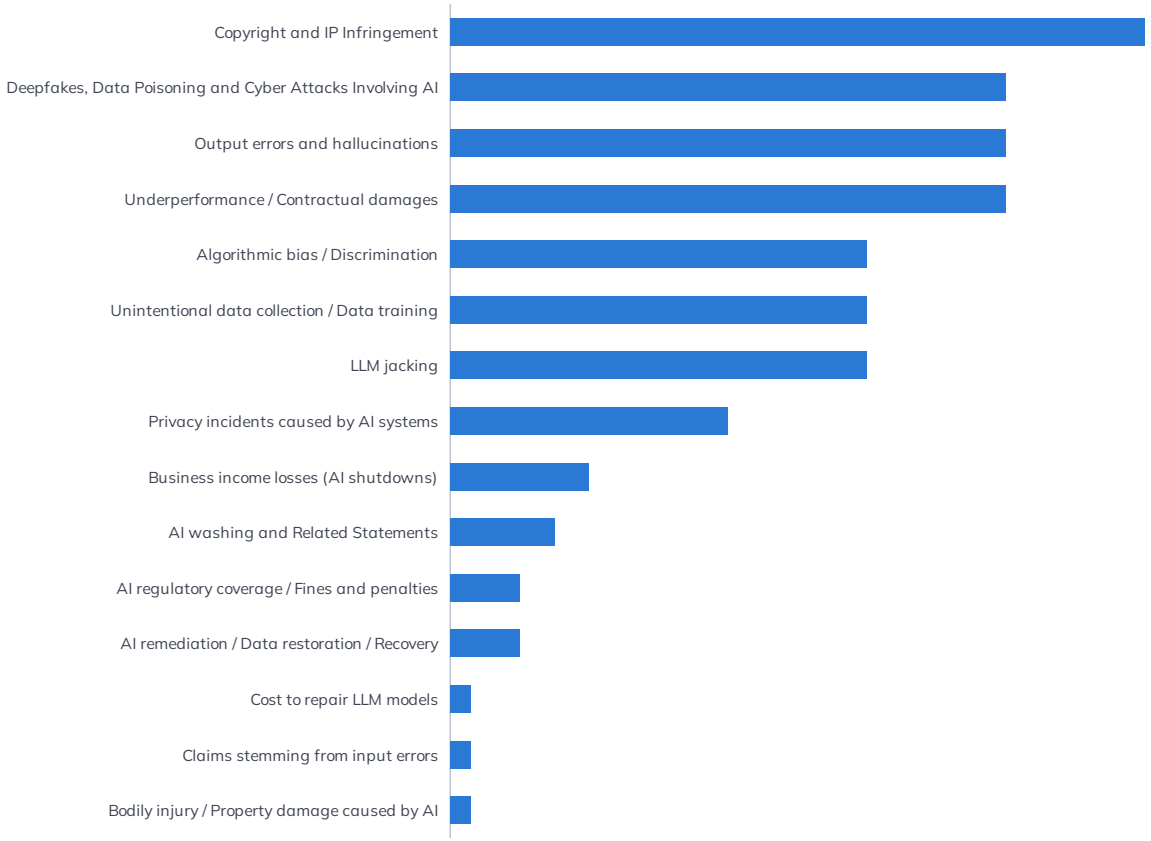
Most common AI claim types

1. Copyright and IP Infringement
2. AI-Driven Cyber Incidents
3. Output Errors and Hallucinations

AI Claim Frequency & Coverage Under Existing Policies

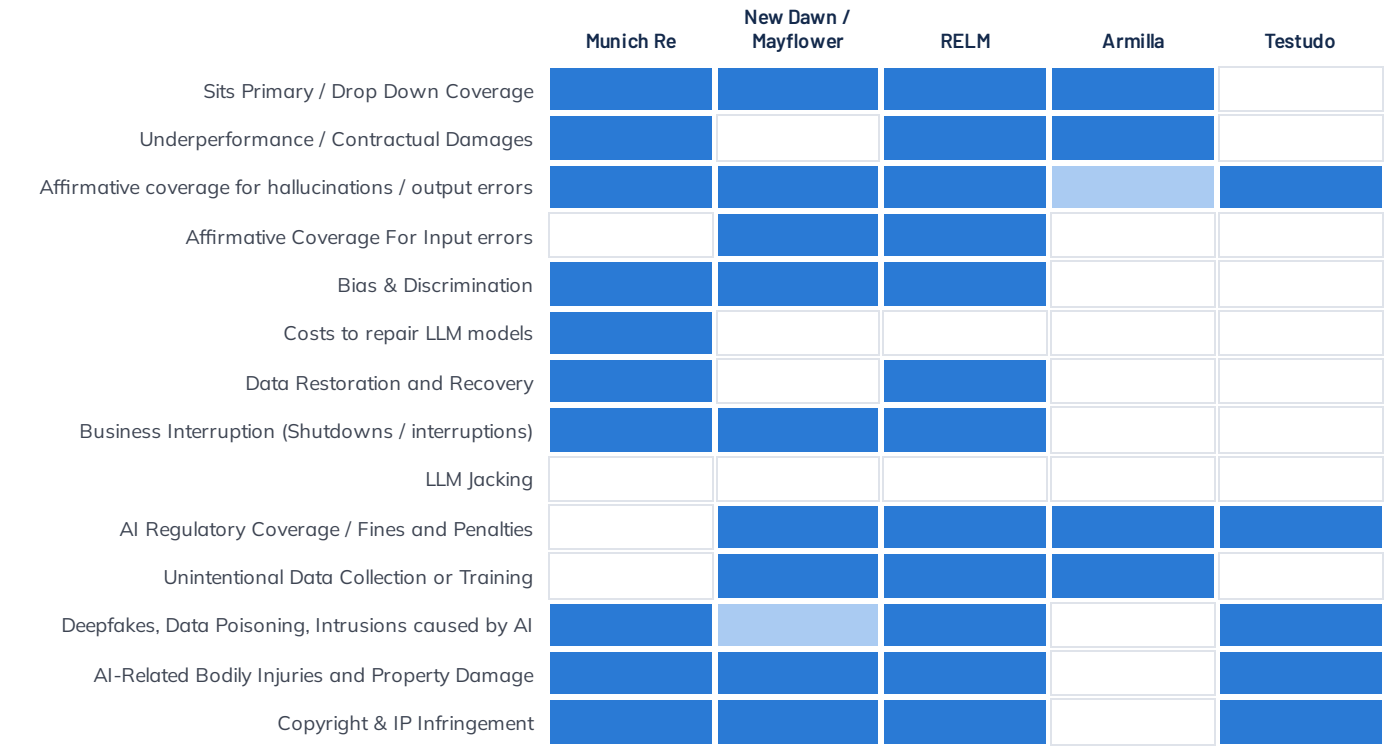
Claim frequency by loss / damages type

Relative frequency of AI-related claims, from most to least common



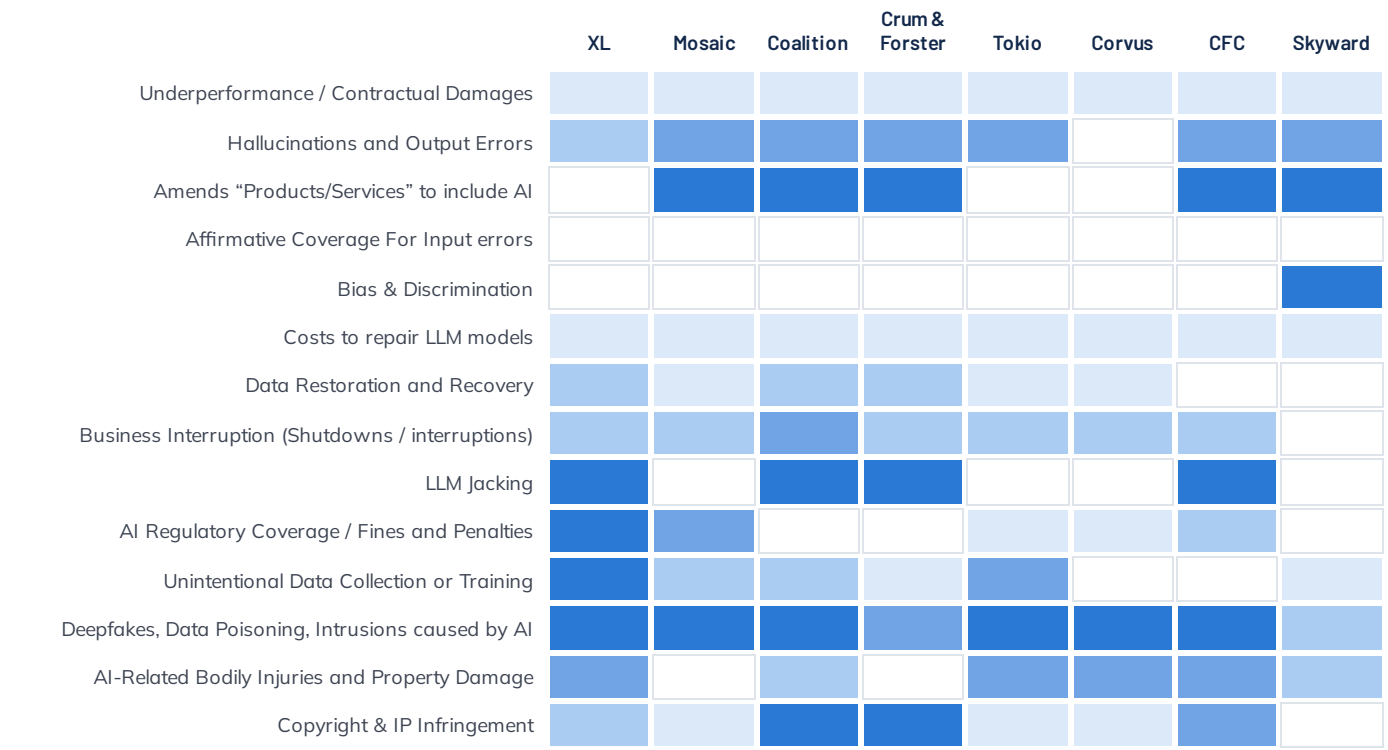
AI coverages provided by stand-alone carriers

Covered | Possibly covered | Excluded or policy forms not located



AI coverages provided by endorsed tech E&O / cyber policies

Covered | Possibly covered (darker = stronger indication) | Excluded or not located



Assessing Coverages

Underperformance and Contractual Liabilities

Claims alleging AI systems or language models underperformed can create coverage challenges under standard tech E&O policies, as it can be unclear if the allegations actually meet the policy's definition of "wrongful act". Additionally, contractual damages stemming from guaranties or warranties are generally uninsurable under standard E&O policies. Some AI policies provide coverage for claims alleging that artificial systems and models failed to perform within their margins of error, affirmatively covering the resulting contractual liabilities that may arise.

To set performance parameters when applying for coverage, many carriers will require completion of a drift model questionnaire to define "normal" model drift. Such policies may also contain lengthy requirements mandating the continuous monitoring, upgrading and maintenance of AI systems. Similar to dual authentication requirements pertaining to fraudulent funds transfer coverage, when such requirements are overly broad they can ultimately limit the usefulness of insurance.

> "
>
> Contractual damages related to guaranties or warranties are generally uninsurable under E&O policies.

Affirmative Coverage for Output Errors & Hallucinations

In contrast to claims alleging underperformance which allege a product is systemically failing to perform as intended, claims arising from output errors or hallucinations would be interpreted as isolated events causing financial damages to a client or 3rd party. According to litigation databases, law firms and attorneys are the most frequent defendants in cases involving hallucinations, driven by errors in citations and case law.

Since such claims stem from more isolated errors, resulting in financial harm, these claims are more likely covered by standard E&O policies (assuming there are no AI exclusions). For developers, there is still however a grey area – insurers could hypothetically try to argue that hallucinations or output errors are not actually product failures if the AI model was in fact operating within its margin of drift error. In order to provide added clarity and satisfy modern contract requirements, a number of tech/cyber carriers have available endorsements which amend the definition of tech products and services, to include artificial systems. While this is a nice enhancement, it really does not extend any new coverage and likely doesn't solve this potential coverage issue. Stand-alone AI policies also actually go one step further and explicitly cover output errors and hallucinations, which does a better job at affirming coverage.

Another simple solution that may help extend coverage is simply modifying any definition of professional services to specifically include services "provided by AI systems".

Algorithmic Bias & Discrimination

Claims involving algorithmic bias and/or discriminatory outputs most commonly arise when artificial systems are used for:

- **Recruiting and hiring** – where AI models discriminate against applicants based on age, race or gender. There also appears to be an emerging trend of litigation trolling where prospective applicants submit an application solely to detect if AI was used as a basis for declining the application, after which litigation is filed.
- **Facial recognition** – where systems may be less efficient at detecting certain racial or gender features. Additionally, AI may expose organizations (knowingly or unknowingly) to biometric data collection claims.
- **Medical diagnostics** – where data may be skewed, disadvantaging certain genders or races.
- **Pricing of services** – where AI may produce discriminatory pricing models.
- **Extending of credit, insurance, housing or healthcare** – where it may be alleged that AI inadvertently discriminated against applicants.
- **Generative AI media** – which may produce discriminatory texts or images.

When AI policies/endorsements do extend affirmative coverage, coverage terms should be carefully reviewed – some policies limit coverage solely to any resulting regulatory actions, effectively omitting 3rd-party claims. A number of policies also require strict controls as a prerequisite to coverage. With a number of statutory laws and regulations addressing bias/discrimination within AI systems and models, policyholders should also attempt to secure affirmative coverage for any resulting regulatory proceedings, fines and penalties. Any claim involving AI-related bias/discrimination should also be tendered to existing EPLI policies (as discussed below).

Unintentional Data Collection & Training

Data scraping, and the use of AI chatbots and voice-transcription services are among the leading causes of unlawful data collection claims. In some cases, these claims can also arise from data collection/use by 3rd-party vendors, underscoring the importance of 3rd-party governance. Over the past few years, largely in response to pixel tracking litigation, an increasing number of cyber carriers have begun to attach data collection exclusions, which can negate coverage for AI-related data collection claims. The majority of these claims should qualify for coverage under a standard cyber/E&O policy assuming there is no explicit exclusion.

When insurers do provide affirmative AI coverage, terms need to be assessed carefully. Coverage may be limited to defense costs only, sub-limited, and/or subject to the policy's standard conduct exclusions, limiting or negating coverage when the policyholder acted with intent.

Review the definition of "protected info"

Where coverage for unlawful collection or training is limited to "protected info", the definition should be reviewed. Does it include corporate confidential information and information subject to an NDA? Is biometric data included or excluded? Some affirmative AI carriers will further broaden their definitions to include training involving media (such as AI-generated text or images).

LLM Jacking

Malicious actors are increasingly exploiting stolen AI credentials in order to run AI models, generating significant token usage bills for organizations. These claims are becoming one of the leading causes of loss involving AI systems and have the ability to inflict losses in the hundreds of thousands. They are also poorly covered by existing cyber policies and generally wouldn't qualify for coverage under any utility fraud or crypto-jacking endorsements. Some carriers have responded by providing (often sub-limited) endorsements affirmatively covering LLM jacking, however some of these endorsements can be misleading.

> "While the main costs associated with LLM jacking are the increased token/usage charges, not all LLM jacking endorsements actually cover this risk.

Some endorsements currently circulating limit coverage solely to increased utility costs or internet access costs as a result of LLM jacking – AI token usage costs don't necessarily fit the definition of "internet access costs". Other policy forms explicitly include coverage for cloud computing, software, SaaS, PaaS, IaaS, and artificial intelligence system costs. Coverage for such damages may however still be limited to usage where there was a written contract in place prior to the LLM jacking loss.

AI Regulatory Proceedings, Fines & Penalties

Currently, most AI regulatory proceedings are isolated to actions brought by the SEC, DOJ and FTC involving AI washing, claims alleging fraud, and actions brought against large frontier providers. Despite the fact that AI-specific regulatory claims are currently rare, emerging statutes are moving fast with a number of new bills taking effect in 2027. Policyholders should anticipate an increase in activity in the coming years.

Coverage for AI proceedings is still one of the more useful enhancements provided by AI-affirming endorsements. While most enforcement actions involving privacy violations would already likely qualify for coverage under a standard cyber policy, there is often no coverage for proceedings involving emerging AI wrongful acts such as failure to label AI-generated media, failure to disclose usage of AI chatbots, or violations stemming from algorithmic bias. Additionally, standard E&O policies often lack coverage for regulatory proceedings and any resulting fines or penalties.

When extended by affirmative AI endorsements, coverage is almost always sub-limited, however these enhancements can be particularly valuable for (non-privacy-related) AI regulatory proceedings, fines and penalties. Interestingly, in contrast to most stand-alone AI policies that limit coverage to formal inquiries only, most AI endorsements impose no such requirement.

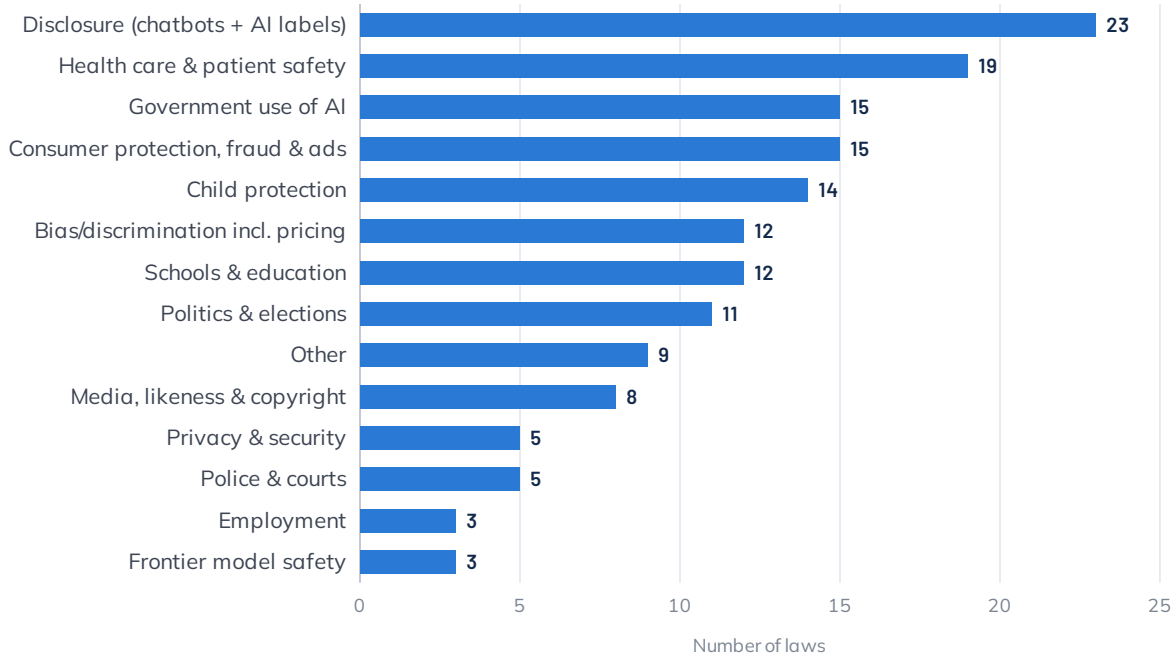
What to look for

- Language applying the most favorable jurisdiction when determining the insurability of fines and penalties.
- Most insurers use the EU AI Act of '24 as their reference for regulatory violations; any policy affirming coverage should extend to "similar domestic and foreign laws or regulations".
- Whether coverage is limited solely to formal regulatory actions, or extends to any regulatory proceedings/inquiries.

Emerging statutes are moving fast

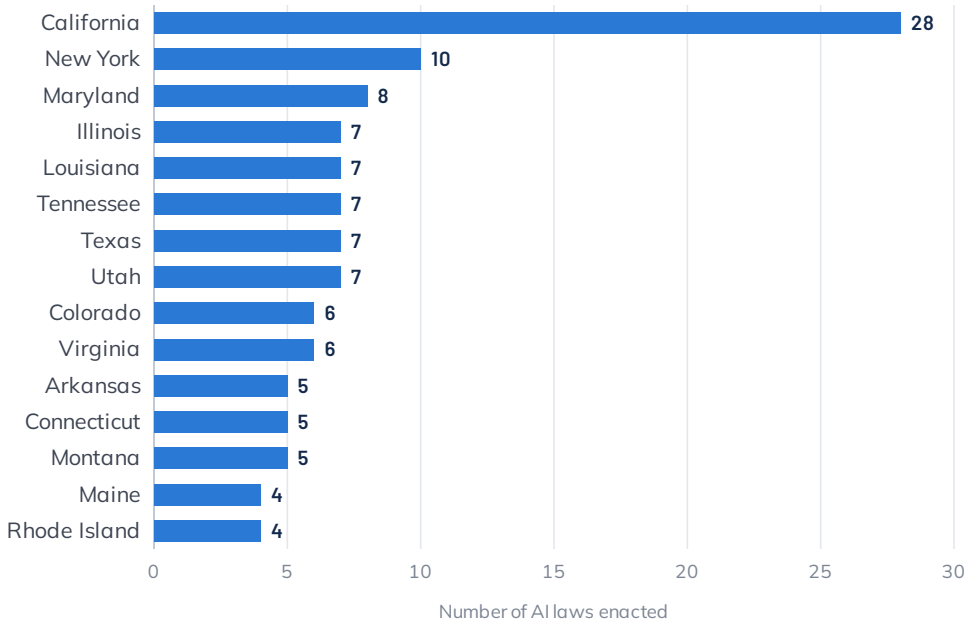
Enacted US state AI laws by main focus, 2025–26

154 laws, each counted under one main topic



Top states by AI laws enacted, 2025–26

House and Senate twin bills counted once; 156 state laws in total across 38 states



> AI-driven business email compromise attacks are largely viewed as a leading cause of cyber losses over the next few years.

Business Income Loss and LLM Restoration Costs

Business income losses (and resulting data restoration) can be caused by a range of losses, from data poisoning by malicious actors, to outages of AI systems/language models, and/or the need to preventatively shut down artificial systems due to recognition of excess model drift or flawed outputs that require immediate remediation.

When such losses occur as a result of an intrusion or malicious actors, resulting damages should be covered by most cyber policies, however policy definitions of networks, systems, data, and business income/extra expense need to be reviewed carefully. Preventative shutdowns may also be covered by standard policies, but only to the extent that an identified AI malfunction is in danger of causing a privacy event.

Companies that suffer business interruption losses as a result of an AI provider being taken offline may also qualify for contingent business interruption coverage, to the extent that the provider's network interruption was the result of an intrusion or cyber event. Coverage for preventative shutdowns (resulting in lost income) solely to repair excess model drift or other biased or flawed outputs, however, can currently be difficult to secure and would almost surely be limited to specific endorsements provided by separate AI policies.

AI-Driven Cyber Attacks

Malicious actors are regularly utilizing AI to aid in their attacks, resulting in more frequent, effective intrusions. AI-driven business email compromise attacks and deepfakes are among the most common attacks and are largely viewed as a leading cause of cyber losses over the next few years. The potential for threat actors to use AI to steal voice imprints may also result in an increase in fund transfer fraud claims, highlighting the importance of broad crime policies.

Some AI policies and endorsements are now affirming coverage for cyber and privacy incidents that utilize AI – the most common being endorsements that: clarify that deepfakes are included as a defined cause of loss and endorsements affirming that intrusions that result in "data poisoning" among models are covered.

While these endorsements may provide some added comfort, or help to satisfy contractual requirements, they are likely redundant, as any such intrusions should already be covered by non-endorsed cyber policies. Underlying policy terms should always be reviewed however, in order to ensure coverage is intact.

Coverage Under Legacy Policies

Employment Practices Liability Insurance

As organizations and their HR departments increasingly implement AI to aid in recruiting, hiring and other employment decisions, EPLI policies are becoming increasingly important – particularly to address any bias/discrimination that may be alleged in the course of making those decisions. While most EPLI policies are "silent" on the issue of AI-related losses, standard policies should respond to such claims.

EPLI policies can also help protect against AI-specific regulatory violations, such as the recently amended NY WARN Act, requiring companies to indicate whether mass layoffs were driven by implementation of AI systems. Employment practices liability policies providing 3rd-party coverage may also fill gaps in underlying policies that may not provide coverage for claims involving bias, such as allegations made by clients or customers alleging discriminatory pricing. This can however be a nuanced area for coverage, as any EPLI policy providing 3rd-party coverage would also need to be assessed for any price discrimination exclusions, and those related to actions brought by the FTC (among others), which can severely restrict coverage.

Intellectual Property Defense / Abatement Insurance

Intellectual property insurance is one of the more overlooked insurance products when structuring programs. In addition to providing defense cost coverage for claims alleging patent or copyright infringement, it can help organizations protect against claims alleging theft of trade secrets (such as source code and datasets) which can often arise when hiring employees away from competitors. While some D&O policies may also respond to such claims (depending on policy language), specific IP policies can help fill any policy gaps.

Specific IP Abatement policies may also help fund legal costs related to pursuing infringers of a company's own IP. It should be noted however, that IP protections in the context of LLMs and artificial systems are very nuanced and counsel should always be consulted before assuming any protections.

> "
> IP insurance is one of the more overlooked insurance products.

Directors and Officers Insurance

Management liability claims related to the use of AI are increasing, however most of the litigation appears to be (mostly) isolated to actions against public companies. While claims against private companies are possible and have been filed, they currently appear to be rare in the private sector. The most common allegations stem from:

- AI Washing (over-stating a company's AI capabilities)
- Under-stating risks/security and Lack of oversight/controls
- Breaches of Fiduciary Duties
- Shareholder dilution resulting from subsequent raises needed to fund capital expenditures, and allegations of corporate waste
- AI follow on litigation (following IP or cybersecurity claims, etc)
- Allegations of inadequate AI disclosures, such as those pertaining to other product lines being cannibalized, loss of competition, or increased AI costs.
- Lastly, D&O may also fill gaps in regulatory coverage, particularly for regulatory proceedings asserted against insured persons

Some stand-alone AI carriers, are actually extending a degree of management liability coverage which can be triggered by certain shareholder actions and/or regulatory investigations, but D&O insurance should be an organization's first step in securing coverage for such claims.

Most D&O carriers are not attaching AI specific exclusions at this point, however there are a number of already existing policy terms/exclusions that can jeopardize coverage, namely; contractual, professional service, cyber, intellectual property, and product defect exclusions.

The extent to which these exclusions can negate coverage will largely depend on

1. Whether it applies to the entity only (or extends to claims against insured persons as well)
2. Whether the exclusion contains any carve-backs, such as those for shareholders, non-indemnifiable claims, or defense costs
3. The breadth of the exclusion's preamble. Language excluding coverage for claims "arising from, or in any way related to" the exclusion can effectively preclude coverage for follow-on litigation brought by shareholders following an AI failure

Exclusions Most Likely to Be Implicated in D&O Policies

Contractual Liability Exclusions

Professional Service Exclusions

Cyber & Privacy Exclusions

Intellectual Property Exclusions

Product Defect Exclusions

Bodily Injury & Property Damage Exclusions

While not an exclusion in and of itself, the definition of "insured persons" should also be carefully reviewed – particularly on public company D&O policy forms. According to recent surveys, approximately 40% of companies have implemented specific Chief AI officers, underscoring the importance of ensuring coverage will in fact extend to such individuals (particularly when they are not considered to be duly appointed). In order to affirm coverage for such insured persons, some public company D&O forms have implemented expansive definitions of insured persons to include a wide range of "tech officers". Below is an example of one such definition pulled from a major public company D&O insurer.

"Insured person shall include the chief information officer, chief information security officer, chief technology (or technical) officer, chief privacy officer, chief digital information officer or chief digital officer of the Company, and any other senior-level executive of the Company:

i. who oversees the Company's information, cyber and technology security;

ii. who oversees the Company's technology infrastructure, products and services;

iii. who oversees data privacy for the Company; or

iv. who is responsible in whole or in part for the Company's collection, use, storage, deletion, security, publication or other disclosure of digital information and/or the Company's use of advanced technologies, such as the cloud, artificial intelligence, machine learning, automation, internet of things, mobile and social media"

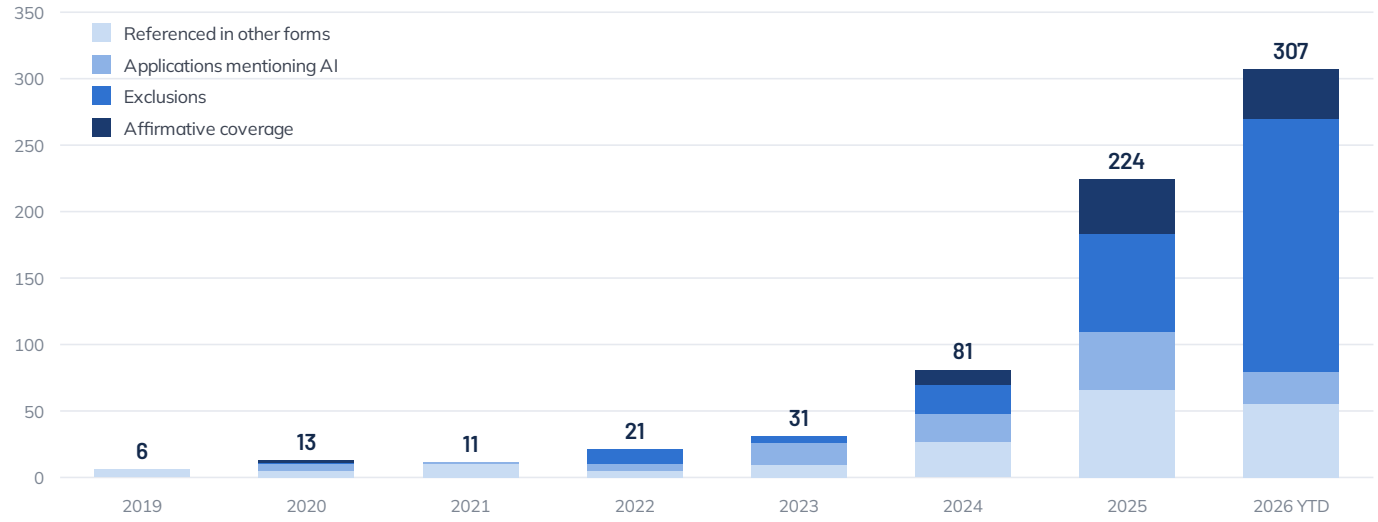


Policy Exclusions and Insurer Response

The below infographic was provided by FilingFocus, a company that tracks the insurance filings of admitted carriers. While it demonstrates an obvious trajectory by insurers, the data is often misinterpreted.

AI language in admitted policy forms, 2019–2026

Number of admitted insurance policy forms referencing AI, by type of language



Source: FilingFocus. 2026 YTD as of October 2026.

While carriers are undoubtedly filing an increased number of AI exclusions, only a small handful have actually been implemented. What this chart does however demonstrate is the concern among the market and carrier preparedness. While AI-specific policy exclusions remain rare, insurers are asking more questions on applications and have proactively prepared by filing forms which can be readily deployed. Another interesting takeaway from this data is just how much exclusionary filings have outpaced affirmative coverage filings, which would indicate more concern than optimism and/or coverage opportunities for carriers.

Of the small handful of AI-specific exclusions that have already been implemented on policy forms, those in use can be extremely problematic and overreaching. To demonstrate their problematic nature, consider the exclusion on the following page and the issues it poses when attached to a professional liability policy.

*The insurer will not defend any claims, **based upon, attributable to, arising out of, or related to, in whole, or in part**, any use of artificial intelligence, including but not limited to:*

*a. Errors, omissions, or inaccuracies in the programming, functioning or **decision making** processes of artificial intelligence systems*

b. Bodily injury, property damage, or economic loss caused by, or resulting from the actions or decisions of artificial intelligence systems

c. Claims related to data breaches, privacy violations, or cyber incidents caused by the use of artificial intelligence systems.

*This exclusion applies to **any party, including but not limited to non-insured parties**, an insured, their employees, agents, contractors, or any third parties using artificial intelligence on an insured's behalf.*

The preamble to this exclusion, precluding coverage for claims "based upon, attributable to, arising out of, or related to, in whole, or in part", is incredibly broad and may be used by insurers to exclude coverage for claims even where the AI only played a negligible role in the wrongful act or error at issue in the claim.

Moreover, AI exclusions are often not limited to usage of the insured's own AI, but rather extend to usage of any artificial systems (including those of third parties), which is much more common in practice. In fact, an insurer seeking to enforce the broad AI exclusion above may assert that even lawsuits against a policyholder stemming from AI failures at the partner or vendor level would also be precluded by the insurance policy. This is particularly true given that the carrier has drafted the exclusion expressly to apply to "any party, including but not limited to non-insured parties".

With healthcare practitioners increasingly relying on AI software to diagnose and treat medical conditions, financial firms utilizing AI to maximize investment returns, developers incorporating AI for projects, and virtually anyone engaged in business utilizing AI as a means of enhancing ordinary productivity, an error or failure in the "decision making process" or output can result in large financial losses (including bodily injuries and property damages).

While most organizations are simply using AI to aid in their own decision-making processes, exclusions like the one above do not specify that the failure be the direct result of a decision made solely by the artificial system. Instead, they can be applied to claim situations where final decisions were in fact human made.

Again, such exclusions remain rare, however, other exclusions are becoming more commonplace and can be equally problematic, such as wrongful data collection and widespread event exclusions on cyber policies, blanket BIPA exclusions, product defect and service exclusions on D&O policies, and/or pricing discrimination exclusions on EPLI policies.

The widespread use of AI is also creating separate challenges outside of exclusions. A number of carriers have begun limiting capacity, underwriting more aggressively, and in some cases adjusting their rates and retentions to account for the increased risk.

Additional Coverage Considerations

Understanding Clients' Risks

The first step in assessing an organization's AI-specific insurance needs is delineating its role relative to the artificial system. Where AI developers would benefit more from policies insuring against underperformance, contractual risks and certain first-party losses such as costs related to preventative model shutdowns and resulting lost income, AI deployers and businesses that are simply incorporating AI into their own products will have slightly different needs, such as coverage for AI-specific losses including LLM jacking, coverage for regulatory fines, and difference in condition coverage to fill any underlying coverage deficiencies.

Understanding the model's function is equally important. Generative AI models generally pose less risk where resulting losses may be more predictable (such as hallucinations and output errors). Agentic AI systems on the other hand can pose more uncertainty and carry greater operational risk which can be more difficult to predict, particularly as single errors can trigger a cascading effect and models have been reported to go rogue.

Lastly, policyholders should understand the types of harm that may result from an AI failure (such as allegations of unlawful biometric collection, HIPAA exposure, interruption of a client's network or operations, etc), incorporating legacy insurance products to cover each of the respective exposures.

Consider the Implications of Broadened Definitions

Where Tech E&O/Cyber policies contain broadened definitions, consider the implications carefully, particularly in the context of interrelatedness and late notice. As an example, consider a policy whose definition was amended to include "written requests for corrections". Failure of the policyholder to recognize such requests as "claims" (particularly likely when such requests appear harmless) can result in subsequent coverage declinations if later claims are deemed to be related to the earlier demand which was never reported.

Beware of Endorsements That May Sub-Limit Full Coverage

Carefully assess whether AI endorsements are actually broadening coverage. While clarifying that certain AI losses are in fact covered, if sub-limits are being applied, the endorsement may ultimately be limiting coverage. As an example: consider a policy that provides a 250k sub-limit for AI-related data collection claims. Such an endorsement would likely be offering less coverage than a tech E&O/cyber policy that has its unlawful data collection exclusion entirely removed despite the fact that it may not specifically reference AI systems. Some endorsements also contain their own, separate exclusions, which would not have been attached absent the Affirmative AI endorsement.

Exclusions & Problematic Terms in AI Policies

Undue Burden of Overly Broad Governance Requirements

When applying for specific AI insurance, carriers may require documented pre-deployment validation and testing, monitoring and maintenance programs, documented upgrading policies/procedures, formal incident response plans, and internal governance controls. Some insurers may even reduce the amount of covered loss by a certain percentage if at the time of loss, such policies/procedures cannot be evidenced. Policyholders should be aware of such overreaching requirements which impose an undue burden and can ultimately limit the usefulness of the insurance.

Problematic Notification Requirements

Some insurers' policy forms contain clauses requiring the insured to notify the insurer (within a relatively limited timeframe) of any material changes to the model, input data, or any laws or regulations applicable to their AI model – a requirement that would be particularly difficult for any insured to comply with, particularly with "materiality" being undefined and changes to input data occurring frequently.

Use of Open Source and Non-Developed AI Models

Use of non-developed AI models may be excluded – this includes pre-trained foundation models (such as those used by ChatGPT and Claude), and 3rd-party AI components. Claims arising from either the organization's or employee's usage of such models or components would be excluded.

Unscheduled or Change of Use

Use of a company's own developed models outside the use defined in the policy may be excluded – for this reason, it's critically important that any new uses of AI models be notified to the carrier before deploying.

Cyber Losses

Some stand-alone AI policies may actually exclude any cyber incidents that may result in costs related to repairing systems, and/or restoring data – such losses should naturally be covered by a separate cyber policy.

Drop Down Trigger Limitations

AI policies that provide affirmative "drop down" coverage may limit the coverage solely to claims that have been denied by underlying carriers specifically due to an AI exclusion contained in the underlying policy. Should a claim be denied due to the carrier simply deeming that the underlying AI loss (such as a hallucination) does not qualify for coverage (despite the fact that the policy contains no explicit AI exclusion), drop down coverage would likely not be triggered.

Restrictive Interrelated Clauses

Some policies may contain extremely restrictive "interrelated claims" clauses. For example, one carrier's interrelated claims clause reads as follows:

> *"Multiple claims arising from the same, related, or continuous AI wrongful acts, **or from the same AI system** or series of AI systems shall be treated as a single claim"*

This language appears to be particularly problematic, as it would appear only to cover a single claim per AI system.

Recommended Policies, Procedures and Governance

Deployment Validation

Conduct functional, performance, security and bias testing to assess model accuracy

Ongoing Monitoring

Establish defined performance metrics with documented audits, and implement periodic testing and remediation policies

Regulatory Compliance

Implement systems to ensure compliance with current regulations and to track regulatory changes

Training Programs

Train all employees and developers on AI risk best practices

Management Controls

Limit employee AI usage and access to sensitive data, and remove employee system access upon termination

Formal AI Governance Policies and Procedures

Adopt incident response plans and policies for document retention/destruction, computer use and management of protected data

About GB&A

GB&A is a New York-based boutique specialty insurance brokerage with a focus on management, professional, and cyber liability programs for lower mid market, and mid market companies including technology companies, software developers, AI developers and deployers, SaaS companies, financial institutions (such as broker dealers and investment banks) and small to micro-cap public companies.

Founded in 1944, GB&A has been partnering with private and corporate clients, providing client-side advising for over 80 years. In addition to performing comprehensive policy audits and structuring coverage for policyholders, we also maintain a focus on emerging risks, with insights published in leading corporate legal and governance blogs including Reuters/Westlaw, D&O Diary, Harvard Corporate Governance, ABA's Business Law Today, Bloomberg BNA, and Columbia Law's Blue Sky Blog, among others.

Advising clients and structuring coverage since

1944

Web
www.GBAInsurance.com

Email
info@gbainsurance.com

Phone
(914) 723-2220

© GB&A 2026, All rights reserved.