Data Security

Predictions 2023

Resilience, talent, privacy and how to stare down the threats of industrialized cybercrime

splunk>

Only the Resilient Survive

There's a shift in security conversations this year. At the business level, we're talking less about an organization being "secure," and more about it being resilient — against supply chain disruptions, pandemics and severe climate events, economic uncertainty, and yes, the seemingly infinite number of cybercriminals probing every aspect of what used to be called your perimeter.

The focus on resilience is changing the role of security leaders in their organizations. These discussions vary based on many factors, most notably the maturity level of the organization. Long-established legacy orgs have a harder time adopting a new approach, be it AI-driven automation, a zero trust framework or DevSecOps practices, while fresh-faced startups may have never done it any other way.

"The other day, a customer told me, 'DevSecOps is our holy grail, but we're stuck in dev-ops-sec, in that order, right now,'" says Simon Davies, senior vice president and general manager of Splunk in the Asia-Pacific region.

"And at the same time," says Dhiraj Goklani, Splunk's vice president of observability in APAC, "there are cloud-native organizations that were in the DevOps mode from the start, and they have almost no choice but to think of this level of integration."

We see those different realities across Europe and the Americas as well. But at organizations where performance and security monitoring are advancing with increasing collaboration, "resilience" is coming to the fore.

"Resilience is also a common theme on the observability side," says CEO Gary Steele, who joined Splunk in 2022 after nearly two decades as founding CEO of security provider Proofpoint. "We're seeing a focus on standardization, on driving resilience through a common set of tools and data."

That approach has a profound effect on how security teams do their jobs, and that is where we begin our 2023 predictions.

Predictions and Survival Strategies for 2023

Prediction

As ITOps and security tools and data converge, CISOs will take on more responsibility for broad cyber resilience.

Resilience is the new hotness. It's on the tip of everyone's tongue, including ours. But it's not always clear what everyone's talking about.

"There are pockets of functional resilience in any organization," says Mark Woods, Splunk's chief technical advisor in Europe and the Middle East. "Bringing that together from being functional to being fully business relevant is the problem for most organizations. But at the moment there is no definition as to what, actually, that means for anybody."

"I often see 'resilience' used as a synonym for cyber hygiene," says Ryan Kovar, Splunk distinguished security strategist. "Resiliency of overall IT infrastructure is important, and cyber resiliency is a more focused aspect of that."

"In Europe, we see financial services firms appointing very senior execs with resilience portfolios," Woods says. "Most often, they're thrown into the security organization, because in most organizations the only people who know how to do robust monitoring properly are security because it's their lifeblood. You can't do security without robust monitoring. Everything else, you can do without monitoring — you just do it badly."

Makes sense, because security teams will never have a shortage of resilience-affecting things to worry about.

"Ransomware is never going away, cybercrime will get worse, and sprawling hybrid environments are increasingly more complicated to secure. Organizational resilience comes into play," says Global Security Strategist Mick Baccio. "So your cyber resilience will impact your organizational resilience."

That holistic understanding of how certain aspects of resilience add up to a whole is necessary, since at the board or C-level, all risk is bad risk, whether it's customer-afflicting downtime caused by a server failure or lousy observability, or an attack that locks up your systems for ransom or steals sensitive data.

"We've been talking about resilience across the enterprise for decades," says Patrick Coughlin, Splunk's vice president of GTM strategy and specialization.

Coughlin, who co-founded threat intelligence startup TruStar, notes that in the past, you could ask 10 people what cyber resilience was and get 10 different answers.

"But, recently NIST has done great work to define cyber resilience, saying that we're now in an era where an incident is an incident whether you're talking about an infrastructure layer failure, a performance issue in an application, a service outage, an insider threat or an external threat actor." he says. "If the resilience of the business is at risk from adverse conditions or malicious compromises, you need to quickly find the problem, fix it, and then layer in automation so you don't have to do it again."

As organizations get better at taking advantage of all their data, rather than siloing it with one team or one tool, security teams are able to take a more holistic approach to risk. And it makes sense that when there's a network outage or other incident, the first step is to figure out whether it's an actual cyber attack or something your Ops team might call a glitch. That changes how teams work together.

"We're starting to see the organizational dynamics and definition of mission reflect the convergence at the data layer," says Coughlin, who has led cybersecurity teams in the public and private sectors. "Job titles and job descriptions are changing to match, and the influence of the CISO is expanding across the enterprise to cover this broader definition of incident, meaning that the CISO is now weighing in on new decisions throughout the organization."

He puts it in terms of the RACI matrix, where traditionally senior discussions of technology and business process across

business units positioned the CISOs as merely *informed* of what's being planned. "CISOs are moving left on the RACI now. They're certainly *consulted* on technology, data and process decisions across the business. Some we're seeing move all the way to the R and the A: They're becoming *responsible* and *accountable* for defining process and tech investments related to the cyber resilience mission."

It may seem as though the CISO is becoming a "chief resilience officer," but don't start printing new business cards. The CISO's title isn't going to change, Splunk CEO Gary Steele says. Just their tools, their relationships and their reach. "These days, CISOs are owning data more broadly and therefore end up with more responsibility over resilience and overall performance."

Prediction

Ransomware ain't going anywhere, but straight-up extortion is also "hot." And the smartest/biggest ransom bandits won't take crypto.

Ransomware is here to stay, because ransomware works. Sophisticated tools are exchanged in a sophisticated marketplace, and somewhere around half of victims quietly pay up. Research from Splunk's 2022 State of Security report found that, globally, 79% of organizations have experienced ransomware attacks; and 35% — or nearly half of the victim cohort — said an attack led them to lose access to data and systems. Among victims, only 33% restored from backup and refused to pay the attackers. The other 66% said that either the organization (in 39% of cases) or their insurance company (27%) paid the crooks. On average, respondents said that the largest ransom their organization paid was about US $347,000.

Ransomware is so successful, criminals are going to keep innovating. For one thing, locking systems is a very public action. Why make a federal case out of what could be a private transaction?

"Ransomware actors will move straight to extortion, skipping the encryption," Kovar says. "We've seen a few cases out there already. With classic ransomware, when you lock every user out of the network, the world knows you've been compromised. Imagine instead that the ransomware operator goes in and only exfiltrates sensitive IP or customer data. They don't even delete it; they just have it. Then they send three emails: to the board of directors, the CEO and the CISO and that's it. They prove what they've done and say, 'For $40 million, this problem goes away quietly.'"

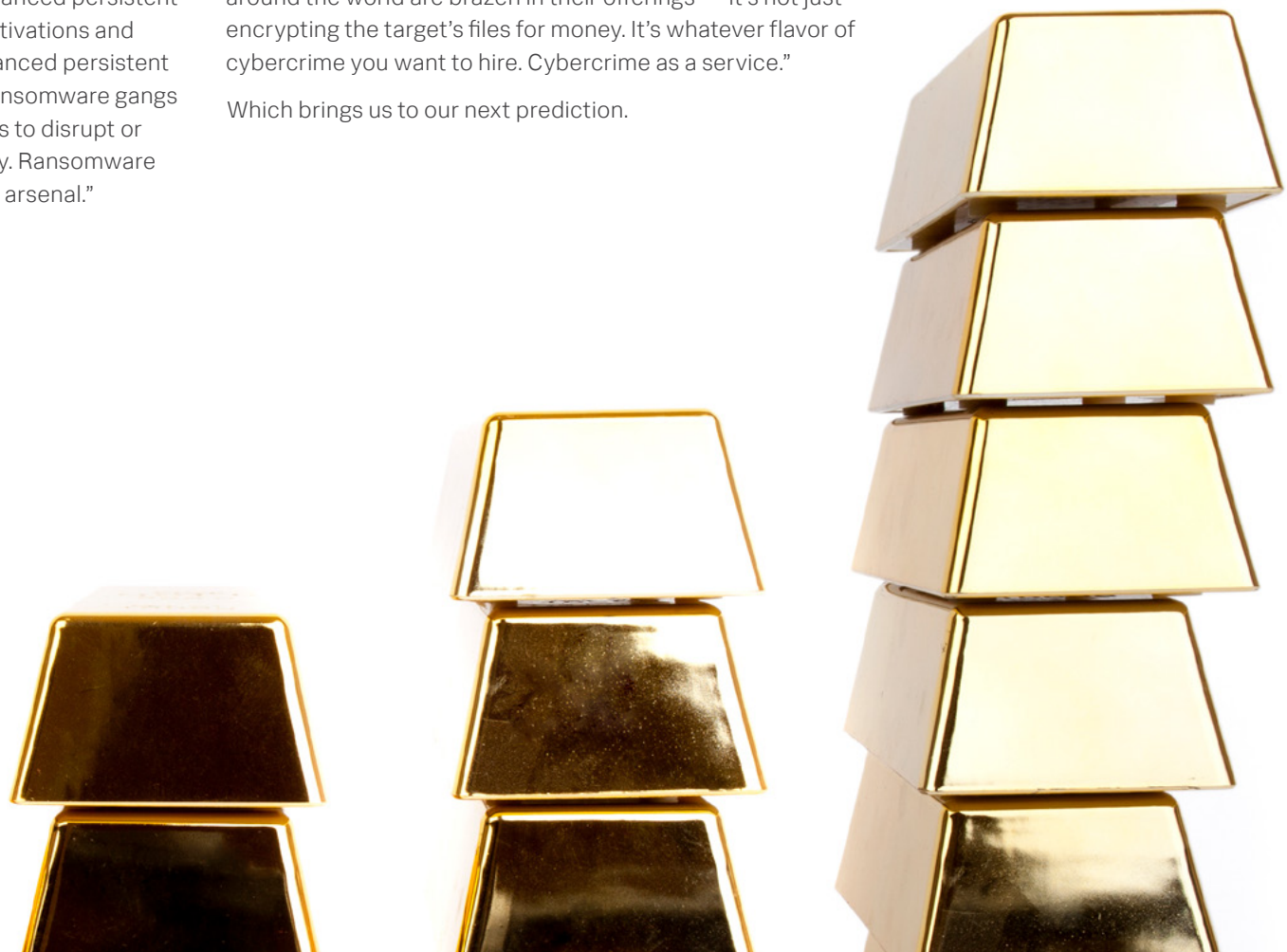
This is an evolution from 2021's big trend, "double extortion," in which the ransomware gang locks up your files, and delivers a twofold threat: 1) Pay or we won't unlock, and 2) Pay or we share your data with the world. Given that straight extortion would be less visible to the public, it's reasonable to assume that it's happening already. Because we already know that beyond the standard flavors of digital extortion, ransomware gangs are keenly interested in diversifying their portfolios.

"There's not a huge difference anymore in the techniques of a ransomware gang versus a nation-backed advanced persistent threat," Kovar says. The difference is in the motivations and objectives of straight-up criminals versus advanced persistent threat actors backed by nation-states. "The ransomware gangs want to make money, and the APT group wants to disrupt or steal IP from a foreign government or company. Ransomware binaries are just one of the tools in a criminal's arsenal."

And, he notes, it's usually the last tool. "A lot of our research shows that attackers are in the network for days, doing things using traditional tools like trojans, PowerShell, CobaltStrike, move, del, all the sort of tools normally used by any cyber criminal or APT actor, but, at the very end, ransomware operators downloaded a ransomware binary and locked everything up."

"And it's not just ransomware anymore," says Global Security Strategist Mick Baccio. "Hack-for-hire groups like we're seeing around the world are brazen in their offerings — it's not just encrypting the target's files for money. It's whatever flavor of cybercrime you want to hire. Cybercrime as a service."

Which brings us to our next prediction.



Prediction

The Cybercrime-as-a-Service economy will accelerate the volume and effectiveness of cyberattacks.

Last year, we predicted the increasing professionalization of ransomware gangs. Unfortunately, we were right.

"Oh, we got that right 100%," says Splunk Global Security Strategist Mick Baccio. "Ransomware moved from being a service to an economy. When you look at the technical end of ransomware, it's really kinda boring. But since it's so easy to spin up, and with the addition of other services, it's grown into a whole ecosystem. It's getting faster, it's getting more efficient. Ransomware operators are learning IT operations at the enterprise scale."

And the enterprise isn't just ransomware. It's any kind of malware, any kind of attack. Need some personal information on high value targets? A botnet for a DDoS attack? Ever wish someone else would install malware on a bunch of machines and just turn over the keys so you could handle the extorting? There's a dark web for all that, and the customer service just keeps getting better.

"These groups will sell you tools with outstanding ROI," says Robert Pizzari, Splunk's VP of security in the APAC region. "And if you have problems deploying the malware — maybe errors pop up because you're dealing with a different type of operating system — their service levels are outstanding, according to dark forums I've been researching."

"They have bug bounty programs," Baccio says. "And they often pay better than the ones a lot of legitimate companies have worked hard to establish."

The result is a sad watering down of the formerly elite ranks of computer hackers, as pretty much any morally deficient amateur can buy the tools to, say, lock a hospital out of its network or blackmail a Fortune 1000 company with lax security controls. It used to take skill to be that supervillain.

And because cybercrime is becoming the fast food of the dark web, a lot more malefactors are going to be able to target a lot more organizations.

"And as much as automation is improving security, it's also helping the bad guys," notes Lily Lee. As senior manager of security solutions strategy, she helps customers with the complexities of securing hybrid, multicloud environments. "Not only can a low-skilled adversary buy these tools, they can launch a bigger, broader attack with them."

It's another reason to have automation in your SOC, she adds. "It's the only way we can raise our game against the automation on their end."

Splunk Distinguished Security Strategist Ryan Kovar says that two things are true in the face of this explosion of corporatized cybercrime. First, the old defenses are still the best defenses. "A lot of techniques that used to be very distinct are converging and overlapping now," he says, "so if you're doing your job well, you're going to be defending against 85% of anything the bad guys would throw at you. You still need to defend against intrusion, against lateral movement, against execution and malicious code on your systems, and against exfiltration of information."

The second truth? "People in our line of work are always gonna have a job."

Prediction

Fewer ransoms will use cryptocurrency.

An Axios article looking at ransomware noted that the crypto market had lost $1 trillion in value between November 2021 and August 2022, and speculated about whether Bitcoin's dive would have an effect on ransomware. While the writer's sources assured her that ransomware will continue unabated, Mick Baccio and Ryan Kovar think that the higher end of data ransoms and extortions will indeed drop the digital dosh.

"Ransomware gangs are going to move away from cryptocurrency, less because of financial instability, though that's a factor, and more due to the traceability," Kovar says.

"Cryptocurrency's not as anonymous as people thought it was," Baccio says. "It's very traceable."

Everything happening on the blockchain is visible; it's all public. The wallet in which the criminals receive their crypto won't have their name on it, and they may try to hide their trail by shuffling the funds among 100 wallets and using a currency mixer like Tornado Cash, but it's still all eventually traceable. Once you try to cash out, the exchange is going to need a name, and that's where criminals have been caught.

"Yes, ultimately, crypto is not really anonymous," Kovar says, "but if you're a criminal who lives in a country that supports, sponsors or doesn't care about cybercrime, then you're probably not getting prosecuted easily unless you really tick people off."

The bigger criminals, he adds, won't want their billion in bitcoin. "They're going to say, 'We've stolen your data, but no one needs to know that, right? Just meet our dude in Switzerland, you'll go to the bank together and handle this in a dignified manner.'"

Prediction

The techniques of cyberwar will come to commercial cybercrime. Quickly. And critical infrastructure will be weaponized to disrupt political discourse.

Nation-state cyber teams are the R&D for cyber criminals at large. As we put this report together, the Russia-Ukraine was in its ninth month, and cyberattacks have included compromising financial centers and energy facilities as well as sowing disinformation — such as a deepfake video of Ukrainian President Volodymyr Zelenskyy ordering his countrymen to surrender. All of this is coming soon to a country much nearer to you, and not necessarily courtesy of a belligerent national government.

"We've seen in Ukraine the ability to disrupt energy and financial infrastructure at a national level," says Patrick Coughlin, vice president of GTM strategy and specialization, "and those techniques will be adopted by more commercially oriented threat actors against more distant and diversified targets for far more commercial purposes and outcomes."

The industriousness of a highly organized cybercrime industry all but guarantees these war techniques will soon be used in service of apolitical greed.

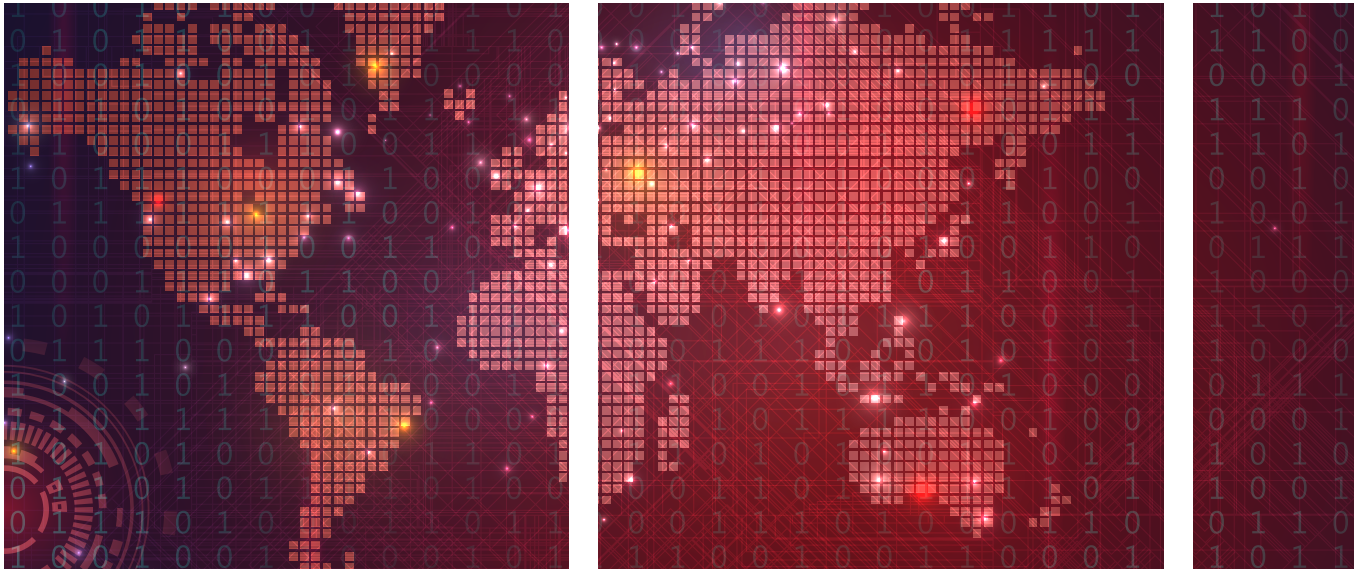
"Bad guys look for commercial uses too," Coughlin says. "These shifts are inevitable, just like legitimate companies figure

out how to go from military drones to commercial drone applications and services."

Ryan Kovar completely agrees, but goes a step further: Expect nation-state actors to up the ante, too.

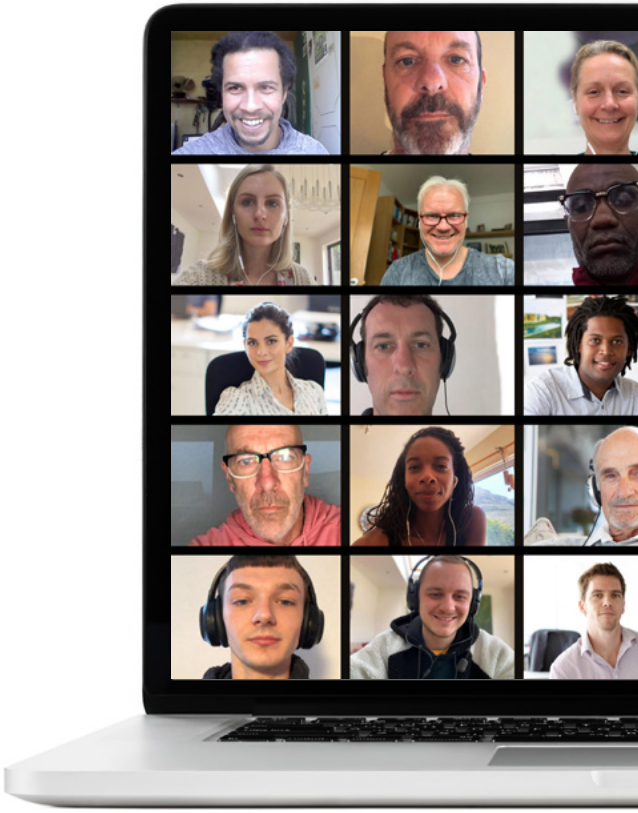
"Operation technology will be weaponized in the next year — and not just more compromises of critical infrastructure," says Kovar, who leads Splunk's strategic cybersecurity research team, SURGe. "Infrastructure will actually be used as a method of changing political discourse."

And, Kovar notes, the weaponized infrastructure doesn't have to be state-owned. Many utilities and other infrastructure are privately owned. "And these days, a lot of technology, including cloud services, are unofficial critical infrastructure."



Prediction

Enterprise misinformation attacks are going to ramp up into a really big problem.



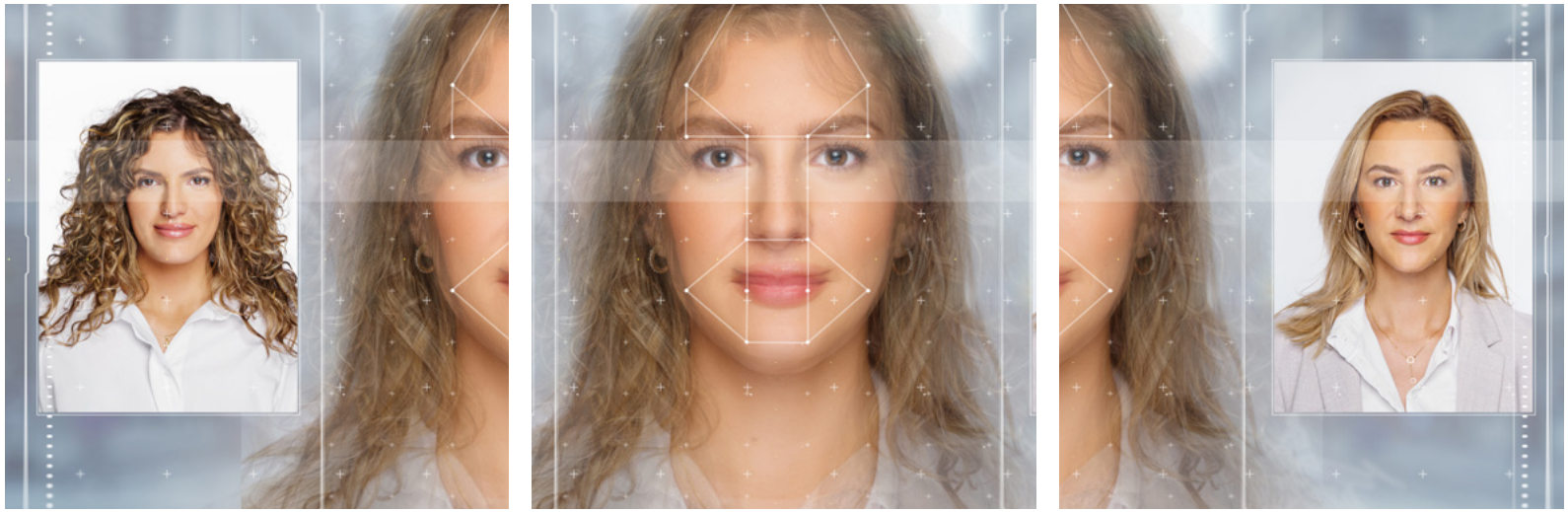
Just as we were starting to plan this year's predictions reports, one of our colleagues got a text from our CEO. It seems the big guy was sitting in a webinar (which is how CEOs generally spend their time) and needed her to run out and get some gift cards for him to lavish on a customer (which didn't sound at all like the bribery example from our annual compliance training). This was pretty easily dismissed as a lowbrow attack whose only point of sophistication was matching our colleague's phone number to her employer.

The very next day, two news articles came across our feeds: Scammers had created a sophisticated "AI hologram" of a senior exec at a crypto company to use in a meeting with the exec's clients, probably similar to the actor who used deepfake technology to impersonate Tom Cruise (while admitting that up front). Though the exec did not immediately provide proof of a video deepfake, he said that executives at four companies had claimed to have had meetings with him that he'd never attended.

We saw this coming in our 2020 security predictions, and it's here: enterprise misinformation with high-tech production values. Voice and video deepfakes will replace (or support) ham-fisted text messages and emails, and social media takeovers will undermine legitimate organizations. Such as the deepfake of Volodymyr Zelenskyy, which went out over Facebook, Telegram and other social channels.

"This is going to be the year that we have to address misinformation at the enterprise level," says Vice President of GTM Strategy and Specialization Patrick Coughlin. "We have to tackle new forms of digital risk in the sense of social media account takeovers for enterprises, deep fakes of CEOs, memestock market manipulation and other activities that would create consternation in the public and private markets. We have not even scratched the surface of the kinds of threats that we will see in the coming decade."

So buckle up, people. And tell your CEOs to buy their own gift cards.



Prediction

Supply chain attacks will continue, with underfunded and under resourced open source a key vulnerability. SBOMs will soon be a mandatory remediation tool.

Our supply chain prediction is not about whether they'll continue. SolarWinds, Log4Shell, Kaseya … the hits will keep on coming, and everyone knows it. A whopping 97% of respondents in our global State of Security 2022 report say they've increased their spending around the issue. Nope, our prediction is around what's going to be done about it: Organizations will drop the SBOM.

The idea of a software bill of materials is simple: a list of the components within a software package, including the obscure bit of open-source code scattered throughout a given commercial product. In the event that any component is the vector of a new attack, IT and security teams can quickly determine whether the compromised element is in any of the products they use or sell.

"It just makes sense," says Lily Lee, senior manager of security solutions strategy. "If you don't know what you have, how do you know what you're vulnerable to? It's as much a part of the job as knowing your users and assets."

SURGe threat guru Ryan Kovar wrote about SBOMs last summer on Forbes.com, and says that they're a smart idea

that will become an industry standard, very quickly. “By 2025, you’re not going to be able to sell software to the U.S. Federal Government without an SBOM,” he says. “And once it’s a government standard, the private sector will quickly adopt them as well.”

And 2025 can’t come too soon, Kovar adds. “Two Christmases in a row, we had major cyber incidents that were supply chain attacks. They’ll continue, and my guess would be that the next big one will be another fundamental open source product. The world runs on open source. It’s very good stuff, but it’s not all well supported. Certainly the companies that use open-source components are not all contributing to the development and upkeep of those products. So you have major software tools running in part on 15-year-old code maintained by a lone coder in Finland.”

Whatever the next supply chain vulnerability, anyone who doesn’t have a comprehensive list of the software components that make up their infrastructure and/or product line will surely wish that they did.

Prediction

The next big cyberheist vector is blockchain.

Blockchain hacks are already happening. Last summer, a massive hack of crypto token Solana captured headlines, reportedly costing thousands of users a total north of $4.5 million dollars. In the same month, a CNBC report put cryptocurrency theft in the first half of 2022 at $1.9 billion. But wait, blockchain is unhackable, right?

No perfect technology is unhackable when it's administered by inevitably imperfect humans. The Solana hack was attributed to embarrassingly negligent security controls, not some deeply buried software flaw. It was the digital equivalent of burglars getting in your house because they had the key to the front door. The Nomad attack reportedly exploited a flawed update to a smart contract that compromised a blockchain bridge, which enables transfers from one cryptocurrency chain to another.

"I think that some of the biggest financial impacts in terms of cyberspace breaches will be in the blockchain space," says Patrick Coughlin, vice president of GTM strategy and specialization and the co-founder and former CTO of threat-intelligence startup TruSTAR. "All these headline-grabbing hacks are just the start."

"The job of blockchain is to be decentralized and traceable," says Tom Martin, principal solutions engineer for blockchain and digital ledger technology at Splunk. "That doesn't mean it's immune from coding errors. In fact, when you look at these incidents, the transactions that took place were legitimate from the system's perspective, based on the parameters that had been programmed. The system worked exactly as intended and fortunately, for the aftermath, it kept a perfect record of everything that happened."

"Even with the crypto crash last year, so much money is moving through these blockchain networks — yet so much of it is still the Wild West,' Coughlin says. "These incidents force us to think about how blockchain is different in terms of resilience. How does blockchain fit into the definition of cyber resilience? How can we apply similar people/process/technology lessons we've learned over the last 20 years to defend these digital networks? That's an exciting challenge that will come with a lot of pain and pioneer tax as we learn from past mistakes and blaze new ground."

And a lot of financial reward for bad guys until the industry gets it right.

Prediction

Machine learning helps secure your systems. It will also become a new attack vector.

Automation is making security faster and more effective. Machine learning is making the automation smarter. But as ML permeates much of your environment, it also becomes another vector of attack.

"When ML pipelines are part of the software systems you're defending from attack, you have to be prepared for the ML model to be attacked, too," says Subho Majumdar, a senior applied scientist on Splunk's security expert analytics and learning (SEAL) team. "For example, attackers might try to exfiltrate the data from those ML models or misdirect their outputs with malicious inputs."

Majumdar recently co-wrote a book on trustworthy ML (Practicing Trustworthy Machine Learning, O'Reilly) and says that transparency is essential to making models both ethical and trustworthy. Machine learning models are often presented as black-box mystery machines whose workings are beyond human understanding. Transparency, the ability to understand what's going on and how the model produces its outputs, is essential.

"And ML security will be more and more important as we see models serving the public in more obvious or important ways," Majumdar adds.

So what do you do about it? First, you assess the level of risk. If the model goes wrong, is your streaming service going to make some hilariously bad movie recommendations, or is your bank going to get sued for unintended redlining? Will it slow backend efficiency for a few days or shut down your whole business?

Then you work with whoever built and trained the model, whether in house or off-the-shelf. Insist on that trust-enhancing transparency that Majumdar is so big on.

Then you keep a human eye on your models. "You have to validate your baselines," says Splunk security expert Lily Lee. "These ideas have always existed — baselining, data poisoning, system manipulation. The challenge today is partly that ML is powerful because it's often unsupervised, you don't have to babysit it, but that's where you are potentially vulnerable. You need to check in with your models and know what success should look like."

So you baseline, you test, you refine. Forever.

Prediction

Businesses are understanding the consumer urgency around privacy, and (some) companies will act ahead of government regulation. And sue someone.

Privacy is the technology industry's personal version of climate change: Most individuals are worried about it, lots of companies say they understand, but governments do somewhere between nothing and not nearly enough about it. In the next couple of years, government will continue to dither, but the private sector, pushed by individual consumers, will start to take action.

"Citizens will force corporations to take more privacy actions and become more cognizant of what data they have on the internet," says Global Security Strategist Mick Baccio. That goes for how your data is sold to compile invasive marketing profiles to better sell you more stuff or keep you clicking your social media feeds, and for what governments might do with your information.

The U.S. Supreme Court's Dobbs decision, which removed constitutional protection for abortion, galvanized concerns in the United States, as it was understood that data from menstrual-tracking apps and cell-phone location data could be sold to law enforcement (no subpoena necessary) to figure out who's been visiting what kind of health clinics, and why.

"A way to dismiss privacy concerns used to be, 'If you have nothing to hide, then why are you worried about it?'" notes Splunk Distinguished Security Strategist Ryan Kovar. "That doesn't hold up so well when courts are banning things that people have taken as solidly established law."

And it's not just recent, jarring developments like the Dobbs ruling or the creepy power (and deep flaws) of facial recognition software, Baccio adds. His anecdotal evidence comes from Signal, the popular encrypted messaging app.

"I've seen a ridiculous number of people pop up on Signal in the last year or so," Baccio says. "For five years, it was me, Ryan and a bunch of thrunters. People who have lived their entire lives online and never thought about privacy are thinking, 'Well, I want to make sure that what I'm saying isn't being recorded by Facebook,' which is a drastic mindset change from 10 years ago."

"I think it goes back to the bigger issue of when you put that data out on the internet, where does it go, and who has what rights to it?" Baccio says. "There's no U.S. equivalent to GDPR, no global privacy standard, and the legislation working through Congress right now might end up pretty watered down."

Which leaves private enterprise to switch from monetizing our every click to protecting whatever remains of our digital privacy.

"We're starting to see the primacy of privacy in the enterprise, with companies being more confident in setting data privacy policies with their partners and providers, and doing a better job of ensuring the privacy of their customers," says Patrick Coughlin, vice president of GTM strategy and specialization. "I don't think the supranational privacy regimes will be the answer we thought they would be. I was starting a company when GDPR took effect, and I remember how terrified companies and investors were of the potential for astronomical fines. We don't see the regulatory regimes as much of a driving force these days as the consumer sentiment around privacy"

If governments aren't going to be there to punish privacy violations, then, who's going to wield the stick when the carrot of happy consumers isn't enough? Coughlin says it'll be companies suing companies.

"In the next three to five years, there will be the equivalent of a class action lawsuit" he says. "Companies will band together to sue, for instance, a software vendor for breach of privacy clauses."

The widespread understanding, he says, is that technology is moving too fast, and often too carelessly, around privacy issues, and government is moving much too slow. It will fall to customer-driven companies to drive privacy compliance for the good of their customers and their own images.

Prediction

Two solutions to the talent crisis: Automation, and diversity of background via a focus on talent (not tech skills). Both are coming.

One solution to the talent crisis is automation to make up for the dearth of human talent. But we have automation already, and the talent crunch has continued. More automation is surely coming, and any tool that helps analysts work smarter and faster, or takes care of basic issues without even needing human intervention, will improve the situation. But we'll never fully automate our way out of the talent crisis.

"We're still going to need people," says Global Security Strategist Mick Baccio. "And we're going to have to stop looking for the usual kinds of people in the usual places."

Baccio says that the key is to bring in a more diverse range of talent. And that's diversity from a gender and ethnicity point of view, but also diversity in terms of background.

"Every year we beat ourselves up as an industry over having too many open positions," says Patrick Coughlin. "We're always pulling our hair out, but nothing changes. We need to ask ourselves whether we have a cyber security skills gap or we're selling our mission incorrectly. The mission itself is compelling: You can sit in a critical place in the security stack of every organization you touch throughout your professional life. A mission like that is a competitive advantage for acquiring talent."

"That's very true," says Petra Jenner, Splunk's SVP and general manager for Europe and the Middle East. "Younger workers

in particular want to join organizations with a clear purpose and vision, and it's really affecting the competition for talent in technology and security here."

"But in security," Coughlin says, "we exclude almost everyone because we portray ourselves as the high priests of complexity because we used to work in classified environments or some three letter agencies. That's ridiculous."

"And we get caught up trying to find people who know a specific technology, and that's where you really come up short," says Lily Lee, senior manager of security solutions strategy. "We say, 'I need someone who knows this special endpoint tool.' What about someone who understands the idea of endpoint security and can learn the tool? If you have foundational knowledge, you can be effective anywhere."

Ryan Kovar, who leads Splunk's SURGe team of security researchers, agrees. He hires for curiosity and problem-solving skills far more than coding experience or familiarity with specific tools or platforms.

"I can teach you how to use a SIEM," he says. "I cannot teach you to care, or to love solving a mystery. So I've found at least as much luck hiring people with a journalist or marketing background as I have had recruiting coders."

"If you're always after people who can think outside the box," Lee says, "sometimes you just have to go out of the box to find them."

"If we cast a wider net, it shouldn't be hard to attract great people," Coughlin says. "The security mission is compelling, and it's a competitive advantage for acquiring talent."

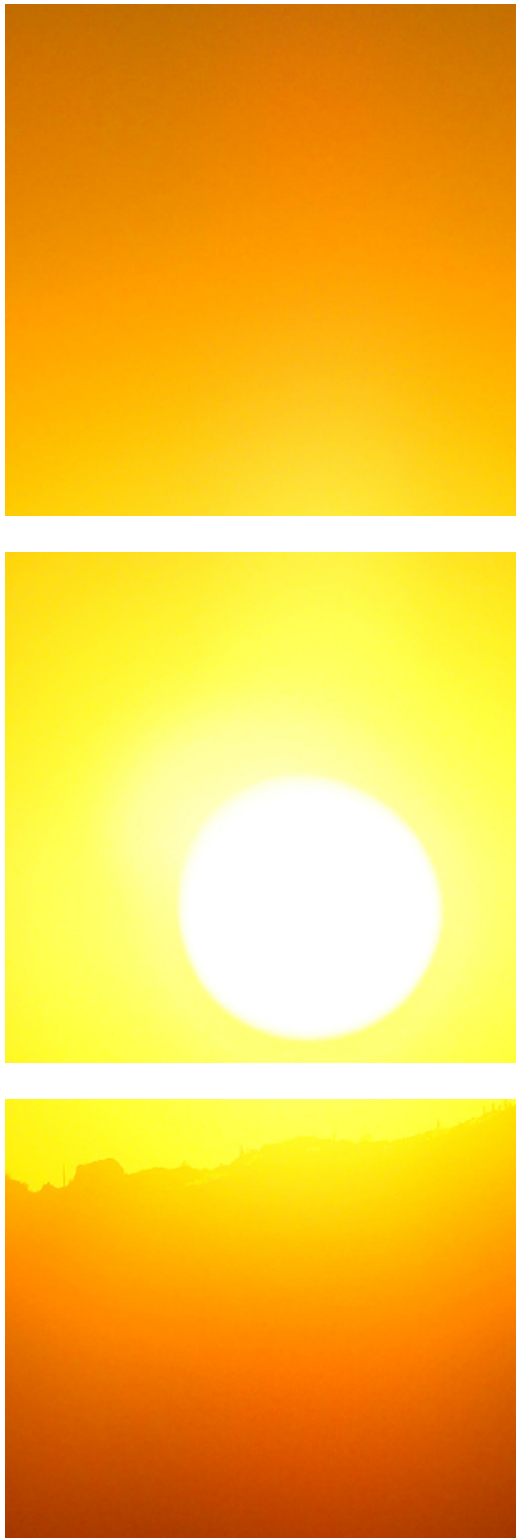
Robert Pizzari, vice president of security for APAC, says the same challenges and solutions are seen in the Asia Pacific region. "There's a shift toward looking at people who are curious by nature and have an innate desire to understand human behavior," he says."Bringing people in from various backgrounds is definitely a new idea that we're seeing organizations experiment with here."

And it works. Despite the eternal talent crunch, Kovar says that a recent recruitment effort for an early career position, with the aim of drawing a more diverse pool of candidates, was almost too successful. "HR had to shut us down early, because we practically crashed the system."

"I'm really optimistic about the new generation of cyber talent," Baccio says. "We're seeing really passionate people with a diversity of experiences and backgrounds that really makes me excited about the future of cyber security."

Welcome to the Golden Age

That was a lot, wasn't it? As Ryan Kovar said, one thing security professionals can count on is that they'll always be needed. And it remains true that basic security diligence, from prompt patching to training employees to not buy gift cards for webinar-obsessed CEOs, will stop most of the threats.



But at the same time, there's no panacea for the many ills of our digital ecosystem. CISA comes at us with "shields up," and you have to wonder what they think we're doing the rest of the time. "Shields up is not a plan for cyber defense," Mick Baccio says. "It's a plan for burnout."

It's very encouraging to see wider adoption of the zero trust framework, but organizations need to remember that the "zero" part is aspirational.

"A true zero trust model is, 'I'm ripping up the house and starting over,'" Baccio says. "And who can do that?"

"Google did that," Kovar notes. "If you don't have Google money, it's harder. Zero trust is the Six Sigma of network defense: If you have a good zero trust network, you are significantly better off than an org with no zero trust. But perfection in zero trust is impossible."

Despite that, optimism abounds. To a surprising degree. Kovar says that while the threats are ever-escalating, security tools, and the very discipline of cybersecurity, are far, far better than they were twenty, ten, even five years ago. Lily Lee agrees.

005 2010 2015 2020 2025

"The cyber world has a certain element of doom and gloom, because the industry is grounded in fear, but I'm very cautiously optimistic," Lee says. "Every cyber incident process ends with a lessons learned session. We learn from our mistakes, close up the gaps and improve."

Security is about the steady wins, she says. "The wins get overshadowed by big negative headlines, but the whole industry is where it is today because these wins have helped shape the current industry."

"We're seeing the technologies that matter in protecting cyber resilience start to converge, and the organizational structure and silos are coming together," Patrick Coughlin says. "Data has been converging for a decade. The beauty of this, I think, is that we're entering a golden age, a turnaround in how we think about cyber security talent and resources."

And that's the prediction we'll end with.

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.

Simon Davies
As senior vice president and general manager in APAC, Simon is responsible for the full portfolio of Splunk solutions in the Asia-Pacific and Japan markets. He is a veteran of Microsoft, Salesforce, Oracle and Citibank.

Dhiraj Goklani
Dhiraj is Splunk's vice president of observability in APAC, where he applies more than two decades of experience in the tech industry to helping grow the observability market in the region.

Petra Jenner
Petra is SVP and general manager in EMEA for Splunk. Previously, she held leadership roles at Salesforce, Microsoft, Checkpoint and Pivotal. She holds a Masters Degree in Business and IT, and studied International Management at the Stanford Graduate School of Business in Singapore.

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

Lily Lee
Lily is a senior manager of security solutions strategy at Splunk. She leads a global team of industry and product experts that support Splunk's security business and serve as thought leaders and trusted advisors for Splunk customers, partners and the security community.

Subho Majumdar
Subho is a senior applied ML researcher in Splunk's threat science group. Previously he was with AT&T Data Science and AI Research. A cofounder of multiple community efforts in ML, Subho recently co-authored Practicing Trustworthy Machine Learning.

Tom Martin
As a principal solution engineer on Splunk's blockchain team, Tom's an evangelist for new technologies and a liaison between customers and product management in the areas of Blockchain and Web3 technologies. Previously, he was at Silverstream, VMWare, Pivotal Software, Wily Technology and New Relic.

Robert Pizzari
Robert is Splunk's vice president of security in the APAC region. Previously, he held leadership roles at Check Point, FireEye, Trustwave and Cisco.

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.

Mark Woods
Splunk's chief technical advisor in EMEA, Mark has been an engineer, consultant, entrepreneur and CTO. He helps executive teams and international policymakers understand the seismic potential of data-driven approaches.

For more 2023 predictions, see the IT/observability, leadership trends/ emerging technologies and public sector reports.

Learn More

22-25648-Splunk-Data Sec Predictions 2023-EB-109