MIT Technology Review Insights

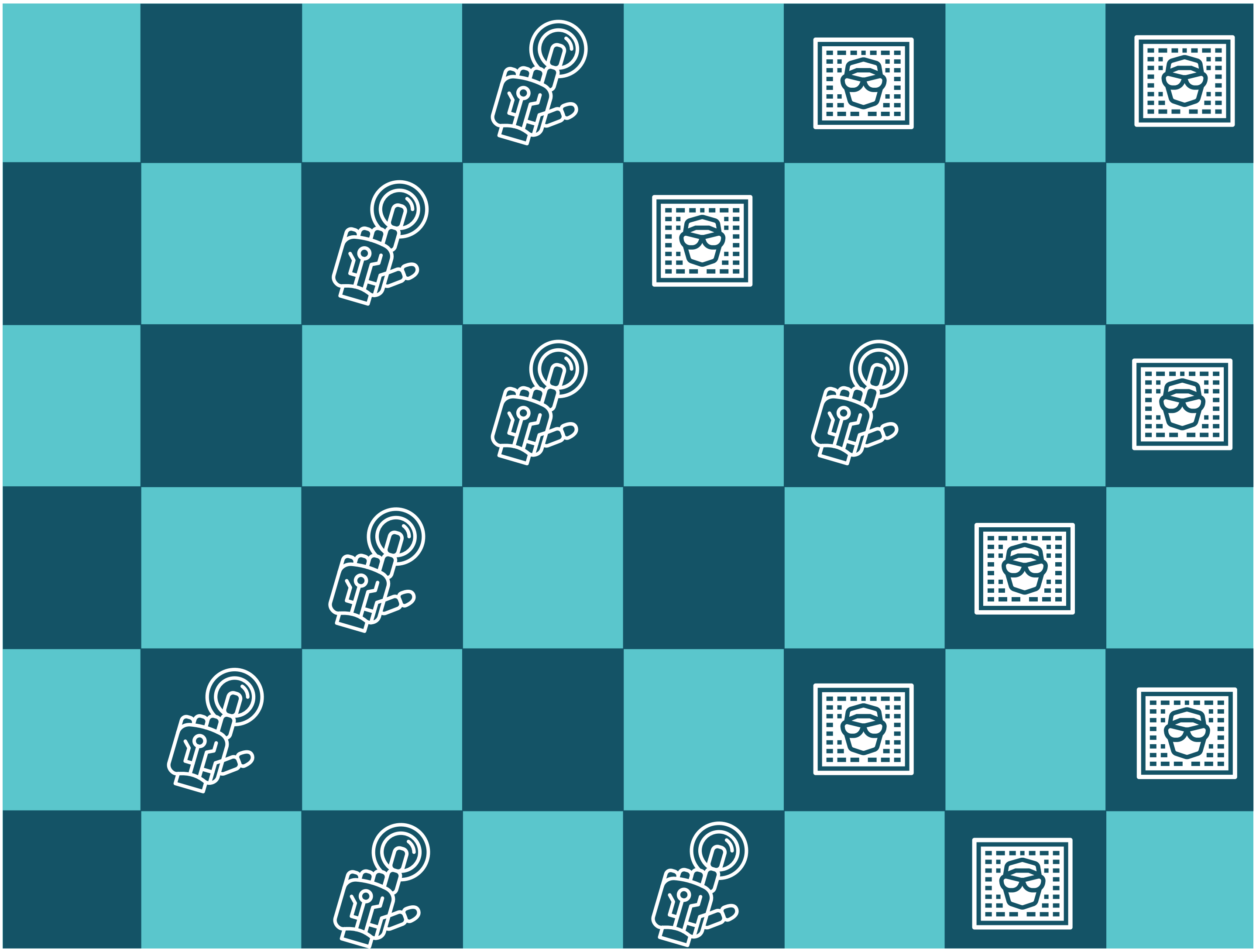
Produced in association with

enterprise.nxt

A digital publication from
Hewlett Packard Enterprise

IT security tools are becoming increasingly sophisticated thanks to artificial intelligence, but advances in the cybercriminal world are close behind.

An innovation war: Cybersecurity vs. cybercrime



EBSCO Industries started using a cybersecurity tool that uses artificial intelligence (AI) to hunt down and help eliminate breaches. Soon after, security analysts at the information services company found failed login attempts the product had ignored. Thinking the unsuccessful sign-ons might signal a cyberattack, the security team launched a manual investigation.

"It was an employee who put his password in wrong," says John W. Graham, global chief information security officer (CISO) at EBSCO, a $2.8 billion conglomerate. It took the team two hours to research the issue; they won't waste time on that again. Instead, they'll trust the tool.

Graham's experience is typical of how AI technology buys back security analysts' time and resources. Some 61% of corporations can't detect breaches without AI-driven cybersecurity technology, according to a study from Capgemini.[1] But for every advance in cybersecurity that puts organizations ahead, there are new cybercrime enhancements that set them back again.

Key takeaways

1 Cybersecurity tools outfitted with AI are helping organizations fend off attacks, but criminal hackers are using AI, too, and their attacks are more refined – and dangerous.

2 Innovation on both sides will continue: Information security software will get better yet at detecting and eliminating threats, and cybercrime tools will find cleverer ways of infiltrating defenses.

3 To stay ahead, organizations need a combination of the latest technologies, communications with government agencies, and inventive thinking about cybersecurity methodologies and practices.

Cybercrime tools that incorporate AI are outstripping their cybersecurity counterparts – malware today can pinpoint their targets from millions, generate convincing spam, and infect computer networks without being detected. All this raises the question – and it's a tough one – can cybersecurity innovations keep pace with cybercrime? They can, if companies use the same original thought and invention that sustains the war, turning not just to technology, but also communications with government agencies and new ways of thinking about cyber defense.

"With AI toolkits now available commercially, it will only be a matter of time before more and more attackers take advantage of these toolkits to create AI-based attacks."

Saumitra Das, Co-founder, Blue Hexagon

AI: A new hope

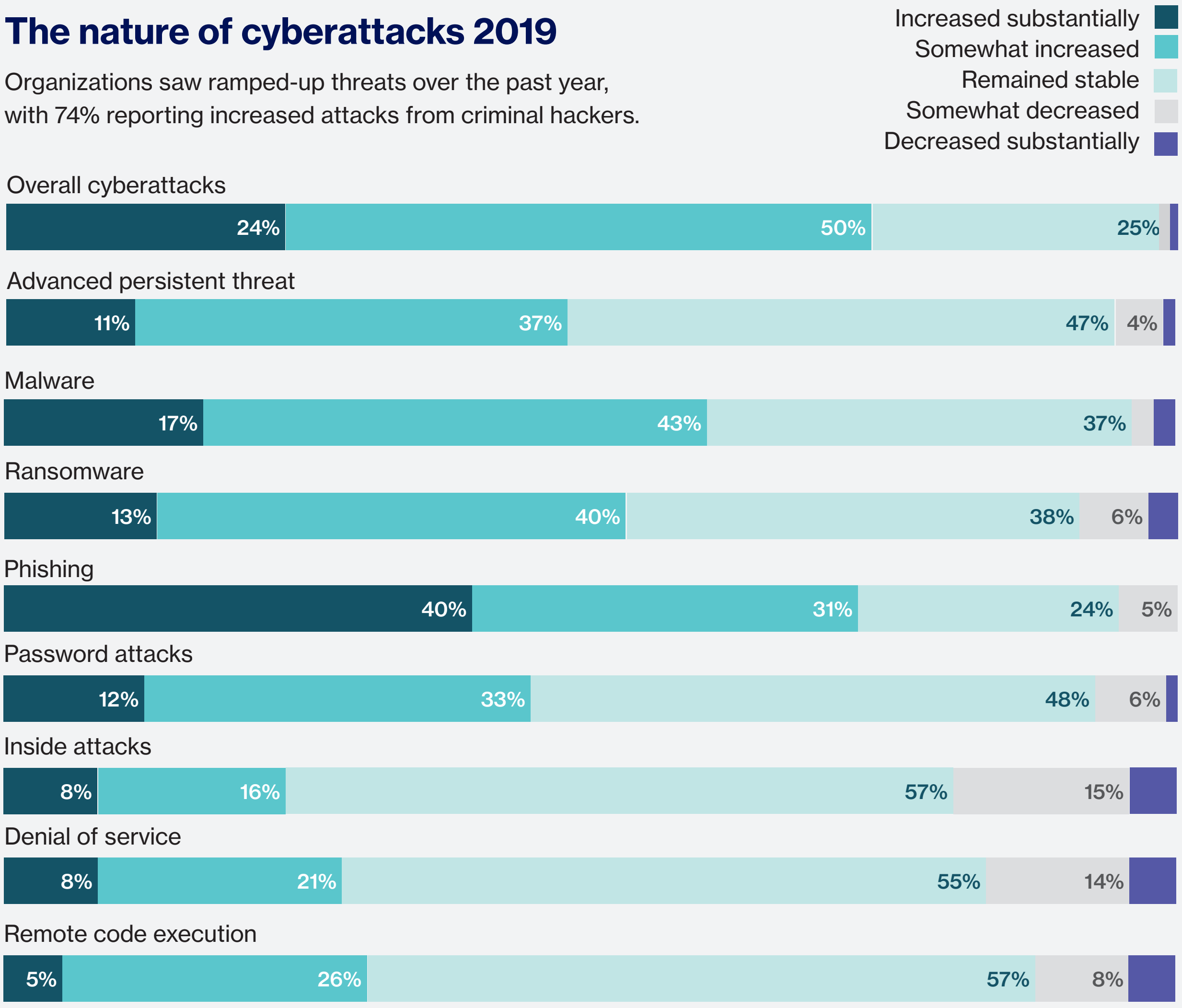
In 2018, high-profile breaches at social media sites Facebook and Google+, Marriott, and Cathay Pacific Airlines compromised the personal information of millions of people worldwide, giving the distinct impression that the criminal hackers had the advantage. Another sign: Phishing attacks rose by 27.5%.

But AI is giving companies a fighting chance. AI tools can scan vast amounts of data and then use machine learning (ML) algorithms to look for patterns, learn how cyberattacks begin, and guide human decision-makers on how to respond. Some 61% of organizations expect investments in AI-enabled cybersecurity to grow as AI technology matures, according to a study from The Ponemon Institute, a research center focused on privacy, data protection, and information security policy.[2]

At EBSCO, Graham is pleased with his investment in AI with Stellar Cyber's unified security analytics platform, a security information and event management system that distinguishes cyberattacks from benign network activity. The tool has augmented Graham's IT security teams. "We've put junior teams in front of the Stellar Cyber tool, and they made valid decisions," says Graham.

AI in cybersecurity has other advantages. In some use cases, AI applications learn how cybercrime applications operate. Cybersecurity vendor Blue Hexagon has applied deep learning, an ML variant that mimics human brain activity, to recognize deepfakes, says co-founder Saumitra Das. Deepfakes allow imposters to impersonate people in video and audio with alarming accuracy. They've been a growing concern. Recently, a criminal hacker used an AI-generated deepfake audio to trick a CEO into wiring $243,000 to a bank account.

Blue Hexagon also detects attacks the industry has never seen before – virtually every family of malicious software now acts like a zero-day attack, so there are no known defenses, says Das. And cybercriminals are creating new "multi-vector" attacks, targeting multiple points of entry into an organization; so instead of infecting a business application at an organization, they might target the network and individual computers simultaneously.



The nature of cyberattacks 2019

Organizations saw ramped-up threats over the past year, with 74% reporting increased attacks from criminal hackers.

Source: MIT Technology Review Insights' 2019 cybersecurity survey of 303 business professionals

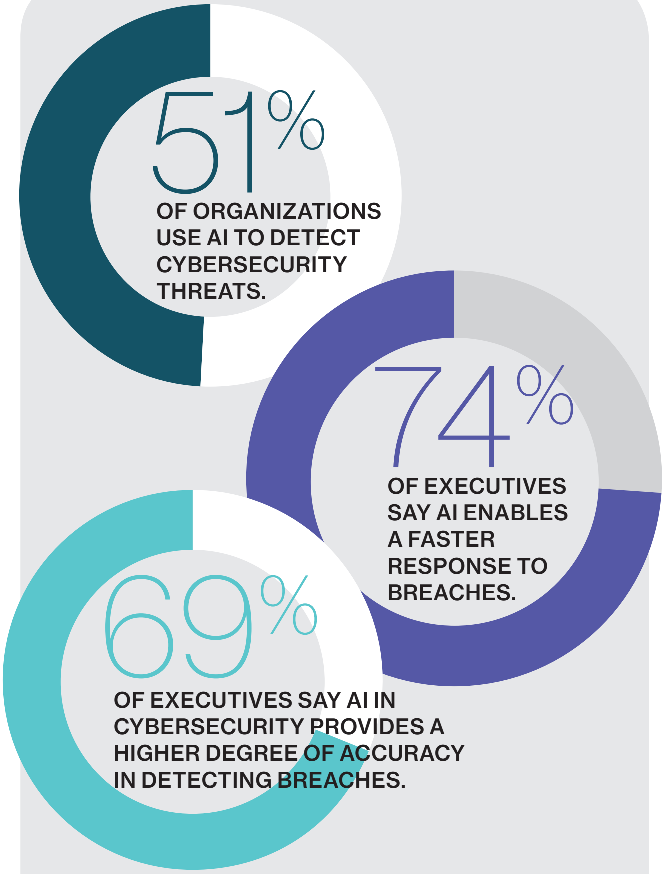
"More than 350,000 new samples of malicious software are generated each day," says Das. "These numbers translate to more than 230 new samples a minute and nearly four new samples every second."

Cybercrime gets personal

AI is the technology of choice for enhancing cyberattacks because it accelerates and automates tasks that criminal hackers previously did manually. For example, AI ingests and analyzes vast amounts of data about a victim company's networks and systems. It scrutinizes its people, too, and how they interact with one another – and it does it all at light speed. AI generates more insights from analyses for the criminal hackers to use and follow up on than they could produce on their own. Cybercriminals will use AI for nefarious purposes, weaponizing AI to attack your business, a Forrester Research study warns.[3]

> "Public and private partnerships need to analyze the dark web and understand the actors, intent, impacts, and potential methodologies of the next attacks."
> Spandan Mahapatra, Global Head of Business Solutions, Tata Consultancy Services

In recent years, cybercriminals have moved from casting a wide net on their prey to hyperfocusing their attacks, and they've used AI to do it. The targets are organizations where proprietary business information, consumer records, or the amount of funds are desirable. Phishing, for example, is a fraudulent attempt to obtain confidential information from masses of people through emails with infected links or attachments. Spear-phishing, in contrast, targets specific individuals or companies, using information about the targets against them. Traditionally, it's a time-consuming task – a hacker does research on, say, a bank, then composes a message that people who work in the bank will think is genuine. Now cybercriminals can use ML to automate heaps of targeted messages in a flash.[4]



Source: Capgemini Research Institute's "Reinventing Cybersecurity with Artificial Intelligence"

Addressing business email compromise (BEC) is among the Gartner Top 10 Security Projects for 2019. Similar to spear-phishing, BEC attacks rely on emails that appear to come from ranking executives so the hackers can trick the recipient, often the chief financial officer, into transferring funds to the hacker. Cybercriminals use AI to learn business users' communication patterns to mimic their writing styles and automatically compose increasingly convincing content. They're also using deepfake techniques, particularly audio impersonations of executives, in BEC attacks. It goes like this: After victims get an email purportedly from an executive, they get a phone call from a hacker impersonating the same exec, adding credibility to the ploy.

The financial fallout from BEC attacks is significant: The cost to US business was $1.3 billion in 2018. The risk of phishing and BEC attacks is that whatever payload they carry into an organization will infect its business. For example, phishing attacks that carry ransomware are peaking in the transportation industry, according to

Sharon Reynolds, president of InfraGard, a nonprofit that facilitates information sharing among public and private organizations. In August, a ransomware attack hit 22 towns in Texas simultaneously, affecting local agencies and prompting a federal investigation.

And in the not-far-off future, criminal hackers could use existing AI to create evasive malware, research from Malwarebytes shows.[5] For example, AI-enabled worms that get caught trying to infect a company's system could learn how they were detected – and then avoid that behavior in a later attempt. Trojans that exploit AI to elude surveillance are another potential threat.

"Just like in defense, hackers who deploy advanced tactics like worms and Trojans also have the power of AI and the cloud," says Tony Velleca, CISO at UST Global, a digital technology services company. "Like the Cold War, it is becoming AI versus AI."

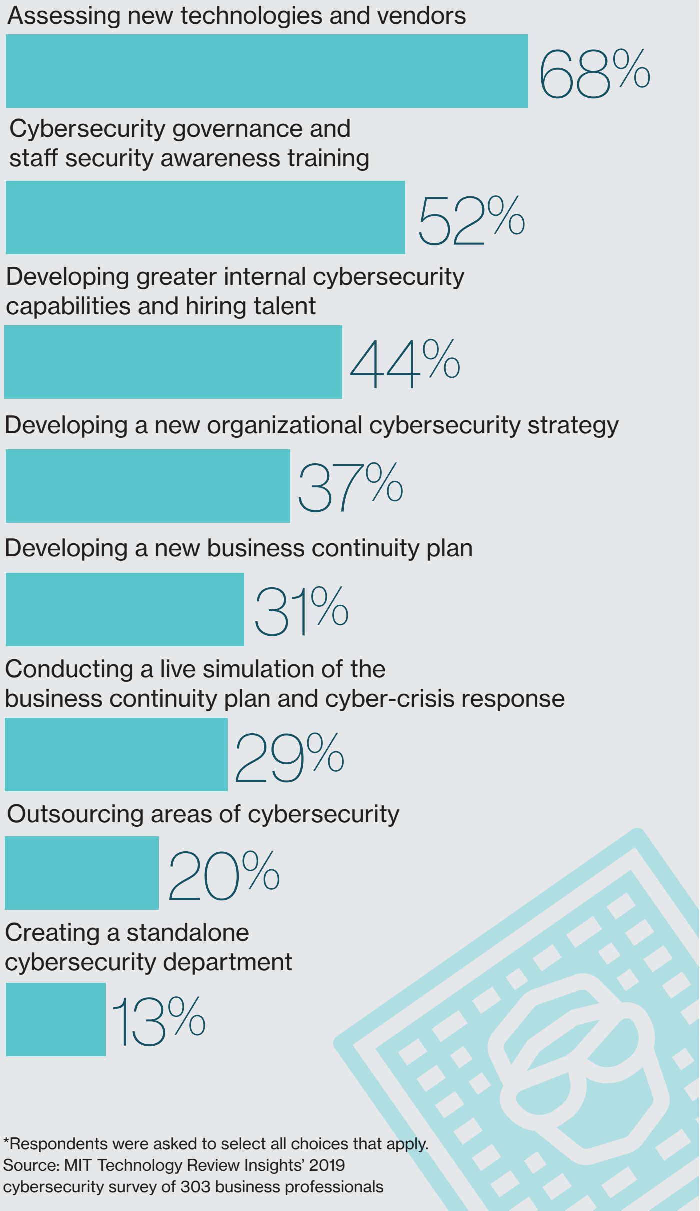
'A difficult problem'

Criminal hackers are prolific because their resources are vast and rich. Some get their hands on technology leaked from nation-states, which have prodigious financial backing to sabotage elections, as Russia did in the 2016 presidential race, or steal trade secrets. Others do their dealings in plain sight. They have access to the same publicly available AI technology that cybersecurity companies do. This technology includes tools such as TensorFlow, an open source ML-infused software library. Cybercriminals use AI tools – often sourced via the dark web, a collection of websites that hide their IP addresses – and automation to accelerate attacks and launch them on a grander scale. This capability is one of the biggest challenges for companies today, according to Das.

"Hackers are now specializing in different types of threats and making their AI toolkits available for other hackers to use, as well. With AI toolkits now available commercially, it will only be a matter of time before more and more attackers take advantage of these toolkits to create AI-based attacks," says Das.

Shielding against attacks

As cybercriminal threats get more sophisticated and frequent, organizations are tweaking, rethinking, and even overhauling their IT security strategies.



*Respondents were asked to select all choices that apply.
Source: MIT Technology Review Insights' 2019 cybersecurity survey of 303 business professionals

> "Higher security must be gained by going beyond generally known security controls and tools."
>
> Tony Velleca, CISO, UST Global

There are also human and technology challenges. It's hard to get all the security tools and employee education working right for combating BEC attacks, for example, says Reynolds. Businesses have to apply software patches to security holes, screen emails for attacks, and train employees to report suspicious emails and not click on links and attachments.

But software patching has its penalties. If a patch alters a system running software and breaks the software, you suffer because you patched. And security tools, training, and patching all cost money. "It's a difficult problem, and that's why attackers are so successful," says Reynolds.

Email filters send alerts when they detect signs of an attack, but they'll never catch all phishing or BEC attacks, because email filters don't think independently. They use a kind of template of words, phrases, and characters that often appear in attacks, and scan the email to see what matches the template. If there's a 67% match, for example, the system is going to trigger what is known as a false positive – that is, identify it as an attack whether it is or not. If it's not 67% sure, it's going to say it's not an attack, but maybe it still is. And employee education is not foolproof. People who are embarrassed they fell for an attack that got through the filters may stay silent, Reynolds says. "Reporting it can be a shameful process."

Updating your cybersecurity practices

Organizations can innovate on basic blocking, tackling, and hygiene in the following ways:

1 Take advantage of vendors that can institute secure settings in their products before they ship and provide guarantees that they have a supply chain that is secure.

2 Develop relationships with managed security service providers, value-added resellers, and vendors. Determine what to entrust to someone else to help to get those economies of scale, advises Sharon Reynolds, president of InfraGard, a partnership between the FBI and the private sector.

3 Do the free stuff first before you buy. "We buy things, not realizing that there were other configurations that we could've put in place," says Reynolds. "Have discussions with your major providers to find out new features that you can turn on and configure on your end."

4 Select a technology vendor that builds security into its systems instead of bolting it on.

Then there are challenges in the marketplace. The cybersecurity vendor landscape is so crowded it's difficult for people to figure out what they should use, according to Graham. He points to the annual RSA Conference, a cybersecurity convention where vendors show their wares. The conference has gotten so big over the years, "it's difficult to go and consume what's available," he says.

What could change for the better

The convention of making cybersecurity investments, maintaining security hygiene, and following best practices is seeing an evolution. US companies are increasingly interested in learning about their adversaries, whether nation-states or cybercriminals more generally. By enlisting partners as well as government agencies such as the FBI, companies can keep pace with new threats rather than succumb to them.

In cyber defense, a community-based approach is one of the best ways to interpret new data sources and security events in real time, according to Spandan Mahapatra, global head of business solutions at Tata Consultancy Services, an IT consulting company. A feedback loop between government agencies and corporations about emerging threats will lead to a stronger security posture across the entire cyber supply chain, Mahapatra says. "Public and private sector partnerships need to analyze the dark web and understand inside-out the actors, intent, impacts, and potential methodologies of the next attacks."

But rigorous adherence to cybersecurity best practices doesn't keep pace with cybercrime innovations automatically. In truth, a regulatory framework can sometimes enable attackers, says Velleca. "It can be a roadmap for expert hackers."

For example, a published capability in a security product allowed a criminal hacker to easily turn it off remotely, Velleca says. The information on how to do these kinds of things is commonly available in sources like sales tools.

Organizations need more data scientists, versus software developers, and more cloud architects, versus infrastructure architects, Velleca says. There's also a need for experienced "white hat" hackers – the good guys – and threat intelligence teams.

"Higher security must be gained by going beyond generally known security controls and tools," says Velleca. "We will still require the innovation in preventative solutions, but I believe there will be a shift to consolidated, integrated solutions – or the integration of data – allowing more focus on detection and planned response."

An AI for an AI

Reports from information security pros that include details of the latest threats they are seeing demand unceasing development of cybersecurity technologies to counter new attacks. "As the attacks evolve, so do the tactics and tools for cybersecurity," says Das. "Techniques like machine learning enable both attackers and defenders to be faster, which then requires both sides to constantly innovate and develop new techniques to be faster than the other."

AI is every bit an answer, and more than a stopgap, for finite cybersecurity expertise, an increasing cause of security incidents and security analyst burnout. AI augments the expertise and experience of security analysts, shouldering the load for repetitive tasks so they can protect data and networks and get ahead of attackers, says Das. Then security professionals can return to core priorities and make their organizations more secure.

"AI-based cybersecurity is the only way for businesses to stay ahead. Attackers will innovate in response as part of the cat-and-mouse game of cybersecurity, but with AI it will be a much tougher endeavor," says Das.

For Velleca, AI in the hands of bad guys means cybersecurity pros have little choice but to be faster and smarter – and then faster and smarter than that.

"The entry of AI technology into the threat actors' toolkit will represent a game changer for the cybersecurity community. AI in the hands of threat actors requires the development of a new breed of cyber detection and response methodologies and experts," Velleca says. "Only the companies that have access to the best cyber experts will be insulated from the impact of AI launched attacks."

IT security weak spots

Organizations assessing their cybersecurity postures identify numerous vulnerabilities, including insufficient staff training, employees' mobile devices, and social media breaches.*

40%
Staff training has not kept pace with the evolving nature of cyberthreats

31%
Lack of internal cybersecurity discipline

30%
Breaches relating to smartphones, tablets, and other remote devices

29%
Insufficient ability to detect serious breaches quickly enough

26%
Lack of internal cybersecurity talent of expertise

21%
Outdated, legacy security controls

20%
Breaches related to social media

18%
Breaches affiliated with the internet of things

*Respondents were asked to select up to three choices.
Source: MIT Technology Review Insights' 2019 cybersecurity survey of 303 business professionals

An innovation war: Cybersecurity vs. cybercrime is an executive briefing paper by MIT Technology Review Insights. It is based on research and interviews conducted in August and September 2019. We would like to thank all participants as well as the sponsor, Enterprise.nxt, a digital publication from Hewlett Packard Enterprise. MIT Technology Review Insights has collected and reported on all findings contained in this paper independently, regardless of participation or sponsorship. Jason Sparapani was the editor of this report, and Nico Crepaldi was the publisher.

About MIT Technology Review Insights

MIT Technology Review Insights is the custom publishing division of *MIT Technology Review*, the world's longest-running technology magazine, backed by the world's foremost technology institution – producing live events and research on the leading technology and business challenges of the day. Insights conducts qualitative and quantitative research and analysis in the US and abroad and publishes a wide variety of content, including articles, reports, infographics, videos, and podcasts. And through its growing MIT Technology Review Global Panel, Insights has unparalleled access to senior-level executives, innovators, and thought leaders worldwide for surveys and in-depth interviews.

From the sponsor

Hewlett Packard Enterprise is a global technology leader focused on developing intelligent solutions that allow customers to capture, analyze, and act upon data seamlessly from edge to cloud. HPE enables customers to accelerate business outcomes by driving new business models, creating new customer and employee experiences, and increasing operational efficiency today and into the future.

Hewlett Packard
Enterprise

enterprise.**nxt**

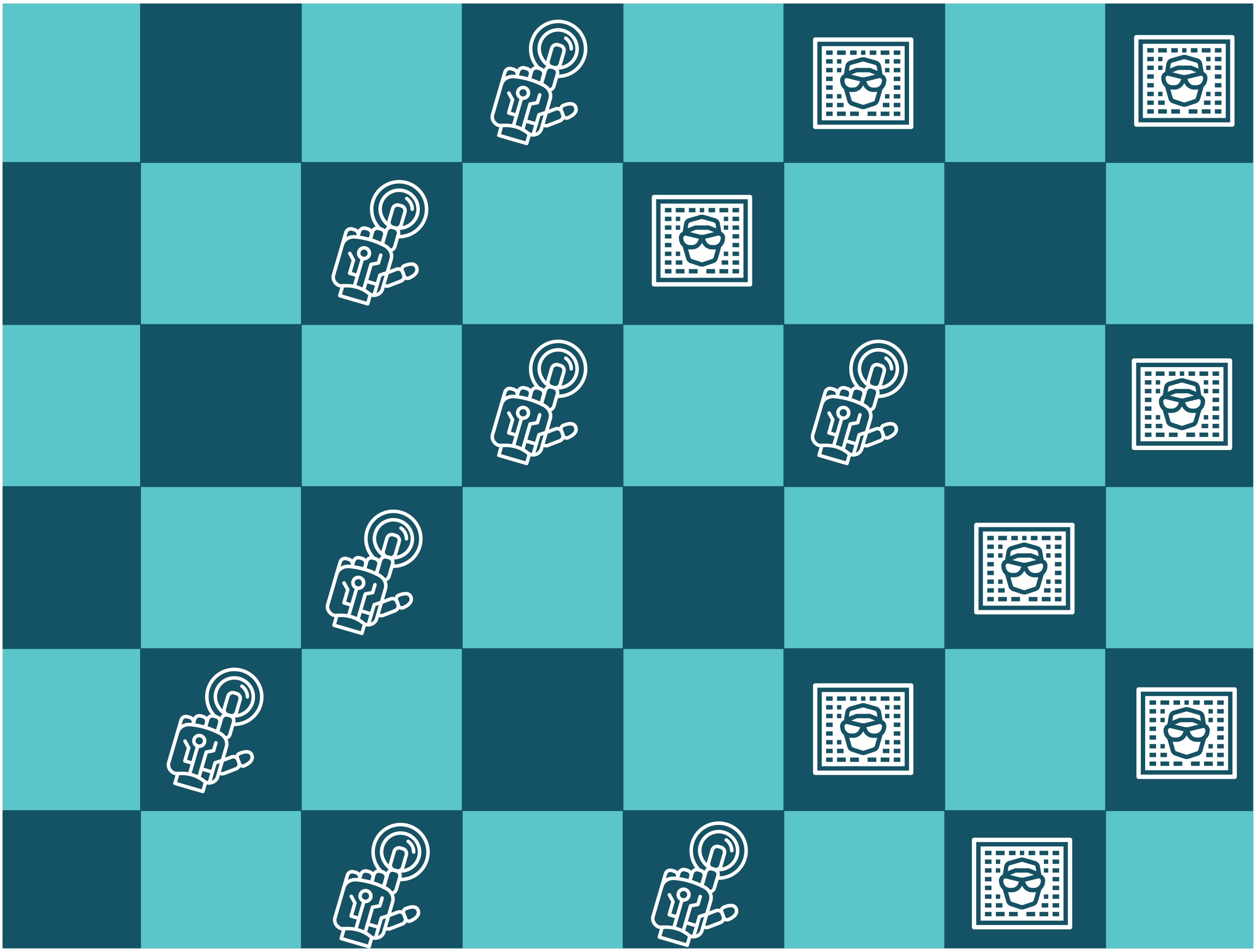
A digital publication from
Hewlett Packard Enterprise

Footnotes

1. "Reinventing Cybersecurity with Artificial Intelligence," Capgemini Research Institute, https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf.
2. "The Value of Artificial Intelligence in Cybersecurity," Ponemon Institute, July 2018.
3. Chase Cunningham and Joseph Blankenship with Stephanie Balaouras, Srividya Sridharan, Bill Barrigham, and Peggy Dostie, "Using AI For Evil," Forrester Research, April 16, 2018.
4. John Seymour and Philip Tully, "Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter (presented at Black Hat USA 2016, Las Vegas, July 30–Aug. 4, 2016), https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter.pdf.
5. "When artificial intelligence goes awry: separating science fiction from fact," Malwarebytes Labs, 2019, https://resources.malwarebytes.com/files/2019/06/ Labs-Report-AI-gone-awry.pdf.

Illustrations
Illustrations by Chandra Tallman with icons by The Noun Project

While every effort has been taken to verify the accuracy of this information, MIT Technology Review Insights cannot accept any responsibility or liability for reliance by any person in this report or any of the information, opinions, or conclusions set out in this report.



MIT Technology Review Insights

🌐 insights.techreview.com

🐦 @techreview @mittr_insights

✉ insights@technologyreview.com