A sword and a shield: AI's dual-natured role in cybersecurity

AUTHORS

 Nic Wall

 Rachel Gregoris

Further reading:

- What should be included in my organization's AI policy?: A data governance checklist
- The board says we need an AI strategy. How do we start?

Artificial intelligence (AI) is an increasingly powerful force in the cybersecurity space. Unfortunately, it is available to both good and bad actors. Hackers use AI tools as weapons to carry out sophisticated cyberattacks, while organizations develop defensive mechanisms to identify and eliminate threats.

With a projected global market value exceeding US$130 billion by 2030, the AI cybersecurity market is one of the fastest growing spaces in the technology sector[1]. This massive growth is believed to be driven by both the rapid development of AI capabilities and the necessity of implementing AI-driven cybersecurity tools.

This article examines the impacts of advancements in AI technologies on both sides of cybercrime and offers guidance to organizations looking to bolster their cybersecurity programs.

How are threat actors using AI?

AI is used to scale up cyberattacks

While AI tools are highly valued for their ability to process enormous quantities of data, hackers can leverage their processing power to increase the frequency, sophistication and calibre of cyberattacks. Since 2021, cybercrime incidents have surged worldwide, with data breaches increasing by 72% between 2021 and 2023[2]. Automated tools used in attacks and extortion, such as chatbots, can rely on AI to become more sophisticated and believable. AI can increase the scale of some types of cyberattacks, like distributed denial of service (DDoS) attacks, where massive amounts of web traffic are used to overwhelm the target's servers. AI's application can also extend beyond the initial cyberattack itself. When criminals succeed in a data breach, they can use AI tools to comb through terabytes of data and identify the most sensitive information, like personal information, trade secrets and financial data.

Generative AI's new role in social engineering

Generative AI models are used to produce high-quality text, images, audio and video. These outputs, also known as

deepfakes, are increasingly responsible for high-profile cyberattacks due to their believability.

In January, hackers targeted an employee of a British engineering firm. Impersonating the firm's CFO, the hackers told the employee to transfer funds to the hackers' bank account. When the employee sought to confirm the instructions via video chat, the hackers impersonated the CFO using deepfake video capabilities and convinced the employee to transfer the funds. Ultimately, the hackers stole US$25 million from the firm before the transactions were discovered to be fraudulent[3]. For more on AI consumer risks, read "AI in financial services: are consumers better protected, or more at risk?"

> Since 2021, cybercrime incidents have surged worldwide, with data breaches increasing by 72% between 2021 and 2023.

The traditional telltale signs of phishing are also becoming increasingly obsolete as generative AI becomes more convincing at impersonating colleagues, friends and family members. Educating employees on hackers' new abilities and implementing authentication procedures will be essential to avoiding impersonation-based cyberattacks. For more on human resources, read "Can HR use AI to recruit, manage and evaluate employees?"

How can organizations use AI to protect themselves?

AI automates cybersecurity practices

On the other side of the coin, AI-driven cybersecurity tools can provide a formidable barrier against cyberattacks.

Another major benefit of using AI is the ability to automate routine security practices such as threat monitoring. Indeed, many endpoint detection and response tools (tools used to detect malicious software) have leveraged AI for some time to help determine how the tools identify and respond to suspected threats. The comprehensive monitoring employed by these and similar security tools far surpasses human capabilities while using fewer resources. These tools not only alleviate some of the workload for cybersecurity teams but can also reduce human error, which is widely attributed as the leading cause of system breaches[4].

Further, AI-based tools can identify, test and patch system vulnerabilities before they are exploited by hackers. A proactive approach to cybersecurity is critical, as bad actors use their own AI tools to locate these vulnerabilities more quickly than ever before.

Increased adaptability through machine learning

Many AI-based cybersecurity tools use some form of machine learning; a process where a program draws conclusions by detecting patterns in large sets of data. Machine learning systems can continuously alter their actions based on new and changing data without any human intervention. This quality makes them indispensable to organizations looking to adapt their cybersecurity response to evolving threats.

Legal considerations for organizations

Most sophisticated organizations are aware of the range of legal, operational and related risks that successful cyberattacks pose. Understanding how the underlying technological threats are changing is essential to maintaining a clear view of these risks. Organizations should therefore ensure personnel are monitoring advancements in cybersecurity threats and solutions.

Organizations should also consider incorporating AI tools into their cybersecurity arsenals to address the increased monitoring and deployment required to address AI-driven attacks. However, organizations should keep in mind that the use of the term "AI" in describing a product does not automatically mean the product is good or effective. Indeed, AI can also be entirely unnecessary for certain functions. Organizations should do their due diligence, and ensure they review product descriptions, documentation and contractual terms.

In addition, businesses should consider deeper and more frequent training of personnel and other (sometimes low-tech) solutions to counter increasingly sophisticated social engineering attacks.

Finally, organizations should monitor the regulatory landscape as Canada and other countries and regulators continue to respond to both cyberattacks and advances in AI (for more on AI regulations, read "What's new with artificial intelligence regulation in Canada and abroad?"). Indeed, Bills C-26 and C-27, both currently advancing through Parliament, respectively contain new proposed requirements for cybersecurity and AI.

FOOTNOTES

This article was published as part of the Q4 2024 Torys Quarterly, "Machine capital: mapping AI risk".

To discuss these issues, please contact the author(s).