Security Predictions 2024

From ransomware to resilience, and how AI will impact a changing threat landscape.

splunk>

To the boardroom and beyond.

As security takes center stage with the C-suite and the board, companies are finally acknowledging that cyber risk is business risk. Whether leaders are justifying the ROI of security initiatives, bracing for stealthier and more insidious ransomware, or helping their teams build new cyber defenses with generative AI, in 2024, security will be a priority from the top down.

“You’ll see organizations introduce more cyber skills on their boards and give their CISOs larger roles as business leaders,” says Splunk President and CEO Gary Steele. “Even though cyber obviously has been a topic in the boardroom for a long time, it’ll be much more prevalent.”

And with good reason. In July of 2023, the Securities and Exchange Commission (SEC) in the United States imposed new rules requiring registered organizations to disclose any cybersecurity incident they determine to be material within four business days of discovery, as well as all material information on their cybersecurity risk, strategy and governance. Cyber risk is now inextricably linked to an organization’s brand, value and market perception. And boards are watching.

Included in that increased scrutiny are new technologies like generative AI, which will emerge as both a tool and a threat for security professionals and cyber criminals alike. Threat scenarios include AI-designed evasive malware, deepfakes, more authentic social engineering and a slew of data privacy nightmares in large language models (LLMs). But experts are also excited about the potential of using AI to build cyber defenses and address talent shortfalls so they can apply more resources to the most critical tasks. Whether the benefits will outweigh the costs remains to be seen.

To navigate this sea of cyber legislation, disruptive technologies and security threats, teams must realize they’re on the same mission. As organizations ramp up adoption of AI, edge and multicloud infrastructure, they will need broader and deeper visibility into expanding environments. This panoramic view is only possible when all relevant teams and stakeholders are aligned. That’s why organizations should ingrain security into all processes, functions and phases of development.

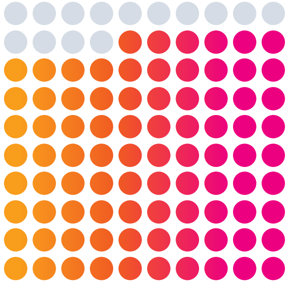
In 2024, collaboration will be essential as resilience becomes non-negotiable. With communication, trust and a commitment to shared strengths, organizations can remain resilient through adversity next year and beyond.

With that, our 2024 Security Predictions begin.

Contents

Prediction: AI, Part I

AI will take on security tasks (and you'll be better off, trust us).



86%

of CISOs believe generative AI will alleviate skills gaps and talent shortages

If we can bet on anything, it's that AI won't be going away anytime soon. Far from it. It will continue to shape the face of cybersecurity well into 2024, and into the foreseeable future.

Will generative AI take security jobs? The short answer is yes, some of them. But that's not a bad thing. Our recent CISO Report revealed that 86% of CISOs believe generative AI will alleviate skills gaps and talent shortages.

There simply aren't enough skilled cybersecurity professionals to meet the mounting and increasingly rigorous demand. Security analysts are stretched thin performing routine and tedious tasks, often at the expense of ones that could elevate both the organization's security posture and culture.

That's where generative AI will come in.

Instead of replacing jobs per se, AI will be more like that assistant you can't function without, who gladly takes on tasks you find repetitive, mundane and labor-intensive. (Think policy creation, process documentation, data enrichment — you get the idea.)

"The idea that humans are going to keep up with the speed of cyber events is ludicrous. We can't keep up; it's impossible." says Paul Kurtz, Splunk chief cybersecurity advisor and field CTO. "There will be jobs in security that migrate or are heavily supplemented by AI tools. That said, IT and communications systems will continue to drive the need for more analysts and operators to support and defend evolving applications of AI."

AI won't just replace jobs, but create them, too. Ryan Kovar, distinguished security strategist and leader of Splunk's SURGe security research team, says functions such as prompt engineering will be one of the fastest-growing job requirements for entry-level security professionals.

"If you are in this space, you will need to learn AI as a tool," agrees Mick Baccio, global security advisor at Splunk's SURGe security research team. "The term 'prompt engineering' will be on par with coding."

AI might help your team avoid burnout, become more strategic and even expose new opportunities, but it will probably stop short of picking up lunch or your dry cleaning — at least for now. No tool is perfect.

Prediction: AI, Part II

AI will open a Pandora's box of escalating privacy and security woes.

> **“The dreams of today will be the cyber nightmares of tomorrow.**
>
> Ryan Kovar, Distinguished Security Strategist and Leader of SURGe

Did we mention that no tool is perfect? What has the power for good also has the power for more malicious aims. While security practitioners will reap the benefits of AI, it's equally likely that cybercriminals will explore ways to wield it as yet another weapon in their arsenals.

AI will no doubt expand organizations' attack surfaces as bad actors push its uses to new extremes. “I believe this year we will start seeing security incidents that are powered by AI,” says Mike Horn, SVP and GM of Splunk security. Some notable attack vectors include AI poisoning, in which attackers tamper with AI's training data to deliberately affect the outcome of the model's decision-making capabilities. “I do think that's going to become more prominent in the news. It's still very early days, but there's lots to learn about both protecting AI systems and defending against AI-powered attacks.”

In 2024, we'll likely see weaponized AI with more sophisticated deepfakes, more lifelike impersonations, better crafted social engineering attacks — perhaps with fewer obvious language gaffes — and more evasive malware.

“The dreams of today will be the cyber nightmares of tomorrow,” says Ryan Kovar, distinguished security strategist and leader of SURGe.

Recent research also supports growing concerns about how AI will be used in the cyber underworld. Respondents to our recent CISO Report survey anticipated that the most common malicious use cases would be faster and more efficient attacks (36%), voice and image impersonations for social engineering (36%) and extending the attack surface of the supply chain (31%).

If there's a silver lining, it's that our experts “don't see it actually providing anything novel” when it comes to attack methods, affirms CISO Jason Lee. “I see it making an easier, lower barrier to entry for script kiddies. But cybercriminals are actually using the same threat model.”

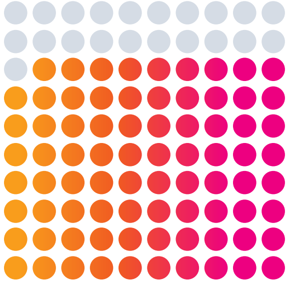
At the very least, generative AI has the potential to create more data privacy issues in 2024. For example, those LLMs such as OpenAI's ChatGPT, Google's PaLM (used in Bard) and Meta's LLaMa could inadvertently leak sensitive data when generating responses. This may include intellectual property, personal or medical information about individuals, or classified documents it was exposed to. "If an outside vendor was working on the most important information in our code base, I'm not sure I'd want that to go into an LLM," Lee says. "What if a classified document goes in there?"

But not to fear — there's also a good chance that governments will introduce stronger privacy regulation to address AI, especially in the wake of an AI-related breach. Global Security Advisor Mick Baccio says that some of the first privacy regulations governing AI security will probably originate from the EU, which has set global standards with regulations such as the General Data Protection Regulation (GDPR). However, if history is any indication, regulation will be late, reactive and probably won't effectively address the threat — at least not right away. "Governments will try — and fail — to regulate AI," Kovar says.

"The challenge that companies have regarding the ethical use of AI is that we need to maintain the right balance between innovation and safety," says Mike Horn, SVP and GM of security. "Unfortunately the bad guys aren't playing by the same rules and won't follow emerging regulatory rules regarding AI."

Prediction: CISOs and the Board

CISOs will have more at stake.



79%

of line-of-business stakeholders see the security team as either a trusted source of information or a key enabler of the organization's mission.

CISOs these days aren't just advising the C-suite, they are the C-suite. Until a few years ago, CISOs filled more of a tactical role. However, in 2024, CISOs will increasingly be heralded as cyber champions and business leaders, sit shoulder to shoulder with members of the board, and be even more instrumental in their organizations' cybersecurity strategies.

"Security risk is business risk, and boards are realizing it," says Mick Baccio, global security advisor at SURGe. CISOs will benefit from their elevated status and hold more sway with their respective CEOs and boards, which will likely mean additional resources, funding and support for their goals and teams. These changes in priorities haven't gone unnoticed — respondents to Splunk's 2023 State of Security report tell us that 79% of line-of-business stakeholders see the security team as either a trusted source of information or a key enabler of the organization's mission.

In 2024, CISOs will also have more at stake as the regulatory environment becomes more stringent, more complex and harder to navigate. New SEC regulations, effective December 2023, mandate that public companies disclose a cybersecurity incident such as a breach within four business days after discovery. If possible, they must also include details such as nature, scope and timing. This legislation links cybersecurity to the value of information systems — in turn driving a need to enhance the board's technical understanding.

"Unfortunately, investors were left in the dark on many cyberattacks. Now with the new SEC regulation, publicly traded companies must inform investors of an event that could have a material impact," says Paul Kurtz, chief cybersecurity advisor and field CTO. "Every board of directors will need to have someone that can understand the potential material impact of a cyber event."

CISOs shouldn't necessarily bear the responsibility of judging material impact, but they must be part of the discussion, Kurtz adds. As critical liaisons to the board, CISOs will face intensified scrutiny on security investments, manage more financial and organizational risk, and become increasingly liable for cyber risk — which includes breaches, attacks and security failures. This also means they are duty-bound to disclose incidents shortly after discovery to avoid risk of legal and/or financial penalties.

"What it's going to force is more in-depth conversations around best practices," CISO Jason Lee says. "How do you translate security strategy and posture so that an investor can understand — good, bad or whatever — your security profile? CISOs need to learn how to speak in that business language."

The good news is that even if other parts of the organization are slashing budgets, most cybersecurity budgets are climbing in the year ahead. "We don't see budgets being cut for security," says Kirsty Paine, Splunk field CTO and strategic advisor for EMEA. "It's a pretty ringed fence. CISOs just have to justify what they're doing."

Prediction: Cyber threats

Power to the people: Threats will become more distributed and democratized.

The concept of cyberwarfare is nothing new, and it shows no signs of slowing down in 2024.

Cyberwarfare will morph as nation-state actors lean on AI to militarize cyber threats in pursuit of their political aims. “Disinformation will happen faster,” says Ryan Kovar, distinguished security strategist and leader of SURGe.

It won’t be just script kiddies and basement hackers taking advantage of new AI tools — although they also will certainly reap the benefits. In light of high-profile national elections and ongoing global conflict, more nation-states will use AI to their advantage and discover new ways to execute politically motivated attacks, hacktivism and sabotage.

“Unfortunately, disinformation has become a critical component of national conflict,” says Mike Horn, SVP and GM of security. “With a U.S. election year coming up, we’ll see more misinformation and targeted hacking on different organizations.”

Digital disinformation campaigns that accompany kinetic warfare are already starting to take hold. “We saw this happen in Russia and Ukraine already, where they were doing joint strikes with cyber and kinetic warfare — not against military targets, but against soft targets,” Kovar says. “What the conflict in Ukraine and Russia has shown is where we’re thinking cybersecurity will be going, as opposed to an attack in the traditional sense that would bring down a power plant.”

Less technologically sophisticated nations will have a lower barrier to entry to launch disinformation campaigns with AI, opening the floodgates for hackers of all types to enter the cyber underworld on a global scale. “The bar to being a cybercriminal will continue to get lower and lower,” says Mick Baccio, global security advisor at SURGe.

> “
>
> **...disinformation has become a critical component of national conflict.**
>
> Mike Horn, SVP and GM of Security, Splunk

We anticipate new types of assaults in 2024, including commercial and economic disinformation campaigns, with more targeted attacks against companies' brands and reputations.

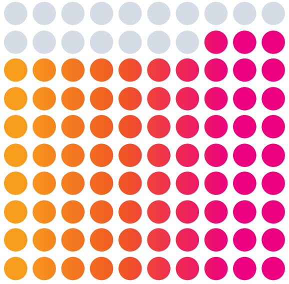
AI won't be the only tool opening the door to new forms of attacks, or within a wider range of industries — 5G will also present opportunities for cybercriminals by expanding the attack surface in ways that aren't yet protected. "I see new threats in 5G, given there's going to be more data at the edge. Data and software will become more intertwined, potentially complicating critical operational technology," says Paul Kurtz, chief cybersecurity advisor and field CTO.

Meanwhile, Kurtz says that 5G security is still a nascent conversation and "not well understood yet." Because 5G infrastructure is distributed and so closely aligned with telecom, organizations will encounter an ongoing dilemma to determine how to effectively secure it — or understand who is responsible for protecting it. "We need to think about edge-based computing and what that means for security and resiliency," Kurtz adds. "For example, how might adversaries disrupt edge processing, and what would be the impact on critical operations?"

In 2024, organizations should spell out responsibility for their edge infrastructure and distributed networks. "Who's responsible?" says Kurtz. "That's where I think it gets dicey and requires clarification."

Prediction: Ransomware

Ransomware actors will diversify their portfolios.



83%

of organizations that experienced a ransomware attack paid the ransom, either directly or via a third party.

It's time to take a look at one of the most significant and costly threats in the foreseeable future: ransomware.

For cybercriminals, new areas of expansion are well worth exploring. In recent years, ransomware has entailed a lucrative and low-risk payout. Findings in our recent CISO Report suggest that 83% of organizations that experienced a ransomware attack paid the ransom, either directly or via a third party. Of those that paid, more than half paid upwards of $100,000.

While ransomware might not become more destructive in 2024, cybercriminals will continue to diversify their techniques and targets in new and creative ways.

According to CISO Jason Lee, ransomware authors will increasingly rely on zero day threats — security vulnerabilities for which there is no known patch — to infiltrate networks. "These are one of the most valuable types of vulnerabilities," he says. "It's very expensive to burn a zero day."

Historically, it's been risky to use an untested zero day. Ransomware attackers have relied on tried-and-true vulnerabilities, banking on the fact they won't yet be patched and their attack will easily slip by defenses. But as teams continue to up the ante on ransomware security, attackers will find novel ways to get around tougher defenses. Those newly-minted zero day threats provide just the answer. "That really ups the watermark in terms of capabilities. That's unfortunately becoming the norm in 2024," Lee says. "It's the first time we're seeing that type of threat profile using a zero day become the norm. And it's terrifying for security professionals."

If there is a silver lining ahead, it's that law enforcement will likely continue cracking down on ransomware as it becomes more costly on a global scale. As a result, we'll likely see more prosecutions in international court.

Still, if you happen to fall victim, don't count on getting your data back any time soon.

Prediction: Resilience

Collaboration and integration will become critical for resilience.

The old adage "it takes a village" is especially relevant when it comes to security.

In light of increasingly stringent penalties for violating regulations like the California Consumer Privacy Act (CCPA) and the EU's General Data Protection Regulation (GDPR), security professionals around the globe need to break down silos and boost visibility to respond to threats faster than ever before. Much faster.

Until recently, security, IT and engineering went about their business independent of each other in fairly rigid operational silos. Going forward, it will be harder for these teams to do their jobs in separate bubbles. "Attack vectors like supply chain threats, including the recent MOVEit vulnerability, are forcing closer collaboration across teams," says Mike Horn, SVP and GM of security. "CISOs are working closer than ever with internal IT teams."

Looking ahead, security professionals will need an even more expansive view of data to help secure software development, AI and cloud environments — as well as accelerate root cause analysis and troubleshoot issues across the organization.

Resilience has been on the minds of security teams for a while. In Splunk's 2023 State of Security report, 62% of respondents (up from 54% the previous year) disclosed that cybersecurity incidents took down business-critical applications between once and twice a month (22 total per year on average, up from 19 the previous year.)

To avoid cyber-caused downtime, teamwork will be non-negotiable — and it will be a shift for teams accustomed to set swimlanes and responsibilities. While collaboration trends are starting to take root now, they will intensify throughout the year. "IT and security teams are getting closer, and it's naturally bringing teams together over time," says Kirsty Paine, field CTO and strategic advisor for EMEA. "Now, it's more of an informal collaboration."

That trajectory will continue into 2024. Our experts declare it's becoming more common for teams to take a security-first approach, which will cause them to integrate security more deeply into the development lifecycle. And as security, IT operations and development teams continue to learn cross-functionally and improve their skills, tool sharing will become a more widely adopted and established practice in 2024.

> "
>
> **Adapt, respond, harden, make things better — resilience is all of those things. Resiliency isn't a new concept for security, it's what we do.**
>
> Mike Horn, SVP and GM of Security, Splunk

20-year outlook: A more integrated security future.

While no one can peer into a crystal ball and foresee the next 20 years, it's a safe bet that cybersecurity will look dramatically different in 2043 than it does today. To celebrate Splunk's 20th anniversary, we asked our experts what that might look like.

Widespread AI adoption may redefine business as we know it as the technology takes over administrative functions and elevates our creativity and capacity to achieve new things. But the extensive use of AI could also drive a sizable privacy incident that forces organizations and governments to reexamine its use and reach.

Another trend that will continue over the next two decades is the evolution of CISOs into business leaders, particularly as organizations ingrain cybersecurity into all operations.

"Security leaders will look more like business development professionals than deep infosec practitioners in 20 years," says Patrick Coughlin, Splunk SVP of global technical sales. "Developing new alliances around different parts of the business will look more like relationship management and will require a growing mix of softer skills compared to our deeply technical roots. We will differentiate less on technical prowess and domain expertise, and more on skills to partner with different parts of the business."

And because CISOs will take on business strategist and development job functions, "BISOs (business information security officers) will not exist," adds Mick Baccio, global security advisor at SURGe.

As security begins to occupy a much larger place in business overall, separate functions will become more integrated. "There is a need for a synoptic view," says Paul Kurtz, chief cybersecurity advisor and field CTO. "Looking back to Y2K, having a synoptic view of networks has been critical. Today it is even more important, given our dependence on IT. Operators will need real time visibility, supplemented by AI, to understand what's happening on the network. Individual security 'mousetraps' will have little impact — unless you can fuse security and observability data in real time."

The nexus of geopolitics and cyber will manifest in nefarious ways. If current threat trends are any indication, cyber attacks will be an integral part of kinetic warfare over the next 20 years. "If you're attacking an American company, cyber is going to be seen as an act of war," CISO Jason Lee says.

Experts say that cyberattackers will also find new ways to execute acts of cyberwarfare, expanding ransomware efforts into critical and civic infrastructure that they can hold hostage. Political motivations, not economic, will be their driving force. The marriage of cyberwarfare and geopolitical interests will rapidly accelerate "as countries move to this greater connected ecosystem," says Ryan Kovar, distinguished security strategist and leader of SURGe. "Take things like drones. It is impossible to shoot down 100,000 drones, but it is absolutely possible to disrupt the autonomous algorithms that these things are using to coordinate their attack."

As security becomes a more crucial function of both industry and politics, cybersecurity legislation and data privacy regulations will be enforced on a global scale. Governments will have to enact more rigorous and punitive laws that will actually hold malware authors and cyber attackers accountable for their crimes.

"Industry can't be apolitical," says Kirsty Paine, field CTO and strategic advisor for EMEA. "Companies need to realize that whatever their politics and their ethics encompass, things like technical standards are really changing the way that the internet works. You have to think about how that's going to impact your future and the kind of society that you're going to live in. It's important to invest upstream because those changes are coming to you."

Contributors

Mick Baccio

Global Security Strategist Mick Baccio joined SURGe after cybersecurity and threat intelligence roles in an alphabet soup of federal agencies. He was the first-ever CISO of a U.S. presidential campaign. He likes threat hunting, Air Jordans and "cyber vegetables," in an unspecified order.

Patrick Coughlin

Patrick, Splunk's VP of GTM strategy and specialization, comes from a deep security background. He was co-founder and CEO of TruSTAR, a cyber intelligence management platform acquired by Splunk. Previously, he led cybersecurity and counterterrorism analyst teams for the U.S. government and private sector clients.

Mike Horn

Mike is the SVP and GM for Splunk's security business. Mike joined Splunk via the acquisition of TwinWave, where he was co-founder and CEO. Prior to that, Mike was responsible for multiple security products at Proofpoint, including Targeted Attack Protection, Threat Response and Emerging Threat Intelligence.

Ryan Kovar

Distinguished Security Strategist Ryan Kovar leads SURGe, Splunk's blue-team security research group. His background in security research and engineering roles include serving as senior principal security engineer for DARPA. Which he won't tell us anything about.

Paul Kurtz

As chief cybersecurity advisor and field CTO, Paul has led organizations involved in counter-terrorism, weapons nonproliferation, critical infrastructure protection and cybersecurity. Ranging from government to private sector, his roles included Special Assistant to the President on the National Security Council and cybersecurity company founder.

Jason Lee

As Splunk's chief information security officer, Jason is responsible for all facets of security engineering, assurance, policy, compliance, awareness and physical security across the organization. A technology industry leader with over 20 years of experience, most recently, Jason led security at Zoom.

Kirsty Paine

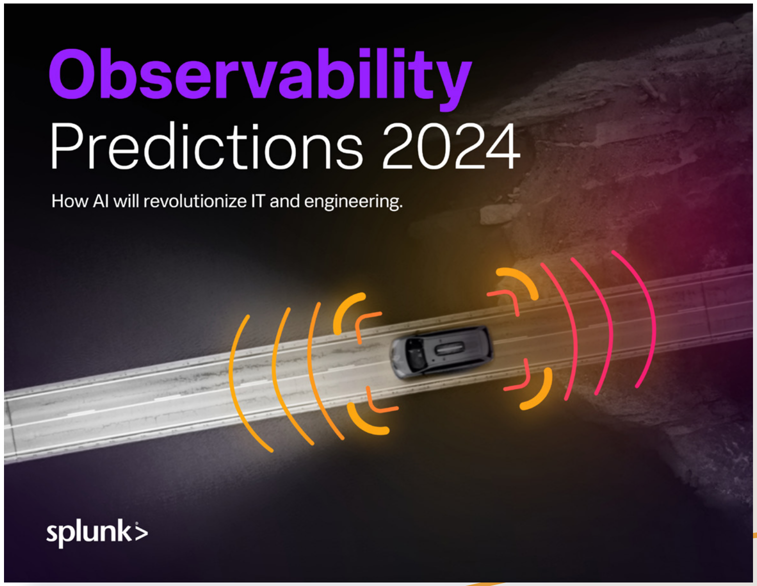
As field CTO and strategic advisor for EMEA, Kirsty provides technical thought leadership at Splunk and is a fellow at the World Economic Forum in the Cybersecurity Centre. Kirsty has spent a decade working in cybersecurity, engaging in security, privacy, cryptography, AI and internet technologies.

Gary Steele

Gary is the president and CEO of Splunk and a member of our board of directors. Prior to joining Splunk in 2022, Gary was the founding CEO of Proofpoint, where he led the company's growth from an early-stage start-up to a leading, publicly traded security-as-a-service provider.

For more 2024 predictions, read our observability and executive reports.

Read now



Observability Predictions 2024

How AI will revolutionize IT and engineering.

splunk>

Executive Predictions 2024

What business and technology leaders should know in the era of AI.

splunk>

splunk>

Keep the conversation going with Splunk