The Future of Cybersecurity

Realistic predictions for what the next five years will bring to cybersecurity

12 min read

Listen to this article

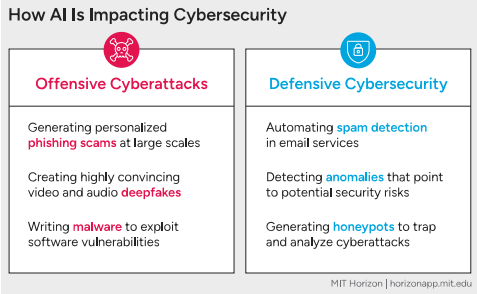
00:00 16:49

Sections:

AI will be used for both offense and defense

AI tools, particularly those built on the latest advancements in generative AI, lower the technical barriers for cybercriminals, allowing them to improve existing attack strategies. Many of those same AI tools can bolster organizations' cybersecurity. "I often refer to this as an arms race, because both the attacker and defender are always seeking an advantage, much like the arms race in warfare. Furthermore, often a particular weapon can be used either for offense or for defense," Stuart Madnick, founding director of Cybersecurity at MIT Sloan, tells MIT Horizon. For example, Madnick says AI can help analyze large volumes of code to detect vulnerabilities in software—a powerful capability for

both defenders and attackers. “From everything I’m seeing, the bad guys are much more aggressive in using it to try to detect vulnerabilities than the good guys are in trying to detect and fix them in time,” Madnick adds.



Attacks powered by generative AI

For cybercriminals, AI can expand the scope and scale of their attacks. “The scalability of these attacks is staggering,” Gil Baram tells MIT Horizon. Baram is a senior lecturer at Bar Ilan University and a nonresident research fellow at the University of California, Berkeley, where she leads an initiative researching AI-enabled cybercrime. “AI allows attackers to automate and personalize attacks at scale, targeting thousands of victims simultaneously with personalized and effective attacks,” she says. For example, generative AI tools can excel at producing convincing *phishing* emails, deceptive messages sent by attackers to trick users into opening a harmful link or attachment. AI models can scrape the internet for information on an intended target and generate persuasive email text customized to the individual—faster and cheaper than it would take a human. One study from researchers at Harvard University’s Kennedy School of Government found that more than half of participants (54%) clicked on a link from an AI-generated phishing email. While human experts achieved the same click-through rate when sending their own targeted phishing email, it took them about 34 minutes per email. The AI tools required barely any overhead time to collect data on a target and send a phishing email, according to the study.

As generative AI models improve, so does their ability to create *deepfakes*, realistic-looking images and video generated or modified by AI. It will become harder to distinguish deepfakes from reality, a threat to individuals and organizations alike. In 2024, U.K.-based engineering firm Arup fell victim to a scam in which a deepfake of the firm's chief financial officer convinced an employee to make multiple money transfers, totaling a $25 million loss. Experts are finding that generative AI can also produce *malware*, computer programs that are designed to cause harm. One study from researchers at the University of Illinois Urbana-Champaign found that OpenAI's GPT-4 model, when given a description of common vulnerabilities that have been detected but not yet fixed (sometimes called one-day vulnerabilities), was able to generate code to exploit those vulnerabilities 87% of the time.

Using AI to spot and study cyberattacks

Opportunities to use AI in cyber defense have evolved as the technology has improved, moving from rigid rule-based systems to detect anomalies to machine learning systems able to identify more complex threats. AI is now commonplace in some cyber defenses, such as email spam filters. Nonetheless, experts generally agree that cyberattackers are moving more quickly to adopt advanced AI tools than organizations are integrating AI into their defenses. This is not for lack of interest: 95% of the 1,800 cybersecurity professionals surveyed by cyber defense firm Darktrace said AI tools would improve their organization's security. Because AI can learn patterns within extremely large data sets, including patterns undetectable by humans, experts say the technology could alert organizations of irregularities that indicate a potential cyberattack—including newer threats that current cybersecurity systems might miss.

Organizations can also use AI to better understand emerging cyber threats—for example, by sorting through large amounts of data to identify new types of risks. Some organizations are

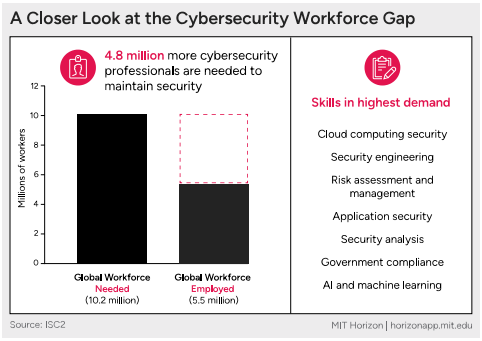
exploring how to use generative AI models in *honeypots*, decoy computing systems meant to lure cyberattackers and study their techniques. A team at Palisade Research deployed an AI-powered honeypot to trap and analyze other AI-driven cyberattacks. Over the course of a few weeks, the honeypot gathered more than 800,000 hacking attempts, including six attempted attacks by AI agents, according to the 2024 research paper. The Palisade team plans to evaluate the AI-driven attacks in future research to determine common behaviors and strategies. Ultimately, experts see AI as a way for organizations to boost their defenses in concert with cybersecurity practitioners. "The key is to integrate AI as a complement to human expertise, not a replacement," Baram says. "Together, they create a more robust and adaptive defense."

Organizations will struggle to hire qualified cybersecurity personnel

For years, many organizations have faced a cybersecurity skills shortage. It's a trend that's likely to continue. As cyber threats grow and become more complex, the demand for cybersecurity professionals will only increase. Only 14% of the more than 300 respondents surveyed for the World Economic Forum's 2025 Global Cybersecurity Outlook expressed confidence that their organizations have adequate cybersecurity talent and skills.

In 2024, the global cybersecurity workforce gap—the difference between organizations' staff and the number they say they need to maintain security—totaled more than 4.8 million people, according to the International Information System Security Certification Consortium, Inc. (ISC2), an association for cybersecurity professionals. That is 19% more than the prior year. Nearly half of those surveyed by ISACA, an organization for IT professionals, said their organization has open non-entry-level cybersecurity

positions. The World Economic Forum found public sector organizations face a larger gap than their private sector counterparts—49% of public sector organizations said they didn't have the cybersecurity talent they needed in 2024, a 33% increase from the year before. Often, even if organizations want to hire more cybersecurity professionals, they don't have the budget to do so. Lack of budget was the top reason respondents identified for their organization's skills shortage, according to the ISC2 study.



A skills shortage has a major impact on an organization's ability to build resilience to cyberattacks. According to the ISC2 study, organizations with critical skills gaps were almost twice as likely to suffer a data breach than those with adequate cybersecurity staff. To address this skills shortage, experts recommend organizations look beyond technical talent and focus on upskilling noncybersecurity workers. "Everybody in the organization has a role to play," Cybersecurity at MIT Sloan's Madnick says. "Yes, you do want to try to increase the technical experts and professionals, the ones with a lot of training. But we're missing the opportunity to augment them with an enormous number of people who right now are off the radar."

As organizations use more AI tools in their cyber defenses, that might also ease the effects of the skills shortage. "As AI tools and these automated agents get better, we may need fewer cybersecurity professionals. You may be able to outsource a lot more of your security to a third party that specializes in this,"

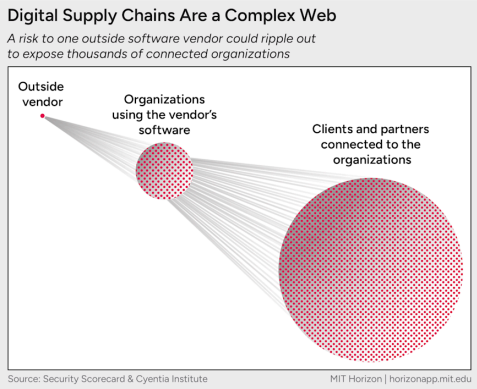
Taylor Reynolds, technology policy director at MIT's Internet Policy Research Initiative, tells MIT Horizon. Reynolds compares this to the IT outsourcing that emerged in the last couple decades, making it possible for specialists to remotely run an organization's IT infrastructure. "For probably the next five to 10 years, we're going to need a lot more cybersecurity people, but that may start to shrink further down the road," he adds.

Complex supply chains will present a growing cyber risk

In a *supply chain attack*, cyberattackers deliberately target companies that produce software in order to infect their customers. These attacks can cause significant harm, as organizations are increasingly relying on a network of partners to provide a range of digital services. The risk can be especially acute when third-party services are run by smaller companies with weaker cybersecurity protections. "Because small and medium businesses don't have the resources to manage cyber the same way, they are being targeted as the attack vector into a larger company," Keri Pearlson, executive director of Cybersecurity at MIT Sloan, tells MIT Horizon.

Third-party relationships are growing as organizations perform more operations digitally and as they look for partners that are specialists in technologies such as AI. But as organizations bring in these third-party services, they are introducing more risk. The larger an organization, the more complex and more vulnerable their digital supply chains are becoming. A survey of 2,000 executives by IBM and Microsoft found that their organizations had an average of 1,284 direct suppliers and 6,420 indirect suppliers. This sprawl of suppliers is increasingly worrying larger organizations. More than half (54%) of large organizations surveyed by the World Economic Forum for their 2025 Global

Cybersecurity Outlook identified supply chain challenges as their biggest hurdle to improving cybersecurity.



If cyberattackers infiltrate a third-party vendor, they could steal the data of customer organizations or bring down critical services that many organizations rely on, causing a damaging ripple effect. And just as one large organization can have many small third-party suppliers, one vendor can serve many, providing a single point of failure for hundreds or thousands of organizations. In 2024, software provider CDK Global suffered a cyberattack that required it to shut off the services it provides to more than 10,000 car dealerships across the U.S. The dealerships, left in a lurch, incurred collective losses of more than $1 billion during the three-week period the software was shut down, according to one estimate.

Managing the cyber risks from third-party vendors will be a big focus for organizations in the near-term. According to a 2024 report, almost all (98%) of the more than 230,000 organizations analyzed by cybersecurity ratings firm Security Scorecard and research group The Cyentia Institute work with at least one third-party vendor that recently suffered a data breach. Reynolds, of MIT's Internet Policy Research Initiative, says his group and others are working on ways to better equip organizations to assess the cybersecurity of third parties. Currently, most security tests are conducted by firms that probe from outside of an organization's network to search for vulnerabilities. "I think in the next five to 10

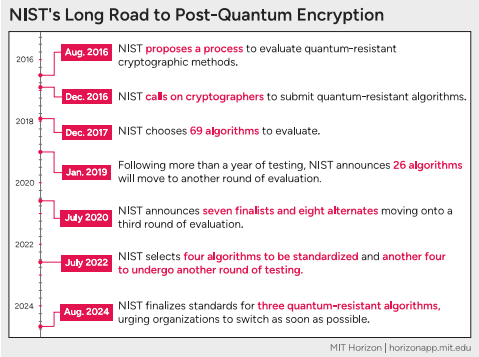
years, we're going to have better diagnostics within an organization that's going to be able to say, 'This is why we think we're secure,'" Reynolds says. "We're going to be able to sum that up into some sort of security score that is talking about the inside of the network and not just the outside of the network."

Organizations will adopt quantum-proof encryption methods

Quantum computing, once fully developed, could upend the ways organizations around the world currently secure information digitally. "The cryptography systems—the encryption, digital signature schemes—that we use to communicate over the internet right now, a lot of them can actually be broken if there is a large-scale quantum computer," Vinod Vaikuntanathan, professor of engineering at MIT's Department of Electrical Engineering and Computer Science and principal adviser at the MIT Computer Science and Artificial Intelligence Laboratory, tells MIT Horizon. "This is because all these systems use a hypothesis that certain mathematical problems, like factoring very large numbers, are hard, and they aren't if there is a quantum computer." (For more on how quantum computers could eventually break today's common encryption methods, see The Future of Quantum Computing.)

The risk to current encryption systems may not materialize for many years. However, governments and organizations are already starting to transition to data security methods that could resist attacks from quantum computers, often referred to as *quantum-proof* or *post-quantum* encryption. In 2024, the U.S. National Institute of Standards and Technology (NIST) finalized standards for three encryption algorithms that can resist attacks from quantum computers, the result of an eight-year long process during which NIST solicited proposals from the world's cryptographic experts. NIST's standards include instructions for

switching to the new encryption schemes, and the institute urged organizations to begin doing so immediately.



One threat spurring organizations into action is the “harvest now, decrypt later” strategy—the possibility that cyberattackers are stockpiling sensitive information encrypted with today’s methods, aiming to eventually decode it once a sufficiently capable quantum computer is available. “If this encrypted data gets into the hands of an adversary, I think it’s game over. Storage is cheap at this point,” Vaikuntanathan says. “If you really have something that you think should be secret 15 years from now, handle it in a different way.”

Some technology companies have recently begun facilitating a switchover for their web browsers, internet networks, and digital messaging infrastructure. In September 2023, Signal announced it had upgraded its service to include post-quantum encryption, the first major messaging app to do so. Apple adopted quantum-proof encryption for its iMessage service in 2024. Network security company Cloudflare says that while it’s been using post-quantum security measures for years, web browsers and apps must also support that level of security for it to work. According to Cloudflare, less than 2% of internet traffic was encrypted with post-quantum methods at the beginning of 2024. By the end of 2024, that rose to 13%, after Google enabled post-quantum encryption on its latest Chrome browser in April.

For most organizations, it will take years to transition away from the decades-old, deeply entrenched current encryption methods to new, quantum-proof ones. The U.S. Department of Defense, for example, is aiming to move its high-priority systems to post-quantum cryptography by 2035, an effort officials have said will be massive. “We’re talking hundreds of thousands of endpoints, perhaps millions in some cases that have to be touched, and the algorithms updated and replaced,” David McKeown, special assistant for cybersecurity innovation to the Department of Defense’s Chief Information Officer, said in October 2024.

Ultimately, though, experts say most organizations will eventually move to new, post-quantum cryptographic systems, particularly if they want to communicate securely with major governments and large organizations. In the meantime, while the timeline for quantum computing is still uncertain and as new quantum-proof algorithms gain their footing, Vaikuntanathan says organizations could take a hybrid approach where “you encrypt data like an onion,” layering both current and post-quantum encryption methods to protect data. Some organizations, such as Signal and Cloudflare, are already implementing this. “An attacker would have to break both to get access to the data,” Vaikuntanathan says. “If you are really paranoid, that is what one should be doing.”

Learn more

- Common misconceptions about cybersecurity
- Cybersecurity policy (Video series by MIT xPRO)
- Cybersecurity knowledge check

Mark Article Complete

0/9 Articles Complete

Previous: Recent Developments

Next: Glossary