Lowenstein Sandler

Client Alert

Insurance Recovery

November 3, 2025

AI, Deepfakes, and Coverage Drift: What Policyholders Need To Know Now

By Lynda A. Bennett and Jeremy M. King

As companies accelerate adoption of artificial intelligence (AI) across operations, the cyber risk landscape is changing faster than most insurance programs. Threat actors are leveraging AI to supercharge phishing, deploy convincing audio/video deepfakes, and execute faster, more damaging intrusions. At the same time, policy language across cyber, crime, errors and omissions (E&O), media, employment practices liability (EPL), and directors and officers (D&O) lines is evolving—often in ways that seek to narrow coverage unless policyholders proactively negotiate terms.

Policyholders should begin with a program-wide review. Most companies now purchase stand alone cyber insurance, but new AI-related risks are emerging that test the scope of that coverage. Public-facing chatbots and large language model (LLM) enabled tools introduce risks of unauthorized disclosure without "system intrusion," potentially creating coverage disputes about the trigger of the insurer's obligation to pay. Look for endorsements that expressly treat AI-related disclosures, errors, and misstatements as covered events, and confirm that business interruption coverage extends to damage to AI systems and training data, including costs to retrain corrupted models.

Social engineering coverage requires particular scrutiny. AI has eliminated many of the telltale signs of fraudulent communications, and deepfakes have moved beyond email to video, voice and collaboration platforms. Definitions of "fraudulent instruction" and "social engineering" should extend beyond email to audio/video and real-time messaging. Sublimits in policies are increasingly common leading; many organizations to discover only after a loss that their multimillion-dollar cyber tower provides a fraction of that limit for social engineering claims. Some insurer's also condition coverage on specific payment verification procedures—requirements that must be understood and operationalized before a loss occurs.

Ransomware and extortion coverages are also shifting. Emerging threats include manipulation of, or extortion against, AI systems themselves. New insurance product offerings address "LLM jacking" and "jailbreaking," where threat actors corrupt or coerce models to produce erroneous outputs or remove safety constraints. Make sure that extortion and business interruption coverages extend to these scenarios, including where the company's network is not the direct hostage, but the AI model is.

Liability for AI outputs is another pressure point. Technology E&O and professional liability can respond to claims arising from inaccurate, defamatory, biased, or infringing outputs; however, the precise definitions of "technology services," "professional services," and "AI systems" matter. If an AI tool effectively acts as an agent interfacing with customers, its outputs should be treated as the acts of an insured "employee" or "vendor," not merely as software. Media liability may address intellectual property and defamation risks, but exclusions for AI-generated content are proliferating in both general liability and specialty lines. In the employment context, EPL coverage should be evaluated for AI-influenced decision-making exposures as carriers increase scrutiny and implement AI-related limitations.

Regulatory risk is expanding in parallel. New state AI transparency and deepfake laws, as well as emerging rules on automated decision-making and cybersecurity disclosures, can lead to investigations and penalties. Many cyber policies limit regulatory coverage to "privacy events" or "security breaches." Seek updated definitions of "privacy law," “regulatory investigation,” and “wrongful act” that encompass AI regimes and automated decision-making rules, and coordinate D&O and E&O to avoid gaps. Consider whether endorsements addressing the U.S. Securities and Exchange Commission’s cybersecurity reporting costs or allegations of “AI washing” are needed—and whether broad AI exclusions are encroaching on D&O or E&O protections.

As renewal cycles begin, the takeaway is straightforward: Do not accept “as-is” terms. The technology, threat vectors, and insurance policy language are changing monthly. Policyholders should, with the help of experienced coverage counsel, align coverage with actual exposures; negotiate definitions and triggers that reflect AI-era risks; address sublimits and conditions precedent; and ensure cohesive protection across cyber, crime, E&O, media, EPL, and D&O. The precise words in your policies will determine whether tomorrow’s AI-related loss is covered—or not.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

LYNDA A. BENNETT
Partner
Chair, Insurance Recovery Group
T: 973.597.6338
lbennett@lowenstein.com

JEREMY M. KING
Partner
T: 212.419.5927
jking@lowenstein.com

NEW YORK PALO ALTO NEW JERSEY UTAH WASHINGTON, D.C

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.