PRIVATE EQUITY

Artificial Intelligence and the Impact on D&O and Cyber Insurance

The recent emergence of Artificial Intelligence (“AI”) and its widespread reach is no longer simply a concern for AI developers, nor is its exposure limited just to Tech E&O/Cyber claims. Litigation implications directly affecting Directors and Officers in all sectors have surfaced with the recent filing of the first AI-related Securities Class Action Lawsuit and President Biden’s Executive Order issued in late 2023. As AI driven cyber crime evolves and regulatory scrutiny surrounding AI practices increases, the insurance market has yet to devise a cohesive approach to address these challenges.

Impact of AI on Cyber Crime

As AI becomes more integrated into critical infrastructure and decision-making processes, the usual cyber threats (e.g., ransomware, business email compromise, etc.) have evolved. While IT departments strive to keep up with these sophisticated threats by investing in AI to enhance their cybersecurity, so too, unfortunately, are threat actors.

As cybercriminals deploy malicious programs capable of adapting and evolving in real-time to evade traditional defense mechanisms, they can now more easily infiltrate protected networks and wreak havoc. AI has also lowered the barrier for less skilled hackers to join criminal campaigns, which is likely to increase the severity and scope of breaches.

Recently, phishing has transformed as threat actors utilize AI-enabled deepfake technology. A deepfake is a deep learning or machine learning technology in which a person’s face, body or voice has been digitally altered so that he/she appears to be someone else. Deepfakes can be used to spread misinformation or gain access to valuable information and data. Deepfake phishing shares the same goal as social engineering attacks, which is to trick users to gain their trust, and therefore bypass in-place security measures.

Outlined below are some tips for companies to protect against deepfakes:

1. Limit the amount of data publicly available that could be used to create a deepfake. Adjust social media settings so that only trusted people can see what you share.
2. Take full advantage of websites’ privacy settings to control who can access your personal information and content. This includes websites where photos are stored.
3. Watermark photos when sharing images or videos online.

4. Use multi-factor authentication along with long, strong, and unique passwords.
5. Keep all software updated with the latest patches available.
6. Be extremely cautious when reviewing emails, direct messages, texts, phone calls, or other digital communications from unknown sources. As deepfakes become more prevalent, ensure that even anticipated communication is verified directly.
7. Report anything suspicious to your cybersecurity team immediately.

Impact of AI on D&O & EPL Insurance

In response to growing concern over a lack of AI governance and its potential social implications, the White House issued an Executive Order in October 2023 to establish new standards for AI safety and security. The order marks the federal government's first attempt to regulate the development and use of AI by establishing the "White House Artificial Intelligence Council." The Council is made up of 28 different federal agencies and departments and is tasked with monitoring/driving the prompt implementation of AI-related policies across the federal government. As new AI protocols are implemented in conjunction with the Executive Order, we expect this may lead to an increased exposure to claims alleging:

1. Regulatory violations
2. Negligent hiring and supervision practices
3. Board level failure of oversight
4. Disclosure issues around the company's use of AI, the impact of AI on its operations and competitive environment, and the impact of AI on future revenues and overall financial performance (particularly for public companies)
5. Company/Board lack of prudence in their reliance on AI technology to identify investment or M&A opportunities, yielding negative results.

AI Litigation Landscape

To date, AI related lawsuits have mostly alleged copyright and privacy claims. Copyright claims arise when AI models utilize copyrighted content, such as songs, pictures, news articles, code, and books without the creators' consent. Privacy claims arise when non-public personal information is collected without consent and then used for AI models. A smaller number of lawsuits also involve right to publicity claims, which protect an individual's right to control the commercial use of one's identity, such as name, image, likeness or other identifiers (for example, AI software that swaps users' faces with those of public figures).

Artificial Intelligence and the Impact on D&O and Cyber Insurance

In two of the most visible AI cases, news organizations, including Intercept Media and Raw Story Media, filed suit against OpenAI and Microsoft, alleging copyright infringement in violation of the Digital Millennium Copyright Act (DMCA). In both suits, plaintiffs allege their copyrighted works were used to train OpenAI's generative AI systems and ChatGPT model. As the DMCA was originally passed 26 years ago, before the advent of today's AI capabilities, the court's interpretation and legal arguments in these cases will be of particular interest to underwriters. In response to these patterns, underwriters must now consider issues related to the content generated by Insureds, such as plagiarism, copyright infringement, and regulatory compliance. The definition of "Content" within cyber or media liability policies is often broad, including physically printed or digitally displayed media as well as social media posts for which an Insured is responsible. Additionally, regulatory compliance issues may arise concerning the sourcing and display of data, potentially violating privacy laws.

To navigate these complexities effectively, organizations leveraging AI in their operations should implement policies ensuring compliance with relevant laws and obtaining necessary permissions for content usage. Proactive communication of these policies during the underwriting process will be critical as AI technology usage becomes more pervasive.

In February 2024, the first AI-related securities class action lawsuit was filed against AI-enabled software platform company, Innodata. This complaint alleged the defendants misrepresented both the extent to which actual AI was being used in its products/services and the monetary investment the company made into research and development. The filing came days after a short seller, Wolfpack Research, published a report stating that Innodata uses largely offshore workers to perform services that were marketed to the public as AI generated. Following the report, the company's share price declined more than 30%. As investor interest in AI surges, companies seeking to promote their use of AI open themselves to misrepresentation claims known as "AI washing." While this new complaint is the first AI-related securities class action lawsuit to be filed, we expect more to follow in addition to AI-related SEC enforcement actions.

Market Expectations

As there is currently no coordinated insurance market approach to addressing AI-related risks and limited comprehensive claims data, we can expect the following from underwriters:

1. Underwriter scrutiny surrounding insureds' policies and procedures on AI technology usage, particularly in content production and other operational domains.
2. Supplemental questionnaires or additional underwriting questions tailored to AI-utilizing organizations.
3. Possible rate increases and limited capacity for companies that develop AI and use AI as their primary product/service offering.

4. Terms and conditions updated within policy language to keep up with technology and claim trends.
5. Possible coverage restrictions added to policies once legal precedent is set

Do your Insurance Policies Cover AI-related Claims?

While there is no universally agreed upon definition for “Artificial Intelligence” at this time, we must rely on current policy language developed prior to AI’s emergence. Depending on the specific details and nuances of a claim, coverage under Cyber/Privacy or D&O insuring agreements could potentially be triggered. There are however common Intellectual Property limitations and exclusions which could play a key factor in coverage response.

Cyber/Privacy Coverage

Most Cyber Policies include a “Media Liability” Insuring Agreement, which generally covers alleged infringement of copyright or trademark, invasion of privacy, libel, slander, plagiarism, or negligence by the organization regarding its online content. However, coverage for Copyright/Trademark infringement claims under these policies may be limited by policy exclusions, which typically preclude coverage for alleged violation or infringement of patents, trade secrets, or intellectual property. Some policies also exclude coverage for infringement of computer code, which can be problematic for companies that develop/use AI. For example, if a copyright infringement suit alleges the use of AI in the transgression, coverage could be denied.

D&O Coverage

Directors & Officers (D&O) Liability policies generally provide coverage for actual or alleged “Wrongful Acts” in managing the operations of the company. These policies are typically designed to protect company assets and its individual Directors & Officers. Depending on the allegations, coverage could be triggered for claims alleging regulatory violations or copyright/trademark infringement arising from companies’ purported lack of AI governance and controls. Nonetheless, it’s important to note that most D&O policies include an Intellectual Property (“IP”) Exclusion. Such policies’ IP exclusions are typically broadly worded; however, a well written policy should include carve backs affording coverage for individual insureds and claims brought by security holders. With the advent of AI-related claims, we’ve seen increased D&O coverage litigation ensue, involving the IP exclusion and its impact on policy wording and interpretation.

Although these policies may contain limitations pertaining to AI-related claims, not all policies are created equal. Policy wording should be carefully negotiated by a knowledgeable broker to ensure that the broadest coverage is included. It will be imperative for brokers to review policy language updates as underwriting modifications (i.e., exclusions) are added in light of future litigation decisions.

Artificial Intelligence and the Impact on D&O and Cyber Insurance

Intellectual Property Coverage:

In addition to defending against intellectual property theft allegations, insureds should also be aware of the risk of protecting against infringement of their own IP. Stand-alone Intellectual property infringement policies can assist in filling these coverage gaps in two ways, by providing broader defense coverage as well as enforcement coverage. These policies can be written in three different ways:

1. Defense – covers litigation and damages against patent infringement, trademark infringement and copyright infringement
2. Enforcement – covers litigation expenses to enforce IP rights against infringers for patents, trademarks, copyrights and trade secrets
3. Blended Defense and Enforcement Policy – a combination of the two forms noted above

Any company with copyrights, patents, trademarks or trade secrets should consider adding a dedicated intellectual property policy.

Tips to Mitigate AI Risks

- Implement clear governance policies on how the use of AI will be monitored at a corporate level.
- Develop a clearly defined strategy for integrating AI. Prior to implementing AI, make sure that your data infrastructure can support such initiatives. Invest in technologies like cloud computing, data analytics, and machine learning tools.
- Promote a "security-first" culture by creating internal AI policies and procedures and continuously train employees to ensure enforcement of same.
- Regularly perform security audits and keep incident response plans current.
- Implement controls to protect the confidentiality of contractually protected information.
- Comply with data privacy regulations and provide options that allow users to have their information deleted or protected from being shared with third parties.
- Be transparent with customers, employees, and partners about the use of AI or chatbots.
- Update operating software, frequently change passwords and implement two-factor authentication (if not already in place).
- Partner with a broker who understands the intricacies of this evolving exposure and associated insurance policy wording.

Artificial Intelligence and the Impact on D&O and Cyber Insurance

Charles Blackmon
Managing Director
Private Equity Practice
cblackmon@risk-strategies.com
312-252-2164

Heather Munz
Vice President,
Private Equity Practice
hmunz@risk-strategies.com
484-324-2858

Roger Conant
Vice President
Private Equity Practice
rconant@risk-strategies.com
617-800-5785

Sara Wice
Head of Management
Liability & Cyber Risk Claims
swice@risk-strategies.com
212-596-3452

ABOUT RISK STRATEGIES

Risk Strategies is the 9th largest privately held U.S. brokerage firm offering comprehensive risk management advice, insurance and reinsurance placement for property & casualty, employee benefits, private client services, as well as consulting services and financial & wealth solutions. With more than 30 specialty practices, Risk Strategies serves commercial companies, nonprofits, public entities, and individuals, and has access to all major insurance markets. Risk Strategies has over 200 offices including Atlanta, Boston, Charlotte, Chicago, Dallas, Grand Cayman, Kansas City, Los Angeles, Miami, Montreal, Nashville, New York City, Philadelphia, San Francisco, Toronto, and Washington, DC.

This paper is not intended to offer legal advice, nor is it intended to be taken as advice regarding any individual situation and should not be relied upon as such. Any descriptions of insurance provided herein are not intended as interpretations of coverage. An actual insurance policy must be consulted for full coverage details.