For gen-AI-enabled threats, fight fire with fire

Generative AI is upending the cybersecurity landscape. PwC's Sean Joyce and Norbert Vas explain how to leverage the technology against those who misuse it.

Blog 5 minute read November 28, 2023

Share

Sean Joyce

Partner, Global Cybersecurity and Privacy Leader, PwC United States

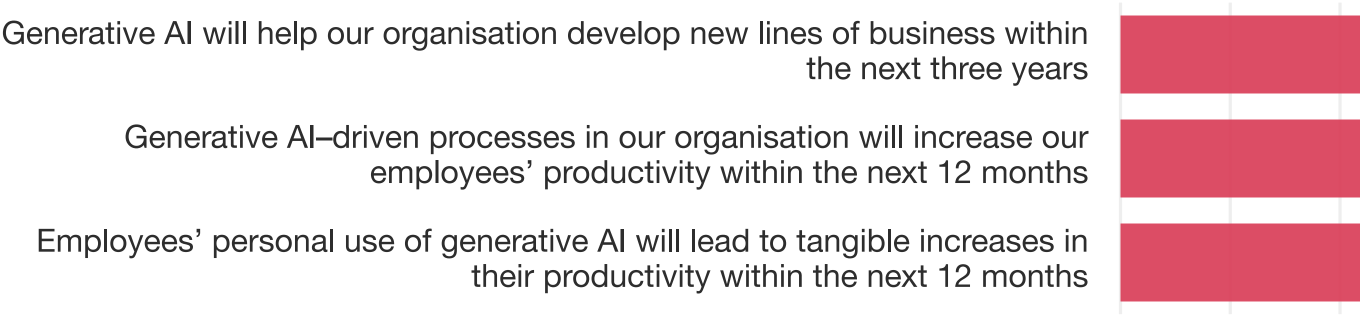
Norbert Vas

Cyber, Risk and Regulatory Services, Director, PwC United States

How do executives feel about generative AI? Conflicted.

Take a look at the findings on cyberdefence and AI from PwC's latest Digital Trust Insights survey. A solid majority of the nearly 4,000 business leaders who participated in the survey are optimistic about the technology's potential impact on their business.

Share of respondents answering ‘strongly agree’ or ‘agree’



Source: PwC's 2023 Digital Trust Insights survey

And yet, 52% of those same survey participants—71% if you exclude IT and cybersecurity executives—say they expect generative AI to lead to a catastrophic cyber attack in the next year. What’s going on?

The fact is, we’ve often seen this tension between fearleading and cheerleading—to borrow a phrase from our colleagues at ***strategy+business***—when working with clients who are grappling with the security implications of generative AI. And we get it. Senior leaders are eager to leverage generative AI before their competitors do, but they’re also apprehensive about the risks and overwhelmed by the flood of news about the technology.

Are those 52 percenters being alarmists? The answer is, yeah, a little. We don’t think most companies will face a catastrophic gen-AI-powered attack in the coming year (the technology is as new to attackers as it is to defenders), but we do think businesses could face long-term consequences if they don’t balance their enthusiasm for generative AI with a clear-eyed understanding of what they’re up against. Among the top threats posed by generative AI are:

A higher volume of sophisticated attacks. The proliferation of large language models has significantly lowered the barrier to entry for being a threat actor. That will increase the frequency of large-scale attacks. Moreover, threat actors have the power to leverage generative AI to create more believable and sophisticated phishing campaigns, as well as deep fakes, which can lead to greater exposure—especially for organisations that do not have a sophisticated cybersecurity risk management program in place.

Faster-changing methods. Generative AI's ability to rapidly design and iterate attack methods means that existing defences, designed to detect anomalous activity, will need ongoing retooling to become more agile.

More ways for perpetrators to cover their tracks. AI can help threat actors hide behind false flags by imitating the tactics of other groups. And because the technology is now so widespread, identifying wrongdoers by their choice of tools is a less viable option.

More credible-seeming disinformation. Generative AI can create sophisticated disinformation at scale, risking an erosion of everyone's confidence in the legitimate data and information that companies want to disseminate.

How can businesses respond? For starters, they need to go back to the fundamentals of what they are doing around cybersecurity. They need to think about how the risks for generative AI are different, and think through what controls can be used to mitigate those unique risks. It's not necessarily about creating anything new—but taking a step back and looking at their cyber risk management program from a new perspective in light of these new risks.

Additionally, they should put in place the governance policies and guardrails that too many executives—including a sobering 64% of the DTI survey respondents—say they're willing to initially forgo in favour of fast adoption. That means establishing training and guidelines for responsible use of generative AI, and creating a sandbox for workers to experiment safely. Many companies are creating proprietary, fully walled-off generative AI solutions that prevent the leaking of data, and they're deploying generative AI in a manner that leverages organisational data to reduce the risks arising from biases and misinformation.

But those are table stakes. When it comes to defending against gen-AI-powered attacks, the technology itself is proving to be a game-changer. CISOs and other cybersecurity leaders should get busy in three areas.

Threat detection and analysis. Many of the activities traditionally performed by level-one security operations centre (SOC) analysts—who form a first line of defence in cybersecurity—can be more effectively managed by generative AI, saving analysts a great deal of tedious manual work. SOCs often rely on predetermined detection rules that help analysts recognise threat sources. Generative AI can analyse those rules and see where they fall short—highlighting new types of attacks you might have missed. Generative AI can also learn to recognise sophisticated spear-phishing attempts and prevent them from landing in your inbox. And it's good at identifying patterns and anomalies that elude traditional signature-based detection systems.

Cyber risk and incident reporting. With the help of natural language processing, generative AI can turn technical data into content that non-technical people can understand. Say you've had an incident that caused a major business disruption. How do you get the pertinent information into the hands of the right people quickly, in the most concise form? Generative AI can create targeted reports; the one for the company's chief compliance officer, for example, would focus on regulatory implications, and so on. Generative AI could also be trained to create templates for comparisons to industry standards, leading practices, and regulations—an advantage in an era of increased regulatory attention to cyber-breach reporting.

Adaptive controls. Securing the cloud and software supply chain requires constant updates in security policies and controls. Machine learning algorithms and generative AI tools could soon recommend, assess and draft security policies that are tailored to an organisation's threat profile, technologies and business objectives. GenAI can also automate, continually assess and assign risk scores for endpoints—laptops, phones and other connected devices—and review user access requests and permissions accordingly.

The good news is that adoption of these tools is accelerating: 69% of survey respondents are planning to use generative AI for cyberdefence in the next 12 months, and nearly half (47%) are already using it for cyber-risk detection and mitigation. Those are big steps toward a future in which business leaders can tap into generative AI's immense potential without constant fear of a catastrophic cyber attack.

Explore the full findings of PwC’S 2024 Digital Trust Insights survey.

Read more

Related content

CISOs should rewrite the playbook for cyber breaches

As threats become more interconnected, incidents are getting costlier and more frequent, according to a new PwC survey. A systemic response rests on five key...

Seven crucial actions for managing AI risks

Executives need to give higher priority to the fast-evolving risks of generative AI. They can start with a few key trust-building actions.

Geopolitical conflict requires a new cyber toolkit

Senior executives are upping their investment in cybersecurity in the face of global instability, according to PwC's latest CEO Survey, and rightly so.

AI is transforming asset and wealth management

PwC research forecasts that assets managed by robo-advisors will double in the next few years. Take four key steps to avoid being left behind.

Make the right decisions for right now

Get expert analysis and data-driven insights with our digital issue and podcast

See what's new

Get in touch

Sean Joyce

Partner, Global Cybersecurity and Privacy Leader, PwC United States

Email

Norbert Vas

Cyber, Risk and Regulatory Services, Director, PwC United States

Email

PwC office locations Site map Contact us

Legal notices Privacy Cookie policy Legal disclaimer Terms and conditions