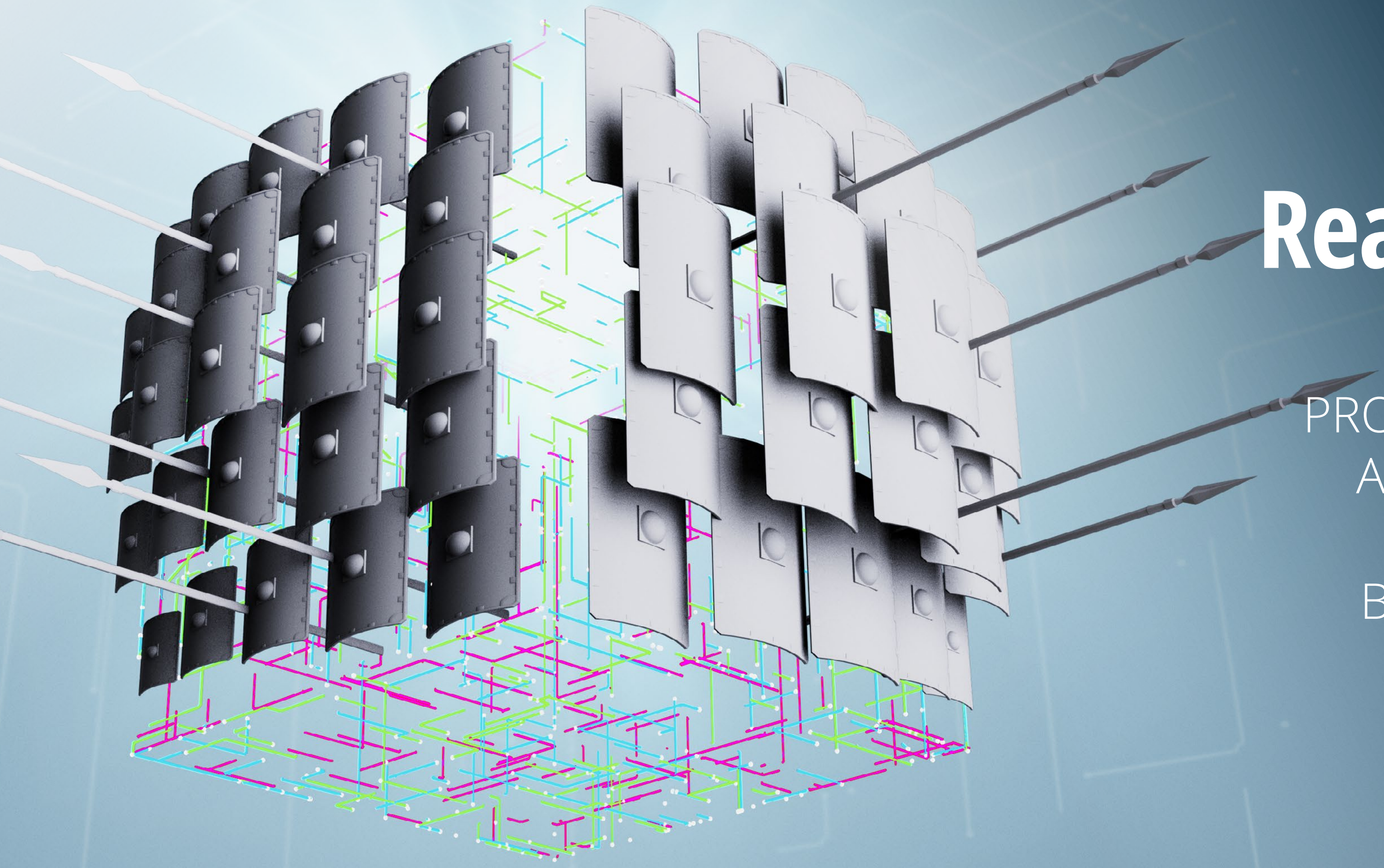


Cyber AI: Real defense

PROTECT EXPANDING ATTACK SURFACES

Enterprise vulnerability is increasing as ever more systems and data are exposed online.

BRIDGE THE CYBER TALENT GAP

AI can help enterprises address their chronic shortage of cybersecurity talent.

FIGHT FIRE WITH FIRE

AI-driven security tools will likely be the best defense against emergent AI-driven security threats.

TREND 5

Cyber AI: Real defense

Augmenting security teams with data and machine intelligence

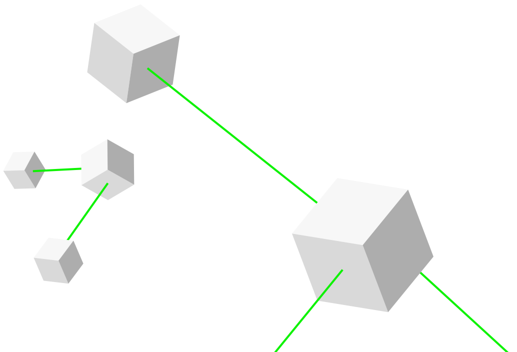
Despite making significant investments in security technologies, organizations continue to struggle with security breaches: Their adversaries are quick to evolve tactics and stay ahead of the technology curve. Humans may soon be overwhelmed by the sheer volume, sophistication, and difficulty of detecting cyberattacks.

People are already challenged to efficiently analyze the data flowing into the security operations center (SOC) from across the security tech stack. This doesn't include the information feeds from network devices, application data, and other inputs across the broader technology stack that are often targets of advanced attackers looking for new vectors or using new malware. And as the enterprise increasingly expands beyond its firewalls, security analysts are charged with protecting a constantly growing attack surface.

Meanwhile, the cost of cybercrime continues to climb; it's expected to double from US$3 trillion in 2015 to US$6 trillion by the end of 2021 and grow to US$10.5 trillion by 2025.[1] The average cost of a single data breach in 2021 was US$4.24 million,[2] a 10% increase from 2019.[3] According to insurer AIG, ransomware claims alone have grown 150% since 2018.[4]

It's time to call for AI backup. Cyber AI can be a force multiplier that enables organizations not only to respond faster than attackers can move, but also to anticipate these moves and react to them in advance. Cyber AI technology and tools are in the early stages of adoption; the global market is expected to grow by US$19 billion between 2021 and 2025.[5]

AI's ability to adaptively learn and detect novel patterns can accelerate detection, containment, and response, easing the burden on SOC analysts and allowing them to be more proactive. Bonus: It can help organizations prepare for the eventual development of AI-driven cybercrimes.



Expanding enterprise attack surfaces

Organizations' attack surfaces are exponentially expanding. As discussed in *The tech stack goes physical*, the adoption of 5G networks and an increase in network connections, together with a more distributed workforce and a broadening partner ecosystem, may present new risks. They're exposing the enterprise outside of its firewalls and pushing it into customer devices, employee homes, and partner networks.

More remote workers. Before COVID-19, only about 6% of employees worked from home. In May 2020, about 35% of them did.[6] In the first six weeks of the 2020 lockdown, the percentage of attacks on home-based workers increased fivefold from 12% to 60%.[7] One survey found that 51% of respondents saw an increase in email phishing after shifting to a remote working model.[8]

For many workers, remote work is expected to remain the rule, not the exception, providing cybercriminals with many new opportunities. For example, outside of the safety of corporate firewalls and web security gateways, remote workers are easier to target. They rely on home networks and VPN connections and often use unsecured devices to access cloud-based apps and data. And legacy on-premises security equipment is typically designed to support enterprise-grade networks, not home-based internet access.

As the enterprise extends into its employees' homes, user behavior and data activity become more diverse and deviate from previous norms. With employees logging in from atypical locations and devices at unusual times, it can be more challenging to identify anomalous behaviors, potentially leading to an increase in false positives.

Increase in network-connected devices. 5G, IoT, Wi-Fi 6, and other networking advances are driving an increase in network-connected devices. When seeking a soft attack vector, cybercriminals will be able to choose from a growing number of network-connected physical assets—29.3 billion by 2023, according to one estimate.[9]

The unprecedented number of devices connected to these networks produce data that needs to be processed and secured, contributing to the data logjam in the SOC. It can be challenging to keep track of and manage active assets, their purpose, and their expected behavior, especially when they're managed by service orchestrators.

Rather than being centrally located and controlled, many of these devices are spread across various remote locations, operating in multiple edge environments where they collect data to send back to the enterprise. Without proper security precautions, devices can be compromised and continue to appear to operate normally on the network, essentially becoming intruder-controlled bots that can release malicious code or conduct swarm-based attacks.

It can be challenging to keep track of and manage active assets, their purpose, and their expected behavior, especially when they're managed by service orchestrators.

Broader ecosystem of third-party partners. An increasingly global supply chain and hosted data, infrastructure, and services have long contributed to third-party risk. And as more and more organizations integrate data with third-party applications, APIs are a growing security concern. Gartner predicts that by 2022, API abuses will become the enterprise's most frequent attack vector.[10]

Third-party breaches are growing in complexity. Five years ago, an intruder might use widely available malware to target specific computer systems, gain contractor credentials, and steal customer data—messy, to be sure, but with a clear source and the ability to monitor and remediate the damage.

Such an attack pales in comparison to today's sophisticated intrusions, in which information stolen from one company can be used to compromise thousands of its customers and suppliers. Supply chain attacks can do the same by exploiting the least-secure embedded components of complex supply networks. A breach with no boundaries can be nearly impossible to monitor and remediate, with active theft potentially continuing for many years.

Adoption of 5G networks. 5G is expected to completely transform enterprise networks with new connections, capabilities, and services. But the shift to 5G's mix of hardware- and distributed, software-defined networks, open architectures, and virtualized infrastructure will create new vulnerabilities and a larger attack surface, which will require more dynamic cyber protection.

5G networks can support up to a million connected devices per square kilometer—compared to only 100,000 for 4G networks[11] —enabling highly scalable and densely connected environments of devices. By 2025, market watchers predict there will be 1.8 billion

5G mobile connections (excluding IoT), up from 500 million in 2021;[12] and about 3.7 billion cellular IoT connections, up from about 1.7 million in 2020.[13]

As public 5G networks expand, organizations in government, automotive, manufacturing, mining, energy, and other sectors have also begun to invest in private 5G networks that meet enterprise requirements for lower latency, data privacy, and secure wireless connectivity. From autonomous vehicles and drones to smart factory devices and mobile phones, an entire ecosystem of public and private 5G network–connected devices, applications, and services will create additional potential entry points for hackers. Each asset will need to be configured to meet specific security requirements. And with the increasing variety of devices, the network becomes more heterogenous and more challenging to monitor and protect.

AI defense against today's cyberthreats

Expanding attack surfaces and the escalating severity and complexity of cyberthreats are exacerbated by a chronic shortage of cybersecurity talent. Employment in the field would have to grow by approximately 89% to eliminate the estimated global shortage of more than 3 million cybersecurity professionals.[14] AI can help fill this gap.

Accelerated threat detection. Threat detection was one of the earliest applications of cyber AI. It can augment existing attack surface management techniques to reduce noise and allow scarce security professionals to zero in on the strongest signals and indicators of compromise. It can also make decisions and take action more rapidly and focus on more strategic activities.

Advanced analytics and machine learning platforms can quickly sift through the high volume of data generated by security tools, identify deviations from the norm, evaluate the data from the thousands of new connected assets that are flooding the network, and be trained to distinguish between legitimate and malicious files, connections, devices, and users.

AI-driven network and asset mapping and visualization platforms can provide a real-time understanding of an expanding enterprise attack surface. They can identify and categorize active assets, including containerized assets, which can provide visibility into rogue asset behavior. Supply chain risk management software incorporating AI and machine learning can automate the processes of monitoring physical and digital supply chain environments and tracking the way assets are composed and linked.

Force multiplier in containment and response. AI can also serve as a force multiplier that helps security teams automate time-consuming activities and streamline containment and response. Consider machine learning, deep learning, natural language processing, reinforcement learning, knowledge representation, and other AI approaches. When paired with automated evaluation and decision-making, AI can help analysts manage an escalating number of increasingly complex security threats and achieve scale.

For example, like its predecessors, 5G is vulnerable to jamming attacks, in which attackers deliberately interfere with signal transfer. Researchers from the Commonwealth Cyber Initiatives at Virginia Tech and Deloitte, who are collaborating to understand 5G network security design and implementation, are working to identify low-level signal jamming before it brings down the network. By implementing an AI-based interference scheme and machine learning models, a real-time vulnerability assessment system was developed that could detect the presence of low-level signal interference and classify jamming patterns.[15]

Automation can help maximize AI's impact and shrink the time between detection and remediation. SOC automation platforms embedded with AI and machine learning can take autonomous, preventative action—for example, blocking access to certain data—and escalate issues to the SOC for further evaluation. When layered on top of the API management solutions that control API access, machine learning models trained on user access patterns can inspect all API traffic to uncover, report on, and act on anomalies in real time.

Proactive security posture. Properly trained AI can enable a more proactive security posture and promote cyber resilience, allowing organizations to stay in operation even when under attack and reducing the amount of time an adversary is in the environment.

For example, context-rich user behavior analytics can be combined with unsupervised machine learning algorithms to automatically examine user activities; recognize typical patterns in network activity or data access; identify, evaluate, and flag anomalies (and disregard false alarms); and decide if response or intervention is warranted. And by feeding intelligence to human security specialists and enabling them to actively engage in adversary pursuit, AI enables proactive threat hunting.

Organizations can leverage AI and machine learning to automate areas such as security policy configuration, compliance monitoring, and threat and vulnerability detection and response. For instance, machine learning–

driven privileged access management platforms can automatically develop and maintain security policies that help enforce zero-trust security models. By analyzing network traffic patterns, these models can distinguish between legitimate and malicious connections and make recommendations on how to segment the network to protect applications and workloads.

Pairing vulnerability analysis and reinforcement learning, security specialists can generate attack graphs that model the structure of complex networks and reveal optimal attack routes, resulting in a better understanding of network vulnerabilities and reducing the number of staff required to conduct the testing. Similarly, cyberattack simulation tools can continuously mimic the tactics and procedures of advanced threats to highlight infrastructure vulnerabilities and routes for potential attack.

Evolving the role of human security analysts. In one survey of security analysts, 40% said their biggest pain point was too many alerts; 47% said it was hard to know which alerts to prioritize for incident response.[16] Another survey found that analysts increasingly believed their role was to reduce alert investigation time and the volume of alerts, rather than to analyze and remediate security threats. More than three-quarters of respondents reported an analyst turnover rate of more than 10%, with nearly half saying the rate was between 10% and 25%.[17]

AI can't replace human security professionals, but it can enhance their work and potentially lead to more job satisfaction. In the average SOC, AI and automation could eliminate the tedious functions of Tier 1 and Tier 2 analysts. (Tier 1 evaluates incoming data and decides to escalate problems, and Tier 2 responds to trouble tickets, assesses the scope of each threat, determines response and remediation actions, and escalates when required.) These analysts could be trained to function in more strategic roles that are more challenging to hire for, such as higher-level Tier 2 analysts and Tier 3 analysts who handle the thorniest security challenges and focus on proactively identifying and monitoring threats and vulnerabilities.

A table-stakes weapon against future AI-driven cybercrimes

The same features that make AI a valuable weapon against security threats—speedy data analysis, event processing, anomaly detection, continuous learning, and predictive intelligence—can also be manipulated by criminals to develop new or more effective attacks and detect system weaknesses.

For example, researchers have used generative adversarial networks—two neural networks that compete against each other to create datasets similar to training data—to successfully crack millions of passwords.[18] Similarly, an open-source, deep learning language model known as GPT-3 can learn the nuances of behavior and language. It could be used by cybercriminals to impersonate trusted users and make it nearly impossible to distinguish between genuine and fraudulent email and other communications.[19] Phishing attacks could become far more contextual and believable.[20]

Advanced adversaries can already infiltrate a network and maintain a long-term presence without being detected, typically moving slowly and discreetly, with specific targets. Add AI malware to the mix, and these intruders could learn how to quickly disguise themselves and evade detection while compromising many users and rapidly identifying valuable datasets.[21]

Similarly, an open-source, deep learning language model known as GPT-3 can learn the nuances of behavior and language.

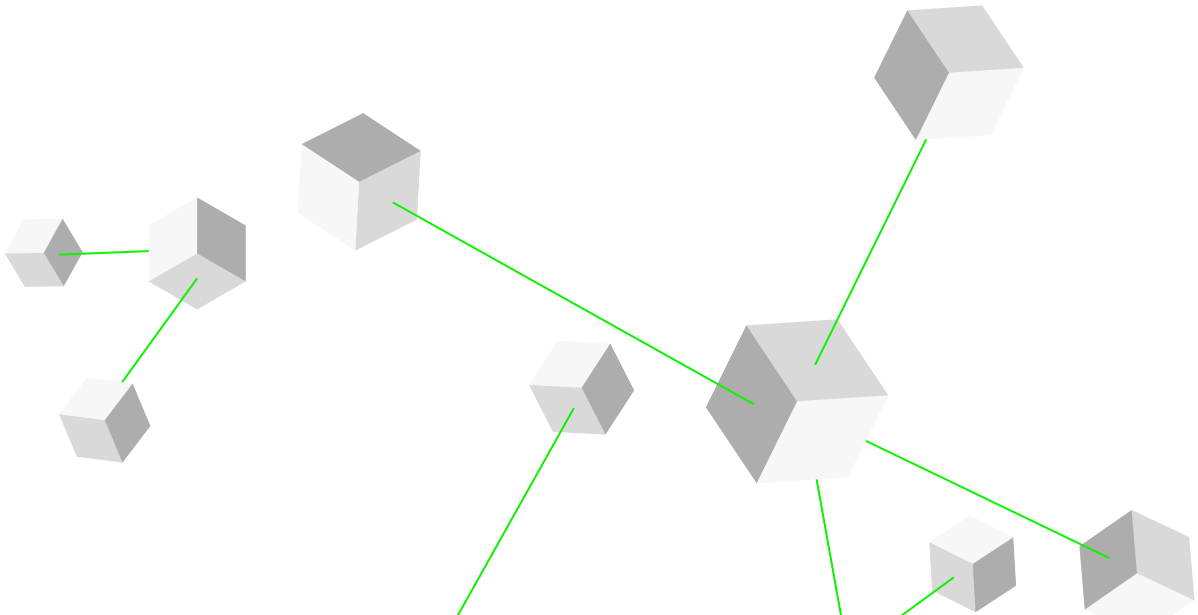
Organizations can help prevent such intrusions by fighting fire with fire: With enough data, AI-driven security tools can effectively anticipate and counter AI-driven threats in real time. For example, security pros could leverage the same technique that researchers used to crack passwords to measure password strength or generate decoy passwords to help detect breaches.[22] And contextual machine learning can be used to understand email users' behaviors, relationships, and time patterns to dynamically detect abnormal or risky user behavior.[23]

The way forward

Humans and AI have been collaborating to detect and prevent breaches for some time, although many organizations are still in the early stages of using cyber AI. But as attack surfaces and exposure outside of traditional enterprise networks continue to grow, AI offers more.

Approaches such as machine learning, natural language processing, and neural networks can help security analysts distinguish signal from noise. Using pattern recognition, supervised and unsupervised machine learning algorithms, and predictive and behavioral analytics, AI can help identify and repel attacks and automatically detect abnormal user behavior, allocation of network resources, or other anomalies. AI can be used to secure both on-premises architecture and enterprise cloud services, although securing workloads and resources in the cloud is typically less challenging than in legacy on-premises environments.

On its own, AI (or any other technology, for that matter) isn't going to solve today's or tomorrow's complex security challenges. AI's ability to identify patterns and adaptively learn in real time as events warrant can accelerate detection, containment, and response; help reduce the heavy load on SOC analysts; and enable them to be more proactive. These workers will likely remain in high demand, but AI will change their roles. Organizations likely will need to reskill and retrain analysts to help change their focus from triaging alerts and other lower-level skills to more strategic, proactive activities. Finally, as the elements of AI- and machine learning–driven security threats begin to emerge, AI can help security teams prepare for the eventual development of AI-driven cybercrimes.



LESSONS FROM THE FRONT LINES

Sapper Labs fights software with software

To help Canadian and US military, government, and critical infrastructure operators solve security challenges, Sapper Labs Cyber Solutions provides cybersecurity thought leadership, intelligence, R&D, implementation, operational security platforms, and training support to solve complex problems. AI is an increasingly important tool in Sapper Labs' technology toolkit.

The Ottawa-based cyber defense firm—which takes its name from the military term for combat engineers who support ground troops through surveillance, scouting, defense engineering, and other proactive defensive activities—starts its projects with the premise that every network, system, and capability is already compromised, and that organizations simply don't have the human resources to defend against or combat this. "The growth of the talent pipeline is not keeping pace with either the growth of the attack surface or the expansion of business and government innovation agendas, so we can't produce enough talent to protect our institutions and assets," says Al Dillon, Sapper Labs' cofounder and CEO. "That's where AI comes in for an assist."[24]

To that end, Sapper Labs is working with several Canadian and US security, defense, and intelligence organizations to create AI systems that aim to flex in real time with evolving threat tactics and procedures of our adversaries. These systems can do much more than inform decisions; they can learn how to defend themselves against threats, regardless of human engagement. "Today, cyber defenses that use machine learning, AI, and automation focus primarily on human-led cyber engagement," says Dillon. "Because of the pace of today's innovation and the proliferation of networks and devices, especially outside of the organization, we're going to need embedded automated system capabilities."

Dillon says the collective goal for national security and defense organizations and other public and private sector organizations should be to shift toward military-grade, software-led engagement: AI-driven software defending—and fighting back against—AI-enabled adversaries. "We're all under threat of attack by nation-state actors and other bad actors with equivalent intent, expertise, and tools," he explains.

For example, Sapper Labs and government agencies are developing a multilayered threat detection system that fuses information and data feeds from a variety of sources, known as all-source intelligence—from satellite-, land-, and sea-based sensors to digital sources such as social media and other public and private network information. Examining this data in the traditional manner might take human-led security teams months or even years. Automating the process of synthesizing this data and intelligence and applying algorithms to it enables evaluation and decision-making to take place 10 or even 15 times faster than with conventional methods. Within three years, Dillon expects cyber AI and automation technologies to have advanced so far that they will be able to evaluate intelligence, reach a conclusion, and make a decision 50 times faster than in the past.

Therein, says Dillon, lies one of cyber AI's toughest problems. "Overcoming the people, societal, and cultural challenges to cyber AI will be far more difficult than solving technology problems," he says. "The biggest hill to climb will be getting people to trust decisions made by AI when they're more comfortable with decisions made by human leaders, even if it takes 50 times longer to get those decisions."

Education is one of the keys to building this trust. Through partnerships with other private companies, public-sector organizations, and academic institutions, Sapper Labs is working to help build awareness of automated cybersecurity more broadly. "We're in an exciting transition in terms of technology adoption and innovation, but it's alarming that we don't fully understand the societal impact with regards to defending national security, personal data, intellectual property, and other crown jewels," Dillon says. "We have to internalize that AI-enabled security platforms may become the only way that we can stay ahead of the bad actors."

MY TAKE

Mike Chapple

Information security leader and IT, analytics, and operations teaching professor, University of Notre Dame

Over the last year, the nature of cybersecurity attacks has transformed.

Previously, one of the main concerns for an organization would have been ransomware attacks, wherein bad actors would gain access to enterprise data through phishing or internet malware, and then encrypt that data to hold it for ransom. Such attacks were opportunistic because criminals would take advantage of whoever fell prey to malware, and they didn't always succeed if organizations were prepared with data backups.

The stakes are now higher because bad actors are engaging in organized crime, akin to cyberwarfare by nation-states. We've seen hospitals targeted during COVID-19 outbreaks, pipelines unable to deliver fuel, and other highly targeted attacks. The bad actors' new paradigm is to present two extortion threats on stolen enterprise data: holding the data hostage and threatening to leak sensitive information, including customer records and intellectual property. Such threats are especially salient for large organizations, which have the money and data desired by cybercriminals. Moreover, the attack surface for such crimes is ever-expanding as trends such as the adoption of 5G mobile networks and work-from-home policies push enterprise technology beyond its traditional borders.

How can organizations respond to this atmosphere of heightened risk? They have two options: hire more people, which is difficult because of the burgeoning skills gap in the talent market, or rely on AI, automation, and analytics to detect and respond to threats in real time. Due to recent shifts in technology, the latter option—cyber AI—is becoming increasingly effective.

The intersection of AI and cybersecurity has been talked about for nearly a decade. Until now, those conversations revolved around buzzwords and rule-based products. Thanks to advances in compute power and storage capacity, we now see cybersecurity vendors starting to truly incorporate machine learning and AI into their products. Today, large enterprises can rely on such vendors to advance threat intelligence.

Premier cybersecurity vendors have deployments across many enterprises, which serve as sensors for picking up data. By applying AI to the anonymized data from each customer, vendors can use the threat data from one organization to look for signs of similar breaches elsewhere. The network effects can be exponential: The bigger and more diverse the dataset, the more these vendors' detection improves, and the greater their protection. For this reason, medium and large enterprises alike could benefit from working with managed service providers. Or, alternately, they can have their data science and cybersecurity teams work together to train AI models in their own cybersecurity warehouses.

Today's computing power allows the development of sophisticated user and entity behavior analytics (UEBA) that detect signatures of bad actors or deviations from normal behavior. UEBA might flag a user who is detected downloading terabytes of data on a Saturday morning—certainly not a habit. By connecting these profiles and patterns, threats can be identified in a far more refined manner.

While these signals always existed, it was previously impractical to analyze them and draw meaningful patterns. Now, these AI-flagged threats can be fed into security orchestration, automation, and response (SOAR) platforms, which can shut down access or take any other immediate actions.

The history of cybersecurity, and really any type of security, is an age-old game of cat and mouse. Just as we develop AI tools to protect ourselves, antagonists are developing AI to further complicate their attacks. Nation-states are already entering this territory, and we may see more from private cybercrime actors in the next 18 to 24 months. If organizations don't want to be a victim, they'll want to act now to future-proof their users, systems, and data by seeking out opportunities for AI support. When the nature of cyberattacks inevitably transforms again, they can be ready.

MY TAKE

Adam Nucci

Deputy director of strategic operations, US Army

The US Army is in the midst of a modernization journey that requires us to adopt a data-driven mindset and embrace digital transformation.

The objective is to evolve not only weapons systems and platforms but also processes, workforce, and culture.

As we modernize, our already-complex technological environment is becoming even more dynamic, and we're challenged from all sides by a broad range of sophisticated adversaries. To meet our ambitious modernization goals, it's critical that we elevate our security posture. Fortunately, the future is now: The tools needed to do this effectively are here today. But a focused effort is required not only to use them for security but also to alter the ways in which capabilities, networks, and talent are delivered. It is vitally important to build in adaptive security. Massive amounts of data are being generated by technology systems and sensors. Advanced analytics techniques and platforms can be used to rapidly analyze and act upon this data. And the broad adoption of cloud computing enables real-time data-sharing as well as full-spectrum data and network management, control, and visibility.

We have the building blocks at hand. The powerful combination of data, analytics, and cloud computing serves as the foundation of zero trust–based security approaches centered on data rather than networks—especially the migration from network-based identity and credential management to data- and device-centric identity access management and least-privilege access principles. This sets the stage for the use of cyber AI at scale.

With machine learning, deep learning, and other AI techniques, organizations can understand the cybersecurity environment across multiple hardware and software platforms; learn where data is stored, how it behaves, and who interacts with it; and build attacker profiles and propagate them across the network environment. AI and predictive analytics can also help us better understand some of the human-related aspects of cybersecurity. Across the operational environment and broader society, the information dimension is woven inextricably into the fabric of just about everything; advanced machine learning and AI have the potential to help us understand how the information sphere impacts users, how we make decisions, and how adversaries behave.

Today's AI is not general-purpose; it's primarily fit-for-purpose solutions built for sometimes narrow but mostly specific use cases. But cybersecurity isn't a narrow problem that can be solved by technology alone; it's primarily a *people* problem. Our adversaries are diverse and creative. What makes them tick? To advance cyber AI, we need to bring that same variety and imagination to the cyber workforce. We need to cross-pollinate the traditional STEM-educated, linear-thinking cyber workforce with application mavericks and polymorphic thinkers who can draw inferences based on not-so-obvious connections. Not only does this add a human dimension to model building and training, it also creates a cybersecurity force multiplier.

Driven by data, analytics, and the cloud, an AI-driven cyber strategy enables organizations to predict, detect, and counter intrusions in an automated fashion. There are emerging challenges and opportunities in mobile and low-bandwidth environments, but the technology foundation is in place.

To further enable cyber AI, we also need stronger collaboration between the public and private sectors. Cybersecurity *is* national security. We as a society need to elevate cybersecurity from a bolt-on afterthought to the embedded backbone of all commercial and governmental systems. But the public sector can't succeed alone. With strong public-private partnerships and cross-pollination among industry, academia, and international partners, we can build an unshakeable cybersecurity foundation based on sensor-embedded systems, data, and AI-driven predictive analytics.

EXECUTIVE PERSPECTIVES

STRATEGY

Cyber risk is a more important strategic concern than ever. With the amount of data organizations collect and the breadth of their partnerships and workforce, protection is growing more complicated. Cyber AI is now a leading practice for guarding against the volume and sophistication of recent cyberattacks. CEOs should be asking questions of their CRO, CISO, CIO, and others to understand the current security posture, and whether it needs to be upgraded. By positioning AI as a security and strategy priority, leaders can help their organizations align on the importance of strengthening defenses and managing risk.

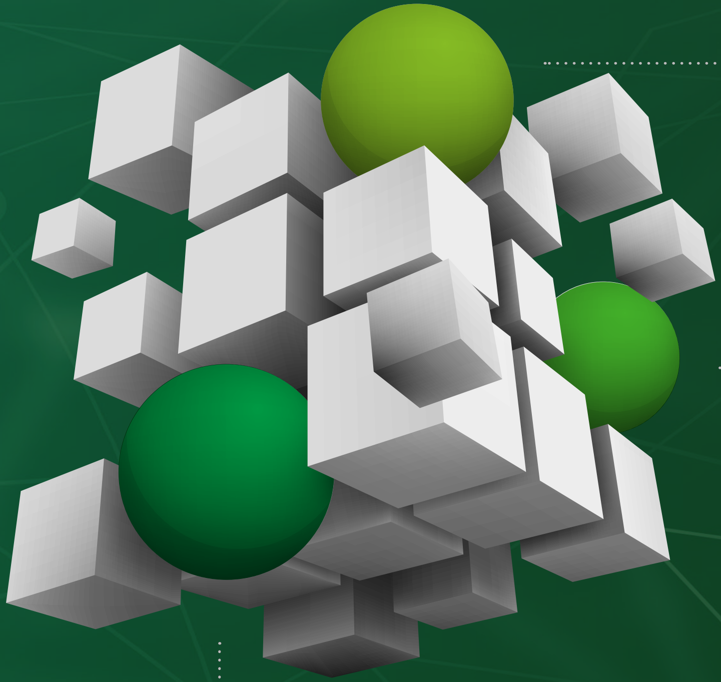
FINANCE

As the prevalence and financial impact of cyberattacks increase, CFOs are taking an expanded role in overseeing risk management. They should use their unique role in C-suite leadership to advocate for a fully funded enterprisewide adoption of AI-enhanced cyber defense. They can work with their cybersecurity teams to understand the investment required, timeline, risks, and benefits of cyber AI, and then present that information to the board as a key priority.

RISK

Bad actors have been leveraging AI for years to conduct cyberattacks. CROs should prepare their organizations for the new normal of fighting those attacks with AI defense and intelligent security operations. Organizations should find internal support to build these new capabilities or evaluate outsourcing cyber protection to augment their security teams. Of course, AI defenses have their own vulnerabilities, and the threat landscape will continue to evolve. Acting now to begin improving defenses gradually—rather than reacting when it's too late—can help organizations protect customers and their data.

ARE YOU READY?



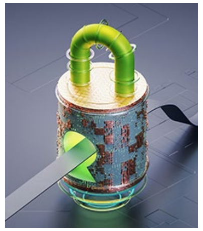
KEY QUESTIONS

1 How has your enterprise attack surface expanded due to an increase in remote workers, network-connected devices, and third-party risk, and what steps are you taking to protect it?

2 How are you currently using AI tools to detect, contain, and respond to cyberthreats? In which areas can the use of AI be expanded to create a more proactive security posture?

3 Do you have the skill sets and organizational structure needed to meet your cybersecurity objectives today? In two years? How do you plan to acquire these skills?

LEARN MORE



Zero trust: Never trust, always verify

See how a zero-trust cybersecurity posture provides the opportunity to create a more robust and resilient security.

2021 Future of cyber survey

Gain insight from nearly 600 global C-level executives who have visibility into the cybersecurity functions of their organizations.

State of AI in the enterprise, 4th edition

Discover what today's AI-fueled organizations are doing differently to drive success.

AUTHORS

Our insights can help you take advantage of emerging trends. If you're looking for fresh ideas to address your challenges, let's talk.

Curt Aubley

Cyber & Strategic Risk groups managing director

Deloitte & Touche LLP

caubley@deloitte.com

Ed Bowen

Advisory AI CoE leader

Deloitte & Touche LLP

edbowen@deloitte.com

Wendy Frank

Cyber 5G leader

Deloitte & Touche LLP

wfrank@deloitte.com

Deb Golden

US Cyber & Strategic Risk leader

Deloitte & Touche LLP

debgolden@deloitte.com

Mike Morris

Cyber & Strategic Risk managing director

Deloitte & Touche LLP

micmorris@deloitte.com

Kieran Norton

Cyber & Strategic Risk infrastructure security solution leader

Deloitte & Touche LLP

kinorton@deloitte.com

SENIOR CONTRIBUTORS

Wil Rockall
Partner,
Deloitte LLP

Jan Vanhaecht
Partner,
Deloitte Belgium CVBA

Sam Holmes
Senior manager,
Deloitte LLP

Ryan Lindeman
Senior manager,
Deloitte & Touche LLP

PaPa Yin Minn
Specialist master,
Deloitte Tohmatsu Cyber LLC

ENDNOTES

1. Steve Morgan, “Cybercrime to cost the world $10.5 trillion annually by 2025,” Cybersecurity Ventures, November 13, 2020.

2. IBM, *Cost of a data breach report 2021*, accessed November 17, 2021.

3. Ibid.

4. *CNBC*, “Cybercrime could cost $10.5 trillion dollars by 2025, according to Cybersecurity Ventures,” March 9, 2021.

5. *PR Newswire*, “Artificial intelligence-based cybersecurity market grows by $19 billion during 2021-2025,” June 21, 2021.

6. NCCI, “Remote work before, during, and after the pandemic: Quarterly economics briefing—Q4 2020,” January 25, 2021.

7. Jasper Jolly, “Huge rise in hacking attacks on home workers during lockdown,” *Guardian*, May 24, 2020.

8. Fleming Shi, “Surge in security concerns due to remote working during COVID-19 crisis,” Barracuda, May 6, 2020.

9. Cisco, *Cisco annual internet report (2018–2023) white paper*, accessed November 17, 2021.

10. Gartner, “API security: What you need to do to protect your APIs,” accessed November 17, 2021.

11. David Flower, “5G and the new age of fraud,” *Forbes*, December 30, 2020.

12. GSMA, *The mobile economy*, accessed November 17, 2021.

13. Steve Rogerson, “Cellular IoT connections grew 12% in 2020, says Berg,” IoT M2M Council, August 4, 2021.

14. (ISC)^2, “(ISC)^2 study reveals the cybersecurity workforce has grown to 3.5 million professionals globally,” accessed November 17, 2021.

15. Wendy Frank (Cyber 5G leader at Deloitte & Touche LLP), interview, October 1, 2021.

16. Palo Alto Networks, *The state of incident response 2017*, accessed November 17, 2021.

17. Critical Start, *The impact of security alert overload*, accessed November 17, 2021.

18. Matthew Hutson, “Artificial intelligence just made guessing your password a whole lot easier,” *Science*, September 15, 2017.

19. Lily Hay Newman, “AI wrote better phishing emails than humans in a recent test,” *Wired*, July 2021.

20. William Dixon and Nicole Eagan, “3 ways AI will change the nature of cyber attacks,” World Economic Forum, June 19, 2019.

21. Ibid.

22. Matthew Hutson, “Artificial intelligence just made guessing your password a whole lot easier.”

23. Tony Pepper, “Why contextual machine learning is the fix that zero-trust email security needs,” Help Net Security, February 16, 2021.

24. Al Dillon (cofounder and CEO, Sapper Labs Cyber Solutions), phone interview with authors, October 19, 2021.

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

www.deloitte.com/us/TechTrends

Follow @DeloitteOnTech

Deloitte Insights contributors

Editorial: Aditi Rao, Blythe Hurley, Andy Bayiates, Aparna Prusty, Dilip Kumar Poddar, Emma Downey, Nairita Gangopadhyay, and Rupesh Bhat

Creative: Alexis Werbeck, Adrian Espinoza, Heather Mara, and Jaime Austin

Promotion: Hannah Rapp

Cover artwork: Bose Collins

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.