

Public Sector

Predictions 2023

Security, talent and supply chains:
Insights to achieve organizational
resilience and mission success




splunk>

It's a Jungle Out There

The political turmoil, economic uncertainty, intensifying cyberattacks and persisting global pandemic of the last few years have made an already tough job even tougher for IT and security professionals in the public sector. Cybersecurity threats are hitting especially hard, what with increasing ransomware attacks and prevailing supply chain risks. And the Great Resignation has severely affected government and nonprofit employers who still struggle to regain staff lost during the pandemic.

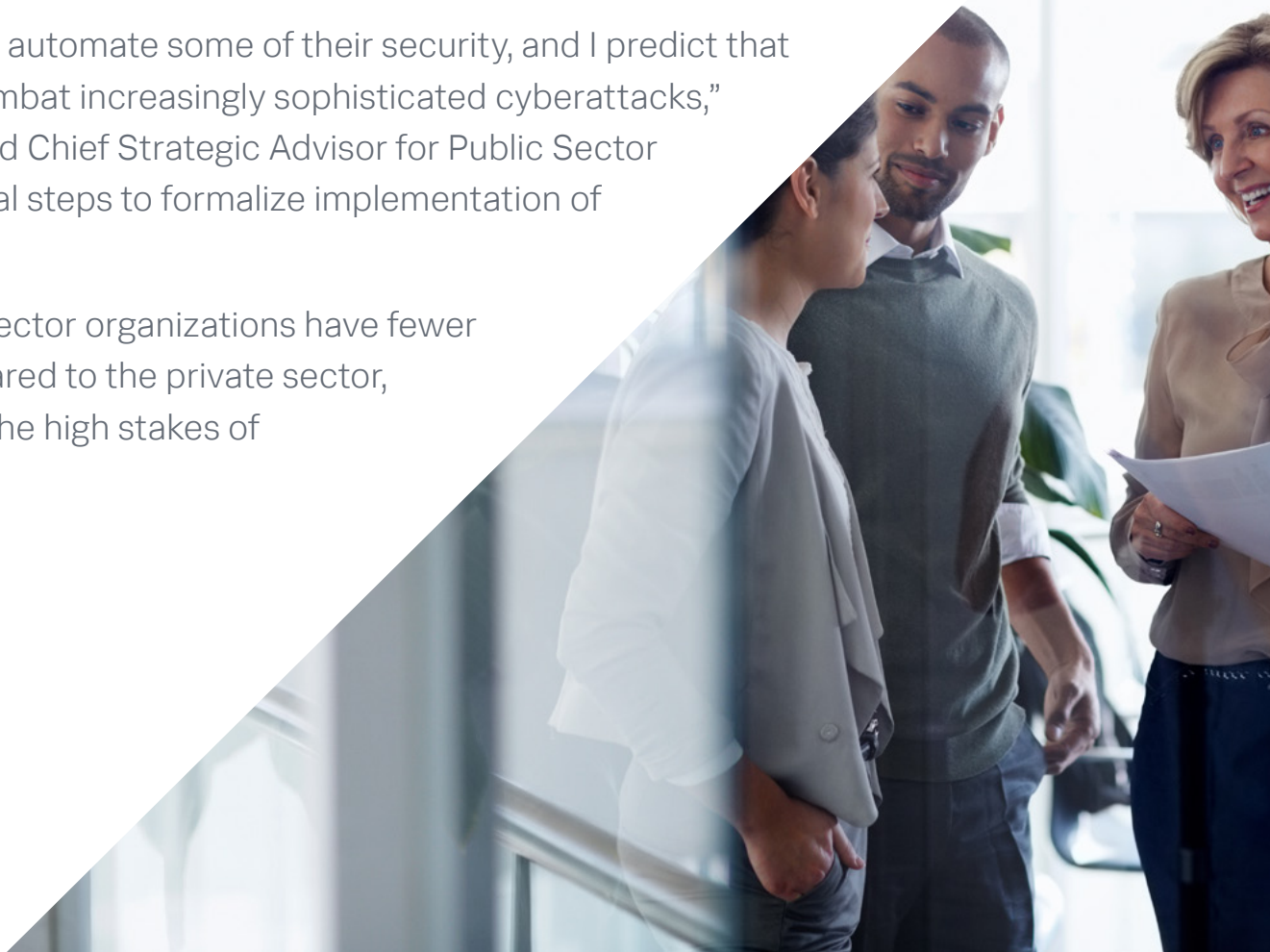




The good news is that some solutions are underway or forthcoming. President Biden's Executive Order 14028, Improving the Nation's Cybersecurity, was issued in May 2021, and the Technology Modernization Fund (TMF) continues to be an available resource. We're also seeing a growing collaboration among agencies and rising adoption of automation and zero trust.

"Agencies are taking tangible steps to automate some of their security, and I predict that we'll see them use automation to combat increasingly sophisticated cyberattacks," says Splunk Group Vice President and Chief Strategic Advisor for Public Sector Juliana Vida. "They're also taking initial steps to formalize implementation of zero trust adoption."

But these are no quick fixes. Public sector organizations have fewer financial and talent resources compared to the private sector, and face more red tape because of the high stakes of their operations.



LaLisha Hurt, industry advisor for public sector and federal government at Splunk, says that “many agencies are not taking advantage of the funds because they either are not aware or need help with submitting successful project proposals to the TMF board for approval.”

Automation will help drive efficiencies in resource-constrained environments, Vida says.

“The public sector is embracing automation,” she says. “It will take another several years to roll out, but it will really make a difference in repurposing the human resources currently spending time on easily repeatable, mundane, administrative tasks to higher-level work requiring creativity and innovative thinking.”





While public agencies have more than their fair share of unique challenges, one advantage the public sector at large has is its unified mission. There's no competition, since the shared mission is the welfare of the public. One of our predictions last year was that we would see more information sharing and collaboration among agencies, as they put their heads together to figure out how to address new risks and cybersecurity attack vectors. And this prediction is coming true:

“Public and private partnerships came into their own during this past year in a very big way,” Vida says. “These partnerships on information sharing and coordinated cyber defense plans are seeing success and finally starting to operationalize collaboration.”

Change is rarely fast in the public sector. At least, it never comes as quickly as leaders want. But the right tools are coming, and improvements are on the horizon.

Predictions and Survival Strategies for 2023

07

Talent

Cross-train and upskill your existing workforce to fill recruiting pipeline gaps.

09

Supply Chain

The SBOM will become standard.

11

Privacy

Regulation will start at the local and state levels.

13

Ransomware

K-12 schools will be hit especially hard.

15

ITOps Security Convergence

CISOs will take more responsibility for IT resilience.

17

Good Things Come to Those Who Wait Prepare

19

Contributors



Prediction

To address the talent shortage, public sector organizations will rely on clever short-term strategies ahead of long-term solutions.

A skilled worker is hard to find, especially for the public sector. Splunk's [Economic Impact of Data Innovation Industry report](#) found that a clear majority, across multiple major industries surveyed, cited recruiting and retaining talent as a key challenge. The inability to hire and retain workers with the right skills, however, is hitting the public sector especially hard. An Axios report last summer found that although the private sector had recovered 99% of all jobs lost during the pandemic, the [public sector had regained just 58%.](#)

Automation is a probable long-term solution, but when we asked our experts at Splunk for their take, they're not counting on it for another several years at least. Juliana Vida, group vice president and chief strategic advisor at Splunk, says, "We haven't seen or heard significant uptake in automation adoption, since many organizations aren't at a place where they can take advantage of advanced capabilities just yet."

While automation won't be the magic bullet, planning ahead and getting more out of existing investments might just be enough to tide organizations over.

"We've been seeing a lot of cross training so skills can be shared across team members," says Tina Carkhuff, industry advisor at Splunk. But retraining can only do so much (and can add to that other problem, burnout). In any case, retraining alone



wouldn't alleviate the **talent shortage of 8.6 million in the EU**, which faces a severe dearth of workers with needed digital and technological skills.

Public sector organizations anticipate short employee retention spans and actually build expected departures into their hiring plans. Carkhuff says, "State, local and government agencies, as well as universities, are hiring junior employees fresh out of college. These employees generally come in at lower salaries but get great training and experience that they can take to their next role. CIOs know these employees will leave for higher salaries, but they often return later in their careers to fill higher-level positions — and so public sector organizations are starting to count on being their first and maybe third employers."

In fact, we know of a CISO who set up a whole SOC around a university to get fresh graduates. He wasn't in the public sector, but had similar challenges around attracting and retaining talent. He turned new grads into junior analysts, knowing that they'd leave in two years for a more lucrative opportunity elsewhere later, and made that his talent strategy.

Public sector organizations will also increasingly partner with their vendors to get more out of their existing investments.

"Coping with the talent shortage will not look like more new tools that automate every process and action," Vida says. "It'll look like making better use of existing tools, to squeeze more juice out of the orange."

If you can't afford an orange juicer right now, use the hands you've already got and just squeeze as fast as you can. This is in the best interest of vendors as well, because driving wider adoption of their tools will boost their customer retention.



Prediction

Driven by a federal mandate and supply chain risks, the software bill of materials (SBOM) will become standard within the next three years.

The supply chain attacks on SolarWinds two years ago have since been followed by a steady succession of additional attacks — Log4Shell, Kaseya and others. It makes sense that organizations are devoting a lot of attention and resources to addressing the risks; 97% have done so, according to Splunk's [State of Security 2022 report](#). We think the next strategy to mitigate supply chain risks is the SBOM.

An SBOM lists the elements within a software package. In the event of a supply chain attack, the organization that's fallen victim would have to trace every component that resides within the product to figure out what components can install software and whether the constituents that use their services are compromised.

Agencies will be the first to require a software bill of materials, or SBOM, when they purchase software, says Splunk Distinguished Security Strategist Ryan Kovar. Given that software products often incorporate many open source

projects, the organization compromised would have to track down various owners of those — including, as Kovar puts it, “that one person in Norway who happens to be the only maintainer in the world of a particular project.” It's a tough job to identify the components and determine whether each was compromised by the attack, but an SBOM would help organizations quickly ascertain the extent of the damage.

There will be more implementation and an increased focus on supply chain security next year, and then eventually, to sell to the government, you'll have to have an SBOM. "By 2025, SBOMs will be required by the government for software purchases," Kovar predicts.

"It won't happen overnight," says LaLisha Hurt, industry advisor for public sector and federal government. "Over time, we'll see each agency and procurement office start to require SBOMs, and it'll become a standard requirement in the next couple of years."

The standard can't come soon enough. Another SolarWinds, Log4J, you-name-it sort of attack is imminent, and it'll probably be open source because, in the words of Kovar, "No one is looking."

GitHub seems to agree: The company has taken [preemptive steps by announcing plans to support code signing](#), which is a digital wax seal that helps open source maintainers verify that the code they create is the same code that ends up in the software packages that users download. But preemptive measures, however necessary, won't stop attacks from happening altogether. Organizations need to be prepared to respond and minimize damage when the inevitable attack does strike — which is where the SBOM will come in.



Prediction

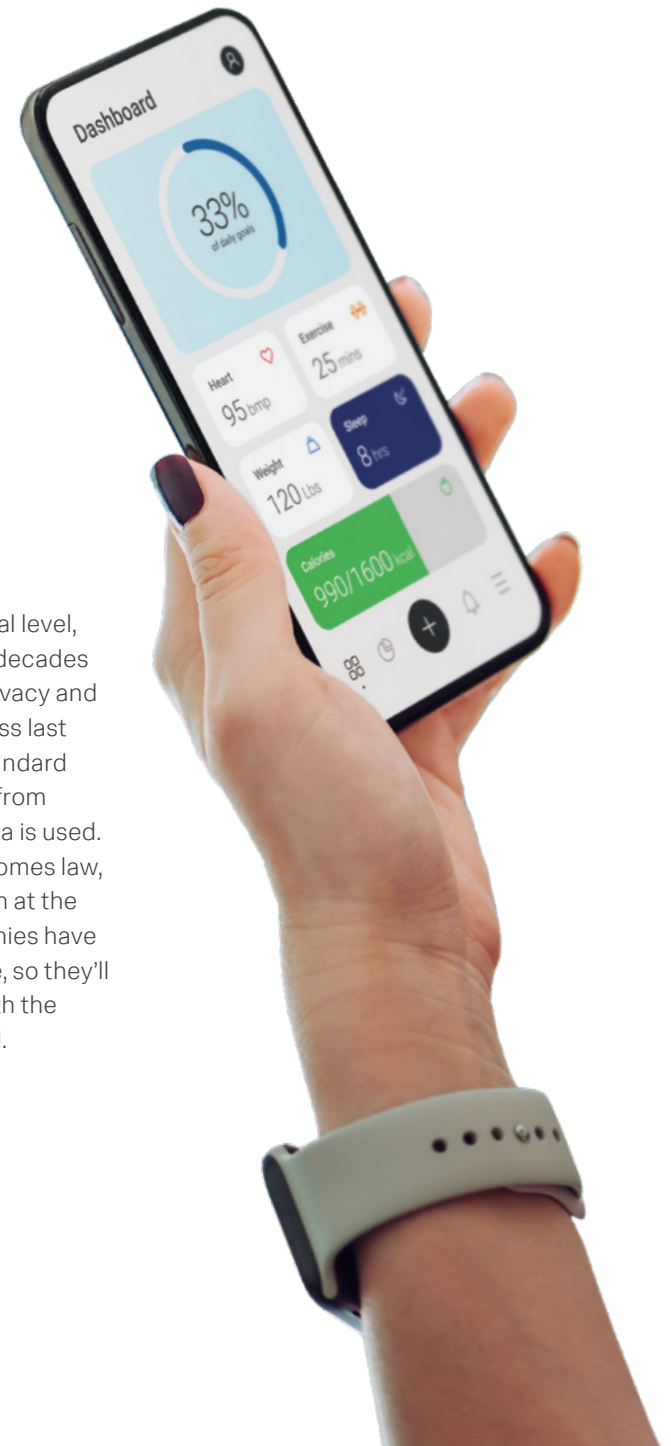
Privacy regulations will tighten, first at the state and local level and then at the federal level.

As a result of recent legislative changes in America, consumers are more concerned about the privacy of their data than ever before.

“I’ve seen a ridiculous number of people pop up on Signal in the last year or so,” says Global Security Strategist Mick Baccio. Gone, he says, are the days when it was just him and a clutch of threat-hunter colleagues. “Now, it’s Boomers to Zoomers and everyone in between. 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.”

This greater collective demand for privacy will affect companies that collect any data (which is nearly all of them). From Google Maps to The New York Times, menstruation apps to fitness trackers, corporations will be compelled to take more measures to protect consumer privacy.

There’s some movement at the federal level, even though such efforts have been decades in the making. The American Data Privacy and Protection Act, introduced in Congress last summer, would provide a national standard on what data companies can gather from individuals and regulate how that data is used. But until — and if — that motion becomes law, we’ll see continued privacy regulation at the state and local levels. Private companies have a patchwork of legislation to navigate, so they’ll often err on the side of complying with the strictest regulations at the state level.



In the public sector, on the other hand, both privacy and secrecy have always been significant concerns. Collecting new types, and greater volumes, of data may present challenges, but not a reassessment of values.

The value of citizen privacy has been and remains strong, says Juliana Vida. “That’s not changing. We just have more data to deal with.”

Inter-agency information sharing, on the other hand, is slowly evolving. Agencies see greater value in responsible information sharing and are increasingly working on secure solutions, says LaLisha Hurt.

“There was hesitancy in the beginning with information sharing, and case studies detailing certain situations,” Hurt says. “But there has been good progress on that front and this momentum will likely continue in 2023.”



Prediction

Ransomware attacks will get more professionalized and only keep on coming, especially against K-12 schools.

The barrage of ransomware attacks hasn't ceased. In fact, ransomware gangs are getting more professional and better organized. And they're seeing results. An [April report](#) found that 46% of organizations paid ransoms in 2021, up from 32% in 2020. And Splunk's [State of Security report](#) found that 79% of organizations have experienced ransomware attacks. "Ransomware moved from being a service to an economy," Mick Baccio says. "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."

Educational organizations are especially at risk. Splunk industry advisor Tina Carkhuff says, "K-12s are the most common target for ransomware attacks. We've seen some large ransomware attacks recently that have forced CIOs to rethink their security strategies. It's a top-of-mind issue as schools investigate ways to protect their data."

It really should be top-of-mind. Throughout the first half of 2022, education and research organizations [suffered 2,297 attacks per week](#), 44% more compared to the same time

last year. What's worse is that the public sector has been paying an especially steep price. Whereas [the average cost to a private organization was \\$1.8 million](#), educational institutions paid \$2.7 million per incident, which includes not only the ransom payment but also other ensuing recovery costs. (Colleges and universities usually don't back up their systems, which makes cleaning up the aftermath of a ransomware attack messier and pricier.)



Not all hope is lost, however. In September 2022, the Cybersecurity and Infrastructure Security Agency released a congressionally mandated report that detailed the cyber threats facing K-12 schools and outlined recommendations for how federal and state resources should be allocated to counteract such threats. The amount of money that public sector organizations spend on cybersecurity is rising, too.

“Twenty-five percent of organizations are spending more money on cybersecurity than they have in the past,” Carkhuff says. “And the average salary for CISOs has also risen. There’s more attention spent on security at the board level in educational institutions. If an organization can’t spend more on security tools or personnel, many will opt for cyber insurance as an alternate protective mechanism.”

Insurance can be an effective remediation strategy, blunting the financial blow. While basic cybersecurity practices will stop many attacks, no organization can count on stopping them all.

“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.”



Prediction:

As ITOps and security tools and data converge, public sector CISOs will (gradually) take on more responsibility for broad IT resilience.

The word “resilience” is coming up a lot more in IT and security circles. Given the last few years, it’s no surprise. We’ve never been able to prevent every attack, error or outage, so the real issue is not only how well you can minimize such incidents, but also how well you can recover from them.

“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.”

Woods says that regulation puts some sectors in Europe, such as finance, ahead of the game on resilience. Legislative and regulatory action comes more slowly in the United States, so organizations in the commercial and public spheres will have to manage their own strategies. One way that we’ll probably follow the European lead is to rely on CISOs for leadership around broader resilience.

“In most organizations, the only people who know how to do robust monitoring properly are security, because it’s their lifeblood,” Woods says. “You can’t do security without robust monitoring. Everything else, you can do without monitoring — you just do it badly.”

“We’ve been talking about resilience across the enterprise for decades,” says Patrick Coughlin, Splunk’s group vice president of security products.

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.

“We’re starting to see the organizational dynamics and definition of mission reflect the convergence at the data layer,” Coughlin says. “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.”

That’s the leading edge of the private sector. LaLisha Hurt says the public sector will eventually follow suit with many newly appointed CISO roles.

“Should the role of the CISO change? Absolutely,” she says.

“But things are evolving and changing faster in the private sector than the public sector. In an ideal world, the CISO should be working closely with the CTO and CIO, creating a true partnership in combating cyber attacks and protecting critical assets. Silos still exist unfortunately, and partnership is definitely needed. We’ll see this trend developing in the next year and beyond.”



Good Things Come to Those Who ~~Wait~~ Prepare

All good things take time, or so the adage goes. This is especially true for public sector organizations, which shoulder not only the burden of mission-critical operations, but also a greater scarcity of resources, compared to the private sector. That's why nearly every prediction we've made for the public sector is a prediction of a gradual evolution, whether it's the convergence of security and ITOps, or an SBOM requirement at the national level.



The real winners, ultimately, are going to be those who make investments to be data-forward. “Data is the new form of power,” says Kriss Deiglmeier, chief of social impact at Splunk. “In the next one to five years, governments will realize the power of data and make investments to become more data-forward. More will use data to drive outcomes, to spend and invest effectively, starting at the agency level.”

While the larger strides to become data-forward are underway, agencies and institutions will have to rely on existing investments and other short-term strategies to fulfill their missions in the here and now. They will take things into their own hands, implementing privacy regulations at the local and state levels, as well as forging information sharing partnerships with organizations in both the private and public sectors.

“These public-private partnerships will continue on in their sharing of threat information,” Vida says. “We’re going to see the next evolution toward operational collaboration, where industries will come together for planning, threat analysis and a coordinated defense against cyber threats.”

It’s a sign of the times: Smart strategies around talent, partnership and data technologies will allow public agencies to continue to serve the public, with the full reach of digital technology.



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.



LaLisha Hurt

LaLisha is industry advisor for the public sector, federal, at Splunk. An IT and security leader with more than two decades of experience, she has served at organizations in the public and private sectors, including GDIT, Capital One, GE and the Federal Reserve System.



Tina Carkhuff

Tina is industry advisor for the public sector at Splunk. She previously was the CIO of Houston, led executive programs at Gartner for K-12/higher education and healthcare, and founded the Cerebral Folate Deficiency Research Organization, helping families navigate the complexities of autism.



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.



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.



Juliana Vida

Juliana is group vice president and chief strategy advisor for the public sector. Before joining Splunk, she was a VP at Gartner, drove ships and flew helicopters for 24 years in the U.S. Navy, and held the role of Navy Deputy CIO in the Pentagon.



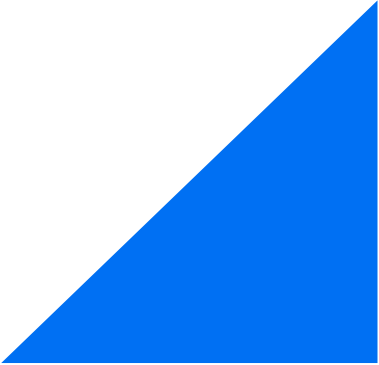
Kriss Deiglmeier

Kriss is Splunk’s chief of social impact and Splunk Global Impact. She is recognized as a social innovator, is a frequent speaker at global events, and was recently listed among the “50 Most Influential Women in U.S. Philanthropy” by Inside Philanthropy.



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 data
security reports.

[Learn More](#)



Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2022 Splunk Inc. All rights reserved.

22-25650-Splunk-Public Sector Predictions 2023-EB-108

splunk>[®]