VERSION NEXT NOW

TEKSYSTEMS SECURITY ISSUE | DECEMBER 2020

SECURITY-BUILT CULTURE

Make Security the Cornerstone That Enables Your Business

EDITOR'S LETTER

Security at the Forefront

Building a Security-First Mindset

It has been two decades since Y2K sent the IT industry into a frenzy. And while technologically we've advanced in leaps and bounds, there's much about security that hasn't changed; the strategies and mindset have remained surprisingly static.

Conventional thinking holds that security operates in the background—lurks quietly in the shadows, handled by a set of uber-geeks in black hoodies. They remain apart from the broader organization, tracking down bad actors through the cesspool of the dark web. They plug noticeable gaps. They use layers of expensive, bolt-on tools to build up a defense, but, like their adversaries, they do little to draw attention to themselves. As Paul Saffo, a futurist and adjunct professor at Stanford University, said back then, "Better to be an anonymous success than a public failure."

Security continues to operate behind the scenes and often, after the fact. And let's face it, the public mostly hears about the failures—that massive data breach, the leaked information, the stolen identities—and not necessarily the successes.

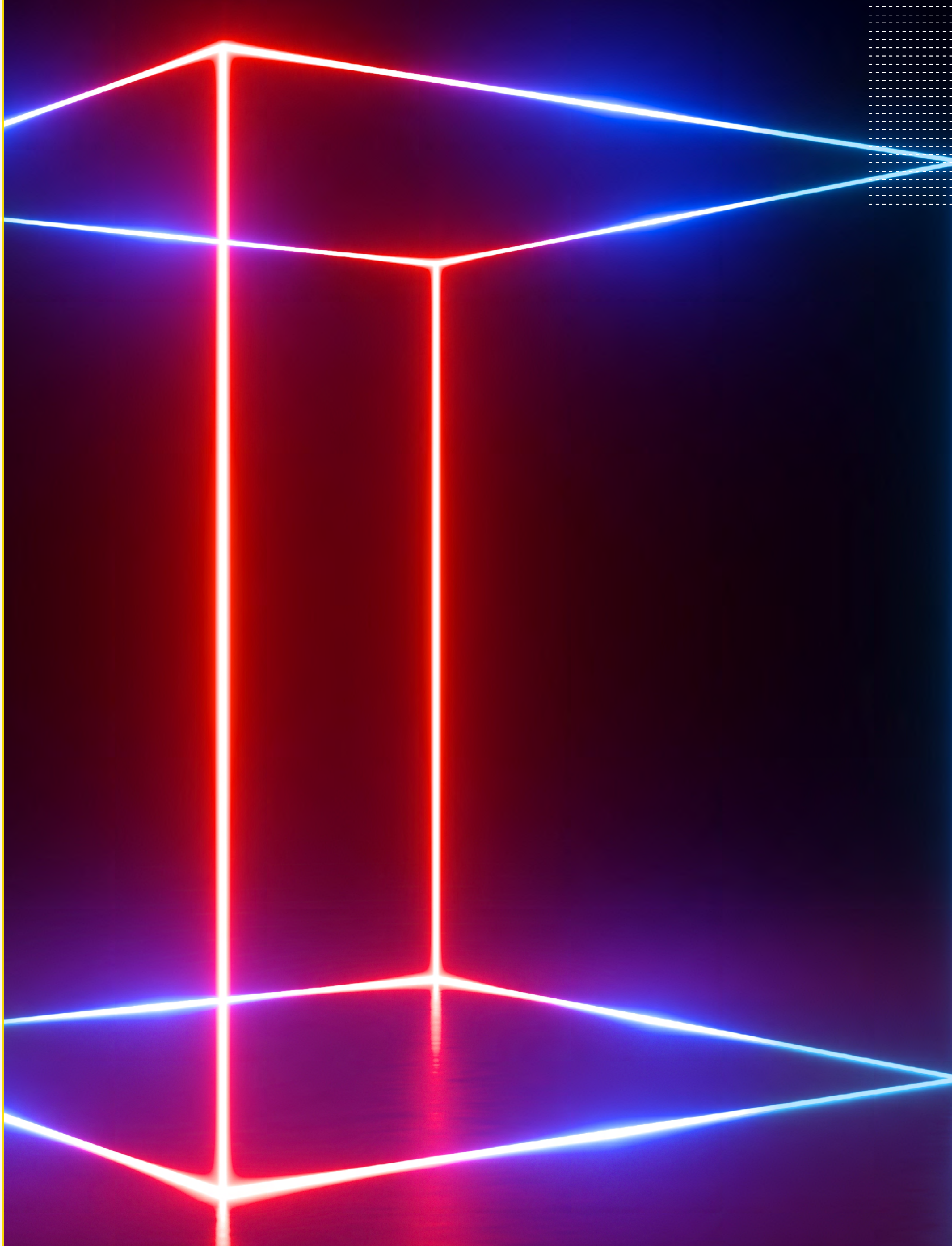
But what if security strategy and thinking evolved, too? People and our all-too-human behaviors are often the weakest link in any security setup. Phishing, ransomware, malware often use psychology to get people to unwittingly give up secrets or facilitate breaches. With a global pandemic scattering the global workforce, it's time to make security a very public, proactive, front-line priority and to spread the responsibility for security across the shoulders of each and every person at your organization.

In this issue of *Version Next, Now*, our experts will talk about the importance of monitoring, analyzing and correlating threat information across the whole organization. You'll learn how to foster better collaboration between IT security, operations and the rest of your company. And, arguably most important, how to infuse security-first thinking, behavior and practices into every facet of your workforce's day-to-day activities.

It's time to bring security out of the shadows.

Sharon Florentine
Contributing Editor

FEATURES



SECTION 01

THE CHANGE AGENT

Whether focused on business continuity or a return to growth, every company finds themselves at different stages of their recovery. Leading organizations are using the pandemic as an opportunity to reset their security strategy.

01

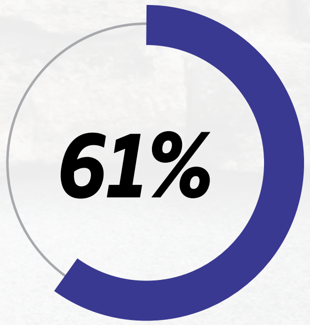
Resiliency in the Face of Adversity

A company's security team is typically relegated to the background. Actively monitoring the perimeter. Setting rules and guidelines to reduce risk exposure. Responding to incidents, protecting the organization. Security is a balancing act. On one hand, security means managing risk, limiting exposure, and securing data and assets. On the other, security means enacting nimble processes to ensure the right employees have access to the right data at the right time, so that products get delivered on time and on budget. Despite these myriad responsibilities, security is frequently an afterthought, bolted onto organizations' public, customer- and user-facing applications and processes. But consider this: what if security was instead at the forefront and a security-first mindset permeated the entire organization?

The pace of change and digital disruption already stretched security teams to their limits. The proliferation of endpoint devices expanded attack surfaces. Increasing regulatory and privacy policy compliance requirements increased risk exposure. The escalating sophistication, volume and velocity of cyberattacks require 24/7 monitoring. Then, a global pandemic and the resulting "work from anywhere" response by organizations exacerbated these pressures almost literally overnight. Security teams had to manage massive deployments of employees to remote work environments, further extending the company's security perimeter. The acceleration of digital transformation initiatives introduced new technology, processes and workflows that must be accounted for and secured. Organizations with mature security operations were able to rise to the challenge and weathered the immediate storm, maintaining business continuity and running the business remotely. However, for every success story, there are many more organizations for whom security is still viewed as an impediment to the business, creating inefficiencies, slowing down product development and requiring rework. Security teams are impacted by inefficiencies and constraints that limit their ability to operate at optimal levels.

Security Team Constraints

- **Lack of alignment across security, development and infrastructure teams:** Different goals, separate priorities and incompatible tools used to get the job done create friction and inefficiencies between teams.
- **Budget ownership:** Politics across security and IT teams generate discontent regarding where and how security funds are spent.
- Shortage of security talent: The U.S. has less than half the cybersecurity candidates it needs to handle increasing demand.[2]
- **Redundancy across the layers of the security organization:** Security teams that have similar skills and perform similar tasks aren't working in concert, leading to inadequate security measures in some areas and an overabundance of measures in others.

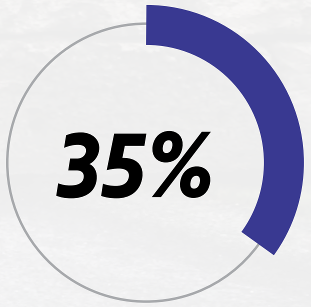


61% of organizations *report they have no real integration between SOC and NOC teams*[1]

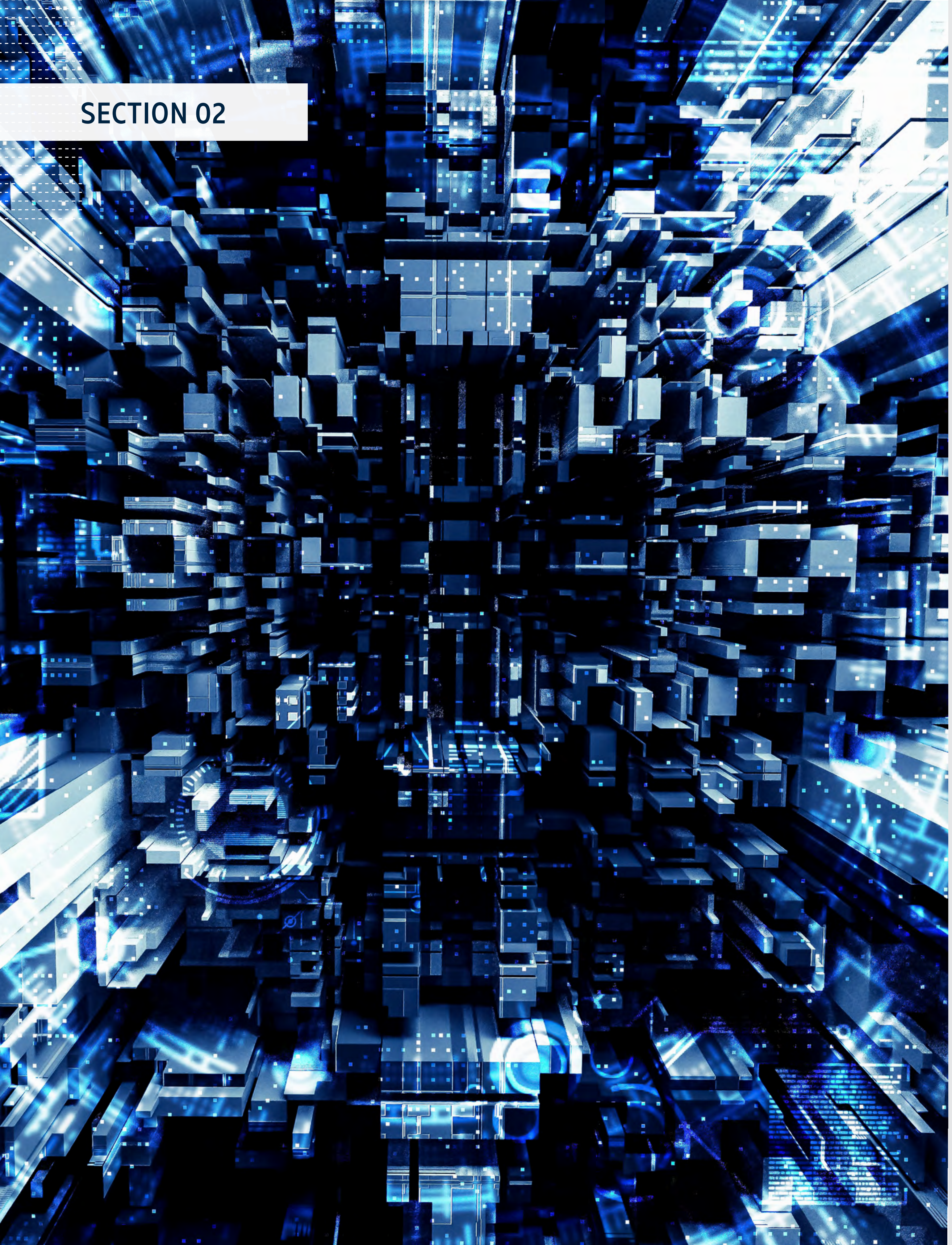
Common Security Layers

- **Security Operations:** foster collaboration across IT security and IT operations teams
- **Security Operations Center (SOC):** monitor, analyze and correlate threat information across the organization
- DevSecOps: focused on infusing security practices into application development

The pandemic has impacted organizations' overall security posture and expanded their risk profile. Whether focused on business continuity or a return to growth in the "next normal," every company finds themselves at different stages of their recovery. Leading organizations are using the pandemic as an opportunity to reset their security strategy, improve alignment and imbed security into the culture of the organization—ultimately enabling business to drive successful outcomes.



35% of organizations cite improving their security *posture as a top outcome achieved from digital transformation initiatives*


SECTION 02

MARKET PERSPECTIVE

An outside perspective from a company, leader, practitioner, analyst, influencer, etc. that highlights how the featured “change agent” shows up in the market and the expected outcomes achieved as a result of owning change.

02

Harness the Power of Security

Q **What has the pandemic taught organizations about their security posture?**

A ***Jason Remillard (Data443):*** *Organizations quickly realized they were not as prepared as they thought they were. Much like everything associated with the pandemic, it highlighted the gaps in information security. Whether it was BCP [business continuity management] or rogue access, it highlighted how far things could go and the new invisible border. For years it was the coffee shop, but now it's truly fuzzy and distributed and remote.*

Q **How should organizations deal with potential gaps created by increasing attack surfaces resulting from the expansion of remote work?**

A ***A: JR (Data443) :*** *What we're really seeing now as the recovery starts are gaps in capacity and capability, which really is a shortage of talented people. So that's putting more reliance on technology processes and procedures. Tools are a great place to start, but you must have a plan and rely on sound methodologies to make these tools valuable. Otherwise, you're just wasting time and resources, automating bad things and re-executing bad behavior. That becomes a big risk, especially as pressure increases on the business. Early in the pandemic businesses hunkered down to reduce risk. Now they're looking to accelerate out of the curve, and they'll rely heavily on infosec to come out of that curve explosively. If infosec teams thought the pressure was full before, it's really going to ramp up now. It's going to be even harder.*

Also, you can't just do blanket things anymore. You must be very focused. Data443 specializes in data identification and risk, and we advise customers to be very targeted and pointed with their spend, activity and efforts. Companies should start looking at data inventory, classification and governance and do more focused activities. You don't want to spend money on tools or services for things that aren't necessarily a risk to the business.

Finally, privacy is another area that should concern organizations. CCPA [California Consumer Privacy Act] and GDPR [General Data Protection Regulation] went on the books in 2020, but everyone sort of forgot about it. Now companies have to get back to that. They are germane and material to the business, and sorry, infosec, but you're going to have to really deal with that. The auditors will be asking for it; COVID doesn't give you a break on compliance. Overall, you've got to get smarter and rely on your partners to manage risk exposure.

> *"Early in the pandemic businesses hunkered down to reduce risk. Now they're looking to accelerate out of the curve, and **they'll rely heavily on infosec to come out of that curve explosively**."*
>
> **Jason Remillard**
> *President*
> *Data443*

Q **What about data breaches? Are there more concerns given the expansion of remote work?**

A ***JR (Data443):*** *Commercial insurance carriers that offer data breach coverage are looking at how they cover companies due to the increased data breach risk associated with remote work. The actuaries can't even fully analyze the risk because people are living at home. Work-from-home polices are tricky. Controls often aren't enforced, and companies are just allowing too much data flowing freely. Risk and insurance firms are looking at the increased risk and saying, we've got a problem. They might have given companies a break due to the pandemic, but it could get ugly. In the old days, you went home with your briefcase and it was locked, but we have many open assets now. It's just way too free, too easy for breaches to occur. Organizations really need to get into a defensive posture. They need to document what they did and what they didn't do to prepare for COVID-related remote work litigation.*

Q

What should organizations keep in mind as they engage external partners?

A

JR (Data443): *First you need to be honest with yourself, assess and identify your most critical gaps. Then set very clear expectations with your partners about specifically where you need help and be open about spend allocation. You'll need to be more intelligent about the how, because spend is a huge concern. You don't want to spend money on tools or services that aren't a high risk to the organization.*

Q

What are some of the lasting impacts of the pandemic on security strategies?

A

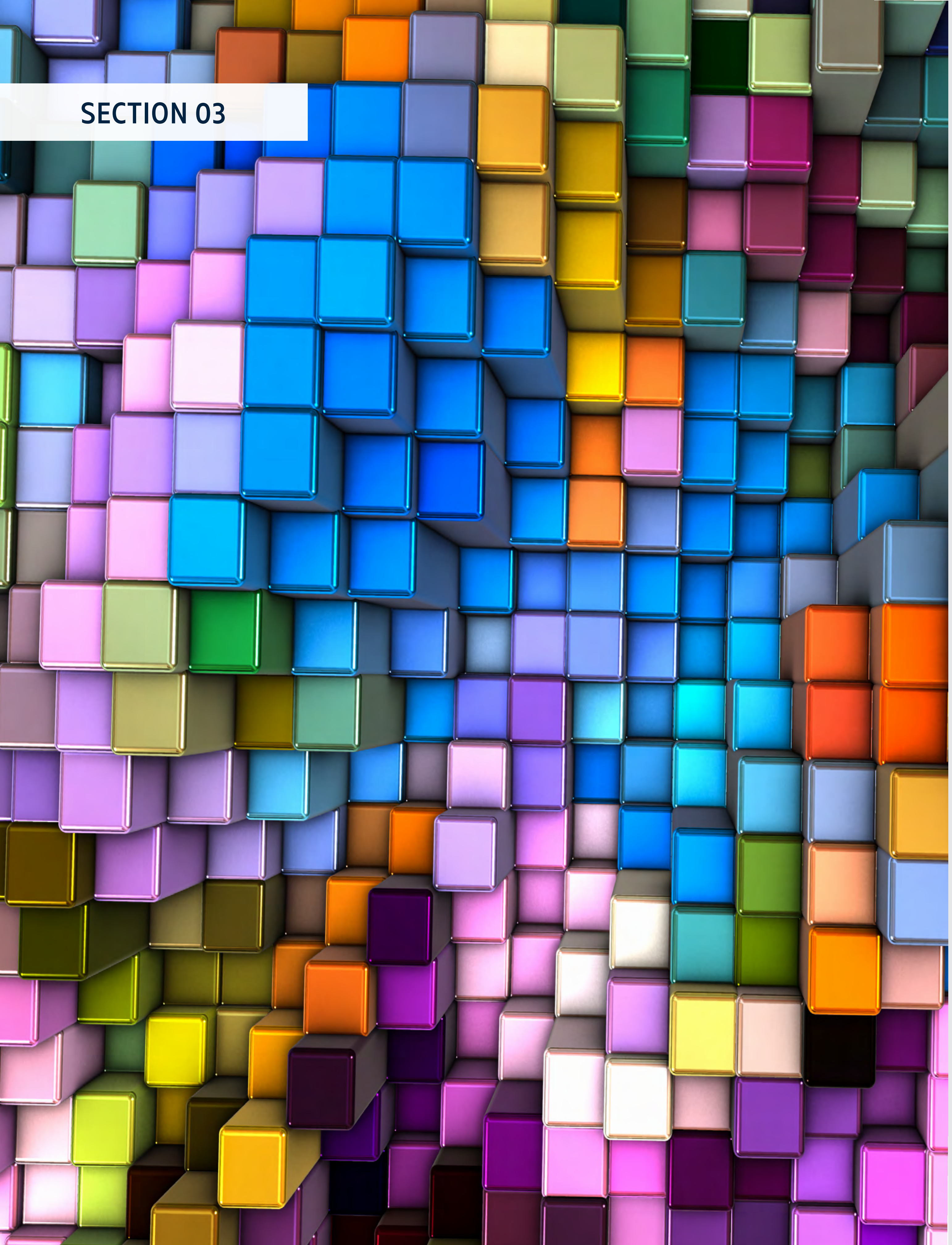
JR (Data443): *Everything will have a lens of data privacy and compliance. That lens includes how we enable data privacy and compliance and how business will react to this new data risk. There will be a cost to respond to data risk, so organizations certainly need to think about the material costs, and it's something every business will have to deal with. For instance, ransomware is already huge, but now you'll have to deal with privacy and litigation with everything you do.*

Q

What should organizations be thinking about for 2021 as it relates to their security posture?

A

JR (Data443): *There should be a lot of consumption of automated risk profiling. Whether it's ISO or GRC systems, it's all about identifying gaps quicker, evaluating third-party risk or insider risk and continuously analyzing that risk. That continuous risk analysis of systems or people will be a big area for companies to get through. If they can automate it properly and intelligently, it helps everything move smoother and faster.*



SECTION 03

OUR PERSPECTIVE

TEKsystems leaders Adam Cavnar, Mike Mulligan, and Kory Patrick, share their points of view on how organizations can fortify the enterprise and enable business to drive successful outcomes.

SECTION 03 | OUR PERSPECTIVE

03

Take Bold Action to Fortify the Enterprise

The "next normal" is not the world we knew before COVID-19. At the onset of the pandemic, companies needed to transform from a primarily on-site work model to a largely remote workforce. To facilitate remote work, organizations quickly deployed company assets and, in many cases, employees increased the use of personal devices to access company data. These moves were initiated quickly at the onset of the public health crisis, when the primary focus was on continued operations and business continuity. But the need for business continuity traded agility for security, resulting in a loss of control and creating blind spots for security teams, lowering their ability to respond to threats, decreasing confidence and exposing the enterprise to additional risk. As organizations moved beyond the initial focus on continuity, they were forced to deal with their new and vastly expanded risk profile. Already stressed security teams were further strained to manage and protect remote assets. Organizations now must fully assess where they are based on their stage of recovery; then they can act to fortify the enterprise to be successful in the next normal. Consider the following:

"Security teams already have a lot of work on their shoulders," says TEKsystems Security Practice Manager Adam Cavnar. "But there's going to be a lot more as organizations evaluate their current security strategies through the lens of the pandemic. They can start by identifying gaps in processes or areas of increased risk exposure stemming from the proliferation of a remote workforce. Also, audit the tools that have been implemented. Organizations frequently find overlap—or even gaps—in capabilities that expose the company to risk. Then, update your strategies to close the gaps and, most importantly, disseminate those strategy updates across the entire organization, not just with the security teams."

> *"The post-COVID normal is not the normal we knew. Your security strategy must be* ***grounded in that reality.****"*

Adam Cavnar
Risk & Security Practice Manager
TEKsystems

"Not everyone thinks about security through the eyes of a security professional. Organizations must evolve that mindset, creating a culture where security, privacy and compliance are fully aligned components of the business," says TEKsystems Risk & Security Leader Kory Patrick. For example, security team members can work with their product team counterparts to help them appreciate how they can simultaneously reduce risk exposure and get products to market faster with a security-first approach to development. "DevSecOps, for instance, can be part of that, but it can't be the only solution, particularly when goals, objectives and metrics vary across different teams," Kory explains. Everyone responsible for getting a product to market must be trained on the importance and understand the value security brings to the table. Once the organization experiences the value, you can more easily shift mindsets and implement security as an enabler for growth.

Massive talent shortages and the pace of change in technology have put incredible pressure on security teams. "Automation and new tools have helped stem the tide but can also create new problems. With no clear guiding strategy, tools often overlap or have gaps in capability, exposing the organization to risk and creating inefficiencies across different teams," says Mike Mulligan, TEKsystems' practice executive for Risk & Security. "Companies frequently want 24/7/365 support and simply want to buy security," adds Mulligan. But that approach is expensive and impractical and, most importantly, fails to solve the underlying problem. To solve these challenges in the near-term, organizations should evaluate the talent they have across different teams. Then, they can identify areas where similar skills can be applied to other areas of need, building their own specialized security teams. For example, employees using tools to monitor applications might apply that aptitude to monitoring middleware or infrastructure to take some burden off the security teams. Other employees could be good candidates for upskilling to help fill security talent gaps. Then, work with your risk and security services partners to help bridge remaining gaps.

The long-term solution is more complex. But the benefits and potential competitive advantage can be huge. "What if my NOC [network operations center] and SOC [security operations center] exist in the same place and perform the same responsibilities?" asks Cavnar. "You can alleviate many of the challenges and inefficiencies security teams face today with such a combined approach," Cavnar says. The specific approach will be dependent on the unique organizational structure. But if you consider breaking down the silos that exist across your security teams, you can create synergies that will improve cyber hygiene, limit risk exposure and drive your business forward. You won't realize the value on day one, but a well-executed plan will set your organization up to succeed in the "next normal."

> *"When you build security into the beginning of development, then you can* ***inject those practices directly into the flow of the business.****"*

Kory Patrick
Risk & Security Leader
TEKsystems

> *"The acceleration of digital transformation expands the* ***attack surface and companies are more exposed*** *than ever before."*

Mike Mulligan
Practice Executive for Risk & Security Services
TEKsystems

SECTION 03

TEKsystems' Tips

Take a holistic approach to changing the security culture. Show how security can enable business, getting products to market faster with less rework and lower risk.

Evaluate security strategies and policies. Mind the gaps that have been created and follow through on addressing and fixing the disruptions.

Keep security talent inspired and connected. Remote work can be stressful, particularly for teams tasked with securing the enterprise. Ensure your security talent is getting the development and support they need.

Build specialized teams. Focus on upskilling your current talent pool and working with partners to help bridge the gaps.

Break down the silos. Look for redundancies across your security teams and tear down the silos to generate synergies and efficiencies.

Real-World Application: Adobe

As the security landscape grows increasingly complex and challenging, security leaders must evolve security practices and educate the entire organization to build a culture of security and help maintain a strong security posture.

As part of their dedication to continually developing a stronger security culture, Adobe recently launched a refreshed version of their Adobe Security Training & Advancement Program.[3] While all employees go through mandatory annual security awareness training and activities, this program is designed to give more technical staff—including engineers, product managers, program managers and other interested team members—deeper security knowledge through more advanced training. Since the launch of this updated program, Adobe has seen even greater overall participation by technical teams as well as positive feedback on the enhancements.

The Security Training & Advancement Program operates similarly to martial arts belt advancements, starting with a green belt and advancing to brown and then black belt. Each of the belt levels denotes a higher level of individual security achievements. To help ensure that employees are getting the most out of the training, this refreshed program tailors different tracks to fit each employee's specific job role and skill set.

With this companywide focus on security, Adobe can proactively help prevent potential security issues from affecting both the company and their customers and also more swiftly react to threats and remediate vulnerabilities when they appear.

All information shared herein was accessed from public sources as indicated.

TEKsystems Risk and Security Portfolio

Core team with expertise from critical including the FBI, top original equipment manufacturers (OEMs), top financial institutions, and top audit and compliance entities

2,800 consultants in the Risk & Security Services group

Process-driven approach enhanced by certified partnerships with major OEMs

Community-centric approach in each of our 120+ offices in North America

Elite partners of enterprise-class cyber and risk platforms like SailPoint and Data443

In good company

Transformational technologies demand equally transformative partnerships. TEKsystems has strategic partnerships with major OEMs and is proud to deliver product-agnostic security solutions that meet the unique needs of our customers.

The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the views of TEKsystems, Inc. or its related entities.

Meet Our Contributors

Adam Cavnar

Risk & Security Practice Manager | *TEKsystems*

Adam Cavnar has worked in the technology industry for nearly 20 years. He currently leads the risk and security practice consisting of experts with federal, government and private sector experience developing innovative new solutions to help clients deal with the increasing complexity of security concerns across digital, data, application, cloud and infrastructure platforms.

Mike Mulligan

Risk & Security Practice Executive | *TEKsystems*

Security executive Mike Mulligan has been in the tech industry for nearly 25 years and has experience overseeing sales and delivery strategies. He helps customers solve technology and workforce challenges related to data center, network infrastructure and security. Prior to his current role, Mike worked in a variety of capacities at TEKsystems, starting as a technical recruiter, then growing into roles including senior account executive and director of network services and regional director of divisional sales.

Kory Patrick

Solution Executive | *TEKsystems*

Kory Patrick is an information security professional offering more than 19 years of experience in designing, developing and managing cybersecurity projects in both public and private sectors. Kory possesses a strong background in threat analysis, vulnerability assessment, crisis management, implementing effective security controls, digital forensics and incident response (DFIR), and technical operations with a deep understanding of information security from multiple perspectives.

Gerard Lendore

Security Practice Architect | *TEKsystems*

Gerard has over 18 years of Information Security experience. With over 10 years in the Department of Defense Special Operations Command and over 5 years as a senior software developer in the private sector, his unique background places him in line with our nation's InfoSec leaders and professionals within the industry.

Jason Remillard

Founder, President, CEO Chairman of the Board | *Data443*

Real Life Security & Technology Expert with over 25 years of experience in pioneering technology solutions for Startups & Fortune 500 companies.

About TEKsystems®

We're partners in transformation. We help clients activate ideas and solutions to take advantage of a new world of opportunity. We are a team of 80,000 strong, working with over 6,000 clients, including 80% of the Fortune 500 across North America, Europe and Asia. As an industry leader in Full-Stack Technology Services, Talent Services and real-world application, we work with progressive leaders to drive change. That's the power of true partnership. TEKsystems is an Allegis Group company.

TEKsystems.com

Sharon Florentine, Contributing Editor

Sharon Florentine is the contributing editor for *Version Next, Now*, TEKsystems' quarterly publication. She is an award-winning independent writer and editor with more than 20 years of experience in the tech industry. Her work has appeared in Computerworld, PC Magazine, CRN and eWEEK, among others, and she is a passionate advocate for equity, diversity and inclusion in tech and beyond. Most recently, Sharon was a senior writer for CIO.com, where she covered software development, Agile, IT careers, learning and development, and DE&I. She lives near Philadelphia.

Listen Now

Don't miss Adam Cavnar, Mike Mulligan and Kory Patrick, on The Agile World podcast. In a three-part series, host, author and business expert, Greg Kihlström sits down with Gerard Lendore, Mike and Kory to discuss how organizations must take action to not only survive, but thrive, in the digital economy.

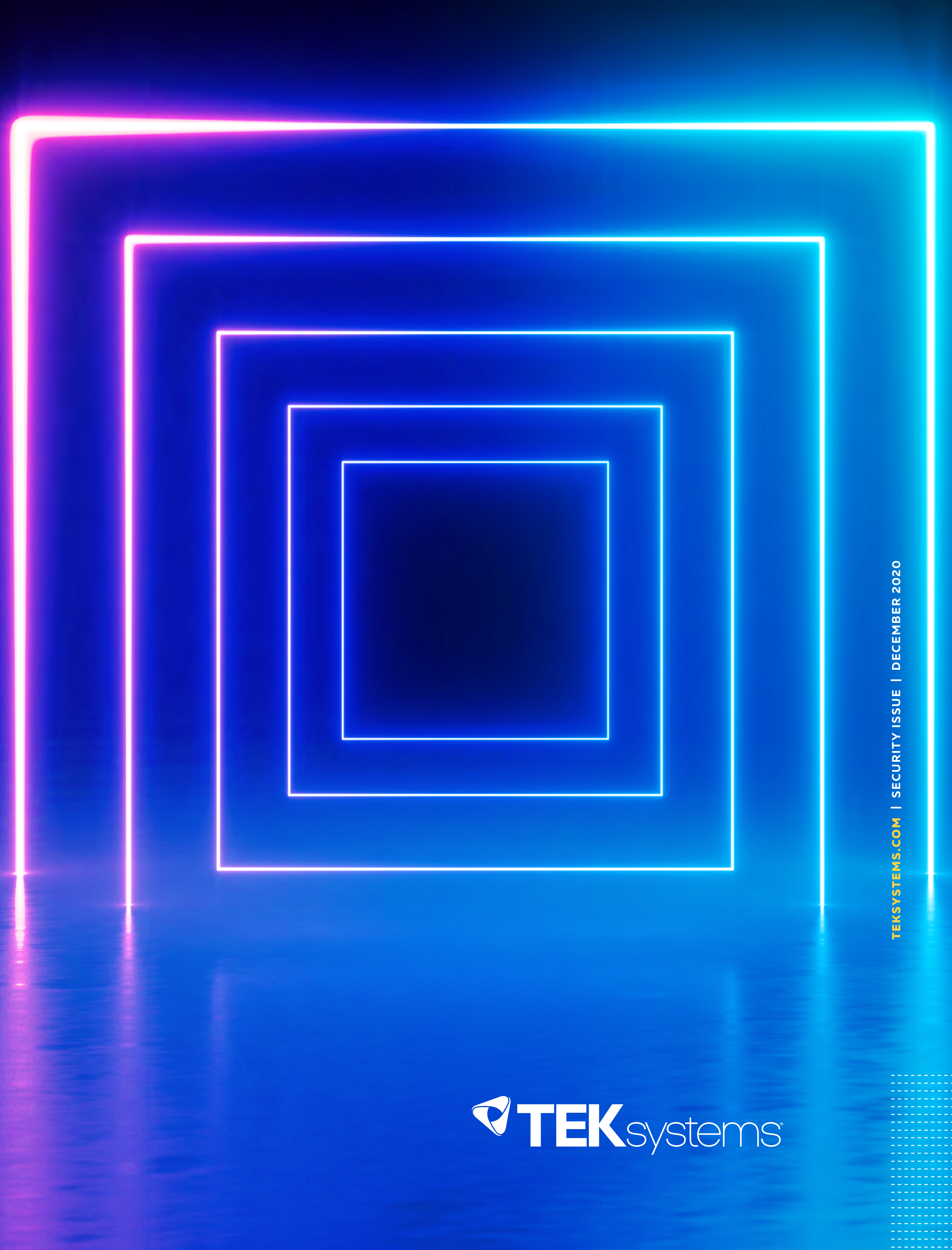
Be in the Know

Check out previous issues and know what's next Version Next, Now

Follow Us

Sources

1. Common and Best Practices for Security Operations Centers, 2019, **SANS Institute**
2. Build (Don't Buy): A Skills-Based Strategy to Solve the Cybersecurity Talent Shortage, **Emsi**
3. Building a Culture of Security, **Adobe**



TEKSYSTEMS.COM | SECURITY ISSUE | DECEMBER 2020

TEKsystems