ALM | LAW.COM

New York Law Journal

The Increasing AI Disruption of Cybersecurity

By Cathy Mulrow-Peattie
March 1, 2024

It is expected that cyber crime globally will reach $9.5 trillion in 2024 and $10.5 trillion in 2025 (Forbes, Feb 5, 2024). Complicating this cybercrime explosion is the use of artificial intelligence (AI) by cyber adversaries and increasing use of AI systems with increasing amounts of data by organizations. As a result, AI is disrupting cybersecurity prevention, regulatory compliance and security incidents management.

How can companies practically respond to this disruption? With an understanding of AI attack vectors, using AI defense tools, leveraging requirements from established federal and state regulations, frameworks and regulatory guidance to manage these new cyber compliance risks, and reviewing their cyber security insurance application and renewal statements so that they are covered in the event of that AI breach or attack.

How Is AI Being Used by Cyber Criminals?

Baracuda Networks reports that cyber criminals are using AI to increase the number and sophistication of their attacks, and about 40% of the organizations surveyed indicated that they were unprepared for an AI related cyberattack (Baracuda Networks, Cybernomics Report 101, January 2024).

Below we have set out AI attack vectors currently employed cyber adversaries:

• AI is being used to track email addresses and create highly personalized emails to bypass counter measures.

• Automated phishing attacks—ChatGPT can mimic the style and language pattern of a legitimate employee or officer of a company.

• AI malware attacks to evade detection by existing systems.

Photo: Digilife via Adobe Stock

• Training data can be tricked/poisoned to produce inaccurate outputs and models can be breached.

• AI can impersonate others through deep fake videos.

This recent deep fake attack is alarming. A fraudster invited a clerk to a video conference where fake images and voices of colleagues downloaded from the intranet were used to look like a valid meeting. The clerk made 15 transactions as instructed from the meeting to five local bank accounts, which came to a total of $200 million Hong Kong dollars. It was only after sending the money that the employee realized it was a scam (*see* Heather Chen and Kathleen Magramo, "Finance worker pays out $25 million after video call with deepfake 'chief financial officer'", CNN, Feb. 4, 2024).

How is AI a Prevention Mechanism for Cybersecurity?

These AI-related threats require thoughtful AI and cybersecurity-related defense responses. Some of the ways that AI is being used as a countermeasure are:

• to compare abnormalities in behavior and data to predict unusual behaviors;

• for malware defense;

• for vulnerability management;

• automated incident response; and

• to recognize impersonation of others through behavior recognition and fraudulent attack vectors (KPMG, AI to Strengthen Cybersecurity, 2023)

Once identified AI can stop the behaviors by logging off suspicious actors and notifying IT/security professionals of the unusual activities. AI can be trained to remember incident behavior and as incidents morph and grow can quickly understand and protect against new threats. AI can predict outcomes, take action and generate alerts.

For example, AI is being used by the Cybersecurity and Infrastructure Security Agency (CISA). Threat hunting and security operations are provided terabytes of data each day from the National Cybersecurity Protection Systems Einstein sensors. This tool allows automated cybersecurity alerts to be issued based on aggregated data and probabilistic based models to ensure cyber anomalies are detected in a timely manner.

Lessons To Learn From Cybersecurity, AI Regulation; Best Practices To Strengthen AI Systems Cyber Defenses

Organizations need to consider how to secure both their AI systems and implement AI cyber defenses. This security and compliance challenge is parallel to the cybersecurity challenges with prior new technologies—it is all about identifying, protecting against, detecting and responding to risk.

Under the Biden administration's Executive Order 14110: for the Safe, Secure and Trustworthy Development and Use of Artificial Intelligence, it is clear that security by design and default needs to be a key attribute for any developed or used AI system.

AI systems should respect fundamental cybersecurity requirements that are established, for example, under leading cybersecurity frameworks of National Institute of Standards and Technology (NIST), and leading edge regulations of New York State Department of Financial Services Part 500, 23 NYCRR Part 500 (NYDFS Part 500) and the Gramm Leach Bliley Standards for Safeguarding CustoTomer Information Title 16 Part 314 (Safeguards Rule). These basic controls should be in place to secure all AI developed and used systems.

While the NIST AI Risk Management Framework lays out the process of Govern, Map, Measure and Manage for AI governance, when addressing AI cybersecurity risk, the framework further advises that AI systems should be robust enough to avoid and detect attacks and resilient enough to operate post incident.

Under the rubric, along with the NIST Cybersecurity Framework, NYDFS Part 500 and the Safeguards Rule, companies using and developing AI should consider and document the following cybersecurity compliance activities:

Identify: Develop an understanding of the AI cybersecurity internal and external risks for the AI systems that your organization develops or uses from a third party including:

• Completing an inventory of your AI used or developed systems.

• Reviewing your cybersecurity policies at a least annually, adding in AI related controls and mitigators.

• Knowing what personal information, including sensitive data, is held within your AI systems and updating these data maps as AI system data is augmented.

• Conducting ongoing risk assessments on the use of AI systems in your business, including identifying the benefits, risks and mitigators for these on premise and supply chain AI system, and reassessing risks with added use cases.

Protect: Develop and implement the appropriate safeguards such as:

• Implementing safeguards to ensure the confidentiality and security of personal information included in your AI systems.

• Implementing multifactor authentication.

• Implementing encryption of AI data in transit and at rest.

• Ensuring that software and hardware are updated/patched promptly.

• Reviewing and managing your user access privileges, including third parties, to limit access to what is needed and terminate what is not.

• Assessing third party AI vendors on their initial and continued adequacy of their cybersecurity practices and controls.

• Adopt secure development practices for all AI systems.

• Conducting cybersecurity awareness and training about AI threat vectors.

• Most importantly, keep humans in the loop on AI systems security reviews.

Detect and Test: Develop and implement appropriate detection capabilities, to regularly monitor and test the effectiveness of your AI systems security, including:

• Using AI cyber detection tools, accelerating AI abnormality and vulnerability detection.

• Implementing endpoint detect/response solutions.

• Using centralizing logging/AI security event alert solutions.

• Monitoring and testing should include continuous monitoring or periodic penetration testing and vulnerability assessments.

• Adopt procedures for AI systems' material change management.

Respond: Develop and implement appropriate policies to respond to an AI cyber event, this includes an updated incident response plan to cover the use of AI systems and defenses against AI threat vectors.

Recover: Develop and implement appropriate policies for resilience and to restore any capabilities or services that can be impaired due to an AI cybersecurity event.

AI Systems and Cyber Insurance Coverage

No discussion of AI cybersecurity can occur without considering cyber insurance coverage issues. Most cybersecurity liability policies require the policyholder to have certain security controls in place at the time of a breach. Failure to have those controls and/or misrepresenting them to the insurance company in the application or upon renewal could be grounds for denial or disclaimer of coverage. Certain policies may contain exclusions if it is determined that the insured failed to implement procedures or policies that may have prevented a breach.

C-Suite and security professionals should consider as part of their AI cyber compliance review what their organization represented in its cyber policy application and renewal as to data inventory, privacy controls, network security, incident response, business continuity, vendor assessments and ongoing security training related to AI systems used and developed by their organizations. These representations will often need to be modified as new AI systems are used within organizations or changes to these systems or data occur.

Organizations should review their cyber insurance policies in light of the use of AI systems and AI related cyber risk to make sure that they have adequately portrayed and implemented the security controls to have continuous coverage.

What To Do Next?

According to leading AI technology compliance solution BreezeML CEO Harry Xu, cybersecurity is a key component of AI compliance. "Confirming that your AI system has adequate and documented cybersecurity compliance controls in place is critical to any developed AI model compliance."

Cybersecurity and AI system resilience is about putting the appropriate controls and documented policies and procedures in place to manage the increasing AI security risks. AI has been used for decades–what has changed is the amount of data it uses, the ways we use it and its increased vulnerability to attack. As result, as with assessing any new risk, the benefits and the ways to mitigate the risks should be considered. The above framework should allow organizations to start their compliance path toward cybersecurity and AI system resilience.

Cathy Mulrow-Peattie *is a partner at Hinshaw & Culbertson in New York, where she counsels clients on artificial intelligence, privacy, cybersecurity and digital media issues, among others.*