LAW360

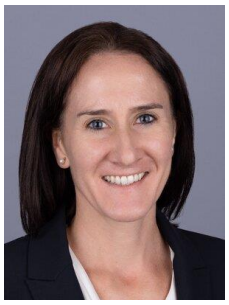
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Mitigating AI Cybersecurity Risks From The Top Down

By **Tracy Wilkison, Eric Vandevelde and Erin Burke** (August 4, 2023, 2:34 PM EDT)


Tracy Wilkison


Eric Vandevelde


Erin Burke

The recent explosion in awareness and popularity of artificial intelligence and machine learning has led to nearly limitless use cases for the technology, including to increase workplace productivity by automating routine tasks, prompting new ideas, and even writing tailored code.

In the cybersecurity space, AI creates efficiencies in analyzing large amounts of information, which can aid in detecting and responding to cyberattacks more quickly through around-the-clock monitoring.[1]

It can also eliminate some of the human error in deciphering vast amounts of information.[2]

However, the rapid rise of AI tools has introduced a slew of cybersecurity and regulatory concerns, and in turn, a response from global governing bodies. The European Union has proposed the AI Act, "the world's first comprehensive AI law."[3]

Similarly, China recently released "a set of provisional rules to govern generative AI services."[4] Lawmakers in the U.S. have been slow to keep pace with global counterparts, but in June, Senate Majority Leader Charles Schumer pushed for a "congressional effort to set new rules for artificial intelligence."[5]

The positive use cases of AI are paired with, and sometimes overshadowed by, the cybersecurity risks it poses through information sharing and its potential to be used against individuals and organizations by threat actors.

While AI and machine learning adoption will likely be necessary for organizations to remain competitive, how can it be implemented into systems successfully, safely and with buy-in from the C-suite and board of directors, given the cybersecurity risks?

Cybersecurity Risks Created by Artificial Intelligence

Reliability Concerns

AI and machine learning models are only as accurate and useful as the information sources they leverage, which can evolve more rapidly than the training process.

Biases not successfully weeded out in the information sources are passed through to assertions and decisions. Algorithms can also generate potentially inaccurate information if they are being relied heavily upon and not double checked.[6]

Privacy Concerns

Using AI further presents information sharing concerns; should sensitive customer data be used in a model, it could be retrieved by others or released publicly if the organization has not appropriately configured and managed the AI implementation.[7]

This could lead to source information accidentally being viewable to other users, which may violate or otherwise conflict with company data privacy policies, data protection regulations, or other requirements.

Threat Actor Concerns

Just as AI can be used to increase efficiency and simplify certain tasks in the workplace, it can also be used by threat actors to more easily carry out their own agendas.

With phishing attacks already a major concern for organizations, AI platforms enable threat actors to create more believable phishing emails with more conversational, grammatically correct language.[8]

These realistic emails increase the risk of global threats, as misspellings and incorrect grammar will no longer be obvious signs of phishing.

Additionally, while some AI models are designed not to generate malicious code, savvy users may be able to circumvent these protections through creatively reworded queries, or to otherwise leverage the tool's capabilities to improve code that can be used for hacking purposes.[9]

Where We Go from Here

Given the widespread nature of potential concerns surrounding AI, many will turn to regulation as a risk mitigator.

Government agencies across the globe are releasing articles and statements about the risks of AI, in addition to proposed laws and regulation.[10]

In January, the National Institute of Standards and Technology released an AI risk management framework to help organizations assess and manage risks posed to individuals, organizations, and society by AI and machine learning.[11]

Similar to how many view the NIST cybersecurity framework as a de facto standard across industries, it is expected that many organizations will also adopt NIST's AI guidance as best practice.

Accordingly, embracing AI where possible requires staying on top of the latest regulations and anticipating cybersecurity risks with proper mitigation strategies in place.

Ensuring Relevant Teams Are Aware of Implementation Plans

The key to successfully implementing a new technology like AI or machine learning is to involve legal and cybersecurity teams from the start to ensure they are incorporated securely and legally.

Cybersecurity and information technology teams can implement proper safeguards to protect sensitive information and systems from malicious actors, while general counsel and legal teams can deploy risk-based AI policies and help ensure regulatory compliance.

Prioritizing Vulnerabilities in Cybersecurity Defenses

As phishing and other cyberattacks become more sophisticated through the use of AI, it is more important than ever to prioritize securing gaps in an organization's cybersecurity strategy.

Companies that offer a product or service that incorporates AI need to consider if their product meets the standards specified by the NIST framework. Regular testing, assessments, maintenance and updates to incident response plans are the most reliable ways to keep an organization secure.

Protecting Employees From Accidental Misuse

Users have a learning curve with all new technologies, and AI is no different.

Having specific policies in place surrounding AI can protect employees from potentially misusing AI tools. These safeguards can include the use of software programs that can prevent employees from pasting data into AI platforms and thus reduce the risk that employees might accidentally share sensitive corporate information.[12]

Employee training on AI, including on how the AI technology works, how the AI tools can be used safely and the potential dangers of misuse, is also critical for organizations.

Assessing Company Policies and Procedures

Use guidelines like the NIST AI risk management framework to assess policies and procedures surrounding AI.

In addition, if an organization offers a product or service that uses AI, the policies surrounding its data sources will need to be closely examined and monitored to determine and mitigate any inherent biases.

Conclusion

AI and machine learning offer tremendous opportunities, but if organizations fail to account for the cybersecurity threats and other risks introduced, they put themselves at risk.

Proper implementation of safeguards and training can assist in the secure implementation of these technologies. Companies should create a strategy that can be shared with leadership at the C-suite and board level to ensure they are aware of the precautions taken.

Staying informed, aware and prepared will allow an organization to successfully and securely take advantage of the benefits of AI.

Tracy Wilkison is a senior managing director at FTI Consulting Inc.

Eric Vandevelde is a partner and co-chair of the artificial intelligence practice group at Gibson Dunn & Crutcher LLP.

Erin Burke is a director in the cybersecurity practice at FTI Consulting.

[1] Victor Fredung, "Using AI to Compliment Cybersecurity and Threat Detection," Forbes (February 28, 2023), https://www.forbes.com/sites/forbesbusinesscouncil/2023/02/28/using-ai-to-compliment-cybersecurity-and-threat-detection/?sh=3ed1035338e0.

[2] Id.

[3] "EU AI Act: first regulation on artificial intelligence," European Parliament (June 14, 2023), https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[4] Rita Liao, "China unveils provisional rules for generative AI, including a licensing regime," TechCrunch (July 13, 2023), https://techcrunch.com/2023/07/13/china-unveils-provisional-rules-for-generative-ai-services/.

[5] Cristiano Lima, "Schumer launches 'all hands on deck' push to regulate AI," The Washington Post (June 21, 2023), https://www.washingtonpost.com/technology/2023/06/21/ai-regulation-us-senate-chuck-schumer/.

[6] Tyler Weitzman, "Understanding The Benefits And Risks Of Using AI In Business," Forbes (March 1, 2023), https://www.forbes.com/sites/forbesbusinesscouncil/2023/03/01/understanding-the-benefits-and-risks-of-using-ai-in-business/?sh=42e0a1e66bba.

[7] "2023 Privacy and AI Governance Report," FTI Consulting (2023), https://www.ftitechnology.com/resources/white-papers/2023-privacy-and-ai-governance-report.

[8] Jim Chilton, "The New Risks ChatGPT Poses to Cybersecurity," Harvard Business Review (April 21, 2023), https://hbr.org/2023/04/the-new-risks-chatgpt-poses-to-cybersecurity.

[9] Id.

[10] "International Community Must Urgently Confront New Reality of Generative Artificial Intelligence, Speakers Stress as Security Council Debates Risks, Rewards," United Nations (July 18, 2023), https://press.un.org/en/2023/sc15359.doc.htm.

[11] "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," National Institute of Standards and Technology (January 26, 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[12] Barath Chari, Laura DeBoel, Stefan Geirhofer. Gary Greenstein, Scott McKinney, Maneesha Mithal, Kristina Wang, "Legal, Commercial, and Ethical Risks Posted by the Rapidly Evolving Field of GenAI Technology," JD Supra, (May 3, 2023) https://www.jdsupra.com/legalnews/dos-and-don-ts-for-developing-extending-6305250/.