Data Security Predictions 2021

Zero Trust, vishing and strategic approaches to a chaotic, rapidly evolving world.

splunk>

Amazingly, the Job Got Harder

2020 was a year of unprecedented challenge for IT security teams.

Consider where they started: Technology is changing quickly, and an organization's attack surface is constantly morphing. They have tools for detecting anomalies — and detect so many that they're overwhelmed. And attack vectors constantly change as adversaries, driven by greed, political agendas or the lulz, come up with new tricks.

Now add coronavirus: Shut down your entire business. Or maybe just certain offices in certain regions in a sort of cascading business brownout. Have any number of workers logging in on personal devices. Have them overwhelm your existing digital collaboration tools, maybe adopting new, unvetted workarounds on the fly. Consider that the biggest security risk is a human who fails to spot, say, an email that is not normal (or legitimate). And consider that since early March, there's been no functional definition of normal.

Marinate in that until late 2021, at best.

As we've seen across the IT organization, the massive disruption of the COVID-19 pandemic has accelerated digital transformation across the board. That means new technologies, new processes, adopted at a faster rate than ever, among greater disorder and organizational stress. In addition, remote work has invalidated corporate network protections to a great extent. That, says Splunk CISO Yassir Abousselham, puts incredible pressure on security teams.

"We have to deliver the same level of security protection to employees and contingent workforce regardless of location: office, home, a coffee shop hotspot," he says.

It's a tall order, and Abousselham says that the challenge will drive CISOs to focus their attention on endpoint protection, and a specific security model: zero trust.

Security Predictions and Survival Strategies for 2021

05

Pandemic workforce disruption will drive a greater focus on endpoint security and the zero trust model.

07

Supply chain attacks mean that the bad guys won't just hack your organization. They'll hack your stuff.

09

Attackers will capitalize on COVID and remote work to tailor more effective phishing — and now vishing — emails and other scams.

12

Faster-moving digital transformation will include more artificial intelligence in the SOC.

14

Defense against adversarial learning will improve in the next few years. Because it has to.

15

You get two-factor authentication, and you get two-factor authentication and you ...

17

Capitalizing on pandemic disruption, attackers will find more openings in newly adopted technologies and through imperfect M&A.

19

Use the new remote work paradigm to ease your eternal shortage of security talent.

21

Once more with feeling: 2021 will continue to provide similar thrills and chills.

Prediction

Pandemic workforce disruption will drive a greater focus on endpoint security and the zero trust model.

The baseline for IT security has been network security: The SOC protects the data within the network by protecting the network perimeter. But the idea of a solid, defensible castle wall has fallen apart, especially when any employee can inadvertently open a door. Sooner or later (sooner), attackers get through your defenses.

Zero trust doesn't rely on network protection to keep data secure. Instead, if you secure endpoints and backend applications, the safety of your network becomes a secondary, rather than primary, line of defense. This is an idea that made sense in 2019, but in the COVID era's sudden spike in remote work, it's an even smarter approach.

"I think zero trust is going to stick," says Splunk Security Advisor Mick Baccio. "It's a longstanding concept that has finally been put to paper: constant validation. That doesn't go away. As the world changes and the workforce changes, visibility becomes an issue."

A zero trust strategy ties employee access to their IT-managed device, and governs the level and range of access each employee has, and which devices can access sensitive data.

That might mean that, from their authorized corporate laptop, employees can use all data and applications they'd have access to in the office, but their personal devices only access email and chat. The right endpoint policies make security independent of the network, and reduce the risk of data leaking onto unauthorized, undersecured devices.

A zero trust approach moves from implicitly trusting devices within a network to requiring verification from every device, user, application and session. Yet, it's a simpler approach than traditional network security regimes. In 2019, Gartner predicted that by 2023, 60% of enterprises would move from virtual private networks (VPNs) to zero trust initiatives. Splunk's CISO says that the coronavirus pandemic will only speed that shift.

"Endpoint security is critical in the COVID age," Abousselham says. "Some organizations had to convert office-based workers to a 100% remote workforce overnight. The abrupt shift resulted in a tremendous pressure on these organizations' VPN infrastructure. That became the single point of failure for the business, which drove organizations to accelerate cloud adoption to mitigate system availability risks. The change to how business systems are accessed creates security concerns that zero trust can help address."

> **"Endpoint security is critical in the COVID age."**
>
> Yassir Abousselham, CIO, Splunk

Prediction

Supply chain attacks mean that the bad guys won't just hack your organization. They'll hack your stuff.

"There was an article around June about Huawei patenting a new phone with a camera hidden under the display. Any new technologies that are being developed should raise security concerns," says Mick Baccio, a security veteran who worked in the White House and the Department of Health and Human Services. "There is a high likelihood that you'd see state actors try to take advantage of that technology in consumer products. Like with early IoT stuff, where weak security made sensors vulnerable to hacking and malware."

The danger, he says, is increased as knowledge workers continue to log in from home, using a MacGyver'd collection of personal and company-provided hardware and software.

"There's a webcam shortage right now. Everybody needs one for work, or for school. So you end up with a knockoff, something cheap. And that becomes a new or more prominent vector for attackers," Baccio says. "Supply chain vulnerability is very real. I don't attack you, I attack your supply chain. Maybe that's some webcam you ordered online, or a software platform you use."

The solution, Baccio says, is internal vigilance, and making your vendors do their diligence.

"Companies should try — and it's very hard — to get a clear understanding of their vendor supply chain," he says. "If I'm buying hardware, software, whatever, from a vendor or reseller, who is that reseller getting them from? What is the vendor's response if they are compromised? Doing research on the vendors before you sign those contracts is a huge thing."

“

Companies should try — and it’s very hard — to get a clear understanding of their vendor supply chain.”

Mick Baccio, Security Advisor, Splunk

There’s a lot of diligence required to make sure your supply chain isn’t compromised. And maybe your security and IT teams can do the work. Not only do your security and IT staff need to be vigilant, you also have to educate your employees as they stock their home offices. And if your workers are buying their own webcams for their own houses, you can’t exactly tell them what to buy.

“You can only advise people from a security awareness posture,” Baccio says. “Push awareness out to your employees.”

On the internal side, he says, endpoint detection is essential. “We’ve got a lot of remote people now, so we’re looking at more endpoints, and we’re looking specifically at more hardware drivers, home routers, just an increase in attack vectors,” Baccio says. “These peripherals are just something you have to incorporate into your zero trust model.”

Prediction

Attackers will capitalize on COVID and WFH to tailor more effective phishing — and now vishing — emails and other scams.

Any discussion of phishing and social engineering can feel like old hat: It's been a problem since dialup, and it'll still be a problem when we all have chips implanted in our brains. Last year, the growing-yet-underestimated danger of social engineering was one of the ills we flagged, and despite all the other earth-shaking headlines in 2020, social engineering did not disappoint.

Consider July's "blue check Twitter hack," in which the verified accounts of such varied luminaries as Elon Musk, Barack Obama and Kim Kardashian were used to scam $120,000 in bitcoin from credulous Twitter users. According to reports, the scheme was masterminded by a teenager using spear-phishing techniques. And back in January, an email tricked the bookkeeper of a judge on TV's "Shark Tank" out of nearly $400,000.

That's why we all have to keep harping about social engineering in general, and phishing in particular.

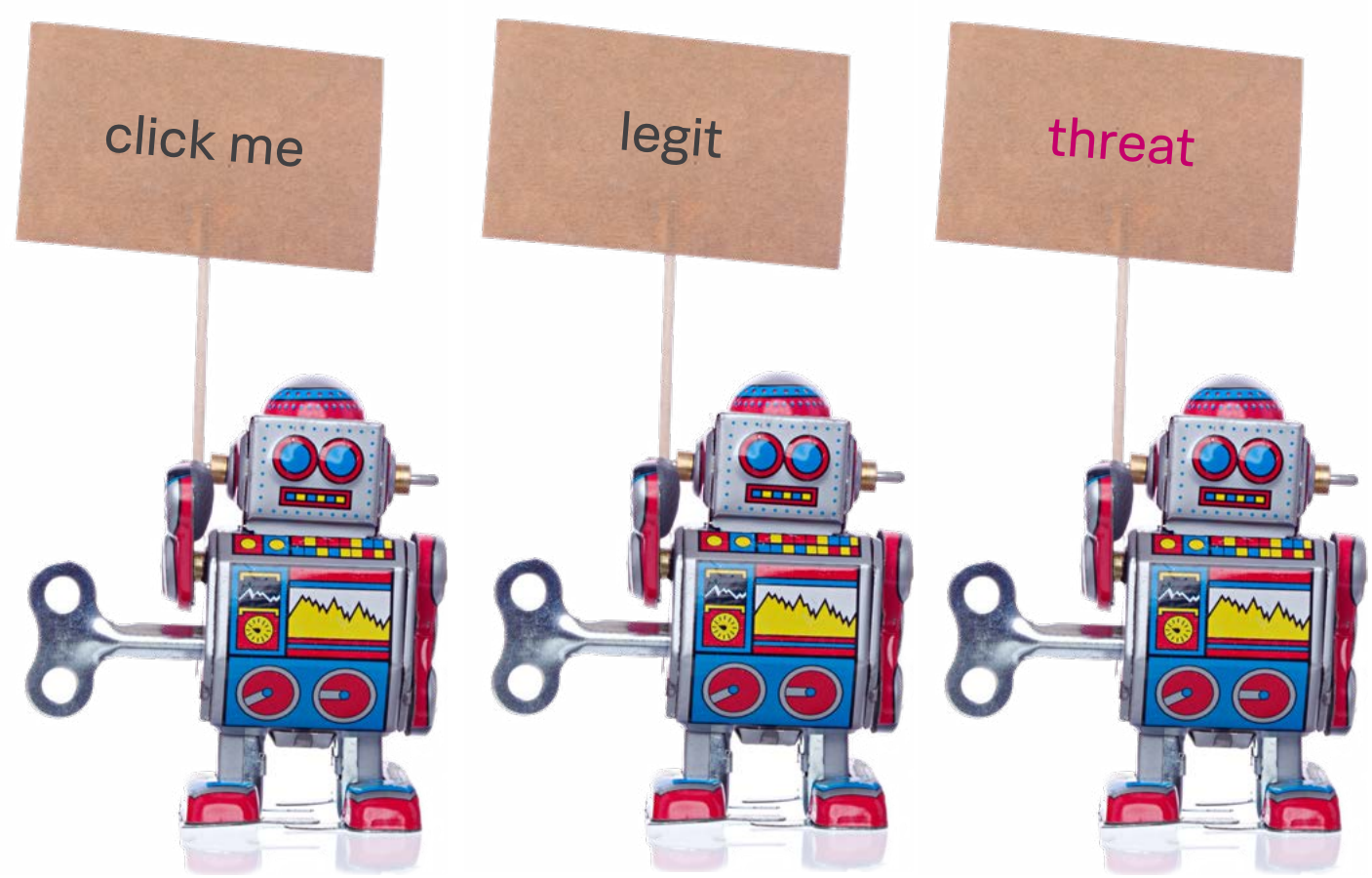
Social engineering attacks rely on tricking employees into doing something that seems legit, but is actually a deception. We train employees to pay attention, to spot fraudulent emails, but at a time when nothing feels normal and circumstances seem

to change every day, it's harder for employees to judge what's normal or illegitimate.

"The attackers' tactics will be the same, but the themes will be different," Abousselham says. "And defending in the remote work era is going to be different, because in the past we've relied heavily on security controls that reside both on the laptop or workstation and on the network. Now that employees are working remotely, laptops are the primary security device, aided by backend monitoring and anti-phishing solutions."

There is one new wrinkle, security advisor Mick Baccio notes. "We've recently begun hearing about 'vishing' becoming more of a thing," he says. With more employees working remotely, attackers are using voice calls to obtain VPN credentials from workers who would normally be in the office.

"Phishing email is still a problem and it's kind of mundane, routine work to counter," Baccio says. But it ain't going away. "I only see that getting worse and more specific."



Heightened alert: Shadow IT still stinks.

Friction generates shadow IT, and unauthorized IT solutions grease the wheels. And the chaos of 2020 has created a lot more friction.

"Because of remote work, shadow IT just becomes more of a problem, due to reduced visibility and unmanaged endpoints," says Splunk Security Advisor Mick Baccio.

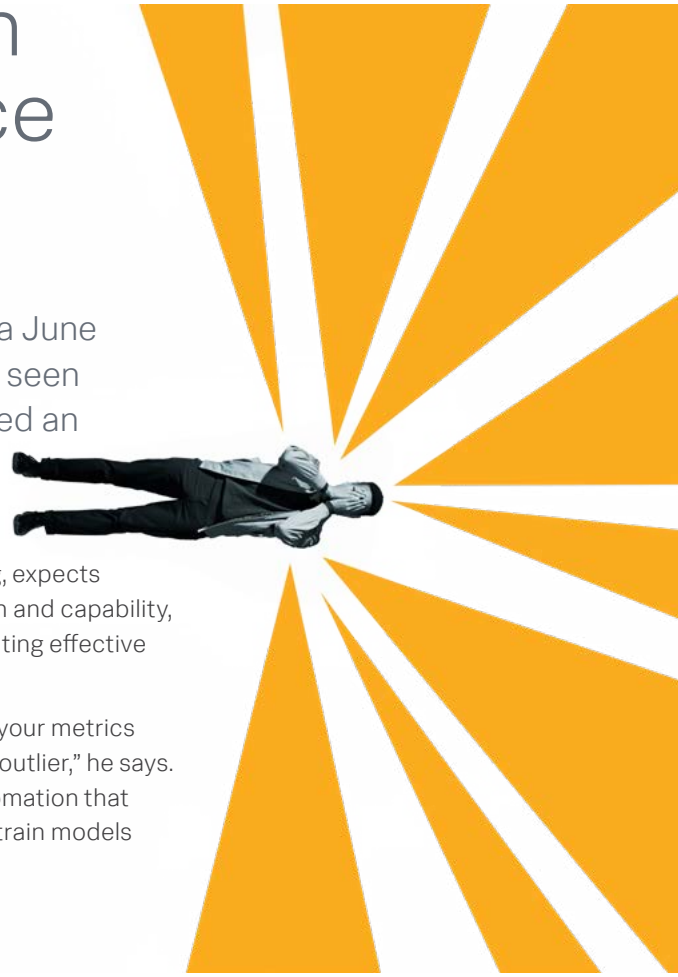
Increased use of personal devices to access organizational resources is a danger. When personal devices are compromised, they can become launchpads into the corporate network.

"It's a problem that we need to solve," Baccio says. "When offices reopen, not everyone will go back. We'll have a more remote workforce post-COVID, so greater visibility and control will be necessary to protect us from malware, phishing and other scams."

The response to shadow IT threats, says Splunk CISO Yassir Abousselham, should include a zero trust solution, endpoint detection and response capabilities, a backend anti-phishing solution, and employee awareness campaigns about phishing and other threats relevant to remote work. In parallel, the security team should raise awareness of the dangers to corporate data from compromised personal systems, such as home computers and personal phones.

Prediction

Faster-moving digital transformation will include more artificial intelligence in the SOC.



As if the pandemic itself, and the economic disruption, weren't enough to worry about, a June report from the Enterprise Strategy Group found that 47% of IT executives said they'd seen an increase in cyberattacks since the pandemic began. And 36% said they'd experienced an increased volume of security vulnerabilities due to remote work.

The sheer amount of security alerts, of potential threats, is too much for humans to handle alone. Already, automation and machine learning help human security analysts separate the most urgent alerts from a sea of data, and take instant remedial action against certain threat profiles. A July article in VentureBeat noted that Chase is using machine learning not only to target customers with more appealing marketing campaigns; the banking giant uses supervised and unsupervised machine learning algorithms to identify known and novel security threats.

Ram Sriharsha, Splunk's head of machine learning, expects AI/ML security tools to grow in their sophistication and capability, both in terms of flagging anomalies and in automating effective countermeasures.

"We're moving beyond algorithms that just look at your metrics and tell a human to do something about a certain outlier," he says. "As a matter of scale, we need algorithms and automation that take action. In the security domain, we won't just train models

on past bad actors and behavior to identify new, similar behavior. We'll see algorithms that just look at what's happening — look at traffic, look at data — to identify bad patterns and take evasive action."

Mick Baccio says that meaningful, practical application of AI is still a ways out. "I don't see that any time soon for most organizations," he says. "There are a million things we've got to do better before we even start looking at AI."

While he pegs transformatively powerful algorithms as two years out, at the least, he sees moving beyond automation to orchestration as an interim priority.

"We're automating a lot of repetitive tasks, but we need to move into orchestrating processes," he says. "So, with phishing emails, you'd automate the analysis and orchestrate that whole process start to finish: The email comes in, the analysis spits out a bunch of indicators. Those go to our firewall and whatever other systems and responses. Instead of automating some repetitive tasks, we'll orchestrate entire repetitive processes."

"We're automating a lot of repetitive tasks, but we need to move into orchestrating processes."

Mick Baccio, Security Advisor, Splunk

Prediction

Defense against adversarial learning will improve in the next few years. Because it has to.

Last year, our predictions report warned of the potential threat of AI sabotage: You can poison the outcomes of AI-driven automation by poisoning the data it learns from. We gave the example of tricking an autonomous vehicle into misunderstanding a stop sign. In September, researchers found that a tiny sticker on an object the size of a fighter jet could hide it from an AI processing drone footage. The threat of data deception remains on the horizon, and a new area of research will have to rise to the challenge, because today's AI is as naive as a week-old puppy.

Researchers found that a tiny sticker on an object the size of a fighter jet could hide it from an AI processing drone footage.

"Machine learning algorithms trust the data they learn from," Ram Sriharsha says. "But what happens if people are trying to hack you? As an industry, we haven't thought carefully about how to learn in the presence of adversaries."

He says that researchers will need to explore how to make their models robust against adversaries. And he says that now is the time to develop those techniques, because the potential power of such attacks will grow thanks to standard market forces.

"In time, there will not be hundreds of machine-learning startups selling hundreds of machine-learning platforms," Sriharsha says. "There will be a few, or one."

And just like the dominance of Microsoft's operating system gave hackers one big target, a small number of dominant AI platforms would draw all the attacks.

"Once that market consolidates around one platform that almost everybody is using, hackers are really incentivized to figure out how to break it," he says. "With that kind of adversarial attention, we have to spend a lot of energy right now to build robust algorithms that can withstand attack."

Prediction

You get two-factor authentication, and you get two-factor authentication and you ...

Once an option, or something your iPhone keeps pestering you to set up, organizations will make two-factor authentication a widespread norm, thanks to COVID-19. Noting that cybercrime is set to cost the global economy $2.9 million every minute in 2020, and some 80% of these attacks are password-related, a January paper from the World Economic Forum (WEF) calls passwordless authentication the next breakthrough in secure digital transformation. Two-factor and biometric authentication and hardware keys loom large in the WEF's perspective, along with AI/ML-driven behavioral analysis, zero-knowledge proofs and QR code authentication (the latter experiencing significant adoption in Asia-Pacific countries already).

Then came COVID-19, and the sudden wave of office workers logging in from home raised even more security concerns, because now there are more people logging in from outside your network who might not be who they say they are.

It's a challenge that should be keeping security experts and mobile software engineers awake at night, says Splunk's head of mobile engineering, Jesse Chor. "The surface area of security has expanded because of COVID and mobile, and that's definitely a concern."

Expect to see more adoption of two-factor authentication, whether by a phone app that asks, "Did you just try to log in?" or a biometric scan. Mick Baccio, a Splunk security advisor who has worked for the Dept. of Health and Human Services and the White House, and was CISO for the Pete Buttigieg presidential campaign, agrees that multifactor authentication is necessary, and he sees hardware tokens as the likeliest solution. Hardware tokens include little USB security keys, or can be incorporated into mobile phones.

"A hardware token pretty much shuts down the risk of account takeover," Baccio notes. "Who wouldn't want to shut that down? It's one of the biggest problems security teams face. Just shut it down and move more resources to your next biggest problem."

"The scary part now is that there are only two incumbent mobile operating systems," Chor adds. "If Apple or Google screw up their operating system, think about how devastating a vulnerability could be. A simple bug around my PIN, say, could let you get into my work network, hack my email, use my ecommerce accounts, hit my bank. You can basically be me."

And as for the form factor of the two-factor, Chor says he's a big fan of biometrics. "I think COVID is going to really accelerate the adoption of biometric identification for security and payments."

An important value of biometric logins, Chor says, is that they replace the physical device. If the mobile phone is the interface for the biometric identification, but does not store biometric data, it's useless to a thief.

"Just like we don't send passwords over the air anymore — we send hashes — the devices will send a hash of your biometric data," Chor says. "The device becomes a conduit for information that is confirmed in the cloud. A lost or stolen phone is no security threat, as long as you still have your thumb on hand. "I think security is going to head that way, where the phone is just a conduit."

Outlook: Consolidation heightens risk.

Security issues also color our emerging technology report, and one recurring theme is concern around vendor consolidation. When Microsoft won the market for operating systems, it became a dominant target for cybercriminals. Just as Jesse Chor notes (at left) that an exploitable flaw in either of the two dominant mobile operating systems could compromise countless organizations, Splunk Head of Machine Learning Ram Sriharsha says that an inevitably smaller number of AI/ML platforms will also provide prominent targets to hackers.

It's an inevitable problem that will have to stay on the radar of any security team.

> **"The scary part now is that there are only two incumbent mobile operating systems."**
>
> Jesse Chor, Head of Mobile Engineering, Splunk

Prediction

Capitalizing on pandemic disruption, attackers will find more openings in newly adopted technologies and through imperfect M&A.

Attackers slip through the cracks, and two sources of vulnerability are the adoption of new technologies and the absorption of new infrastructure through mergers and acquisitions. The acceleration of digital transformation increases one, and the volatility of the recession exacerbates the other.

"The gap between IT adopting a technology and the security org and its vendors being able to secure it at scale is an attacker's window of opportunity," CISO Yassir Abousselham says. "We saw developers deploying Kubernetes infrastructure, for example, while some security vendors were still factoring that into their solutions."

He notes that with the ease of cloud adoption, and the increasingly common practice of maintaining large numbers of disparate accounts on AWS, Azure and Google Cloud, there's plenty at risk.

Security organizations will have to keep a particular eye on new technologies, with a heightened propensity for shadow IT, as everyone faces new challenges during and coming out of the pandemic. (This is not to let old technologies off the hook. Older government systems running on COBOL, which today's computer science students might mistake for mythical, were severely taxed by the demands and disruptions of the pandemic, too.)

Another risk is through M&A, as companies quickly work to integrate their applications and infrastructure — again, at a time of added tumult across the board. "You might acquire a company that isn't using your preferred cloud platform, but you have to continue running on their infrastructure because conversion can be onerous," Abousselham says. "You need to establish trust between the acquired company and your internal systems, which results in added risk if you don't have a robust M&A integration program in place."

The result? Misconfigurations, or systems that are out of compliance or not fully secured. There's no one solution. It's a matter of staying on top of new technology as it enters the organization, and establishing best practices for ensuring the right levels of protection as needed.

Cloud security is a new skill set.

Splunk Security Advisor Mick Baccio sees familiar risks for organizations that hurriedly accelerate, or begin, their move to the cloud due to pandemic chaos. "Remember when IoT was the new hotness and we started throwing all of these things on the internet, and then realized we should maybe throw some security at it too?" he says. "The public cloud providers do a fantastic job, with fantastic security protocols in place. But I worry about people just moving to them without knowing the specific threat models."

From an ITOps and IT security perspective, he says, cloud-related skill sets will be essential. He predicts that the cloud providers' robust tool sets will lead to a contraction in the market for cloud security tools, and that cloud providers will provide different tiers of security access. Do you just want the threats stopped, or do you need to see how the sausage wasn't made?

Strategy

Use the new remote work paradigm to ease your eternal shortage of security talent.

Management traditionally likes to keep its eye on employees. Most organizations have been hesitant to fully embrace work-from-home, though global organizations with regional offices and sales organizations have long had a leg up on various forms of telework. Not only have there been productivity concerns, but there are security issues and a Silicon Valley maxim that creativity and innovation come from a critical mass of talented people sitting in the same office, having quick conversations in the hallway or kitchen.

Organizations have seen productivity stay stable, if not rise, and leaders have adapted to a remote management style.

Yet as knowledge workers were forced to dial in (for months, across entire continents), organizations have seen productivity stay stable, if not rise. And leaders have adapted to a remote management style. Splunk's chief technology officer, Tim Tully, admits to having been a bit of a WFH skeptic, and says he has been fully won over since the pandemic forced remote work on the 6,000-plus Splunkers worldwide.

"I'm definitely more willing to take on remote employees," he says. "Two years ago, I would've said my teams should at least be in the same time zone. Now, if I can find the best talent to work on a key initiative, I don't care where they are. And that's a different model for us."

Splunk's chief people officer, Kristen Robinson, agrees that more organizations will be willing to look further for talent. "We've proven, across industries, that remote work works," she says. "And I definitely think that it will open up new opportunities in terms of recruiting the best talent, regardless of geography."

CISO Yassir Abousselham agrees. “Greater comfort with managing remote workers allows us to hire talented people worldwide when there is a skill shortage locally.”

And in IT security, the skills shortage is acute. A July report from labor market research firm Emsi found that the U.S. demand for cybersecurity analysts was double the supply. That report recommends reskilling existing employees, but greater comfort with remote employees, and better systems for managing and empowering remote analysts, will also help.

Cross-border employment creates regulatory hassles, Abousselham notes, around salary, taxation, benefits, etc. But that shouldn’t stop us. “Remote work is the new normal. We need to put the necessary processes and capabilities in place to capitalize on the opportunity,” he says.

A July report from labor market research firm Emsi found that the U.S. demand for cybersecurity analysts was double the supply.

Once More, With Feeling

It has been hard to feel secure, in any sense, in 2020, and 2021 will continue to provide similar thrills and chills. Security teams have to factor in massive potential disruptions. The pandemic shut down business on entire continents. Unprecedented wildfires disrupted Australia in the first half of 2020, and the entire western United States in the second half. Other climate-driven disruptions will interrupt business on a regular basis, and risk tearing holes in a CISO's security program.

In a time of constant disruption, two of the biggest security strategies also reflect the human strategies that leading organizations have adopted. Just as we need to care about every individual's welfare, beyond the collective working of the whole organization, security teams need to focus on endpoint security. And in a world where, "Are you okay? Do you have what you need to cope right now?" should start nearly every business meeting, a focus on communication with employees and partners to help them navigate new, perhaps unseen, security challenges is also necessary.

Just as 2020 was one for the record books, 2021 will present massive challenges. Security teams have been instrumental in getting their organizations this far into the COVID disruption. They'll help us make it to the other side.

Contributors

Yassir Abousselham
Yassir Abousselham is Splunk's chief information security officer. Previously, he was CISO at Okta and SoFi, and held leadership roles at Google and EY. He's active in the cybersecurity industry, from co-chairing the San Francisco Evanta CISO Summit to acting as an advisor to cybersecurity startups.

Kristen Robinson
As chief people officer, Kristen Robinson leads with her belief that people are the foundation of innovative, fast-growing companies. Before Splunk, she was chief human resources officer at Pandora, and SVP of HR at Yahoo.

Mick Baccio
Prior to joining Splunk as a security advisor, Mick was CISO of Pete Buttigieg's presidential campaign, and held cybersecurity and threat intelligence roles in the Obama White House and the Dept. of Health and Human Services. He's also a professional lockpicker.

Ram Sriharsha
Ram is the head of machine learning at Splunk, leading the application of state-of-the-art ML techniques, including the ML that powers Splunk. Previously, he led engineering and product development for genomics at Databricks and started the R&D center for Apache Spark in Amsterdam. He was a principal scientist at Yahoo Research, and he holds a PhD in theoretical physics from the University of Maryland.

Jesse Chor
Jesse is head of mobile engineering at Splunk. Before that, he was director of software development engineering at Yahoo, which had acquired Sparq, a mobile marketing startup he founded and led as CEO.

Tim Tully
Tim is our chief technology officer, responsible for Splunk's Products and Technology organization. Before that, he spent 14 years at Yahoo as chief data architect, VP of engineering and more. He's big on the intersection of data, design and mobile, and advises entrepreneurs, startups and universities.

Get the 2021 predictions Executive Report and our focused editions on Emerging Technology and IT Operations for more insights.

Learn More

20-15669-SPLK-Data Security Predictions 2021-110

splunk>