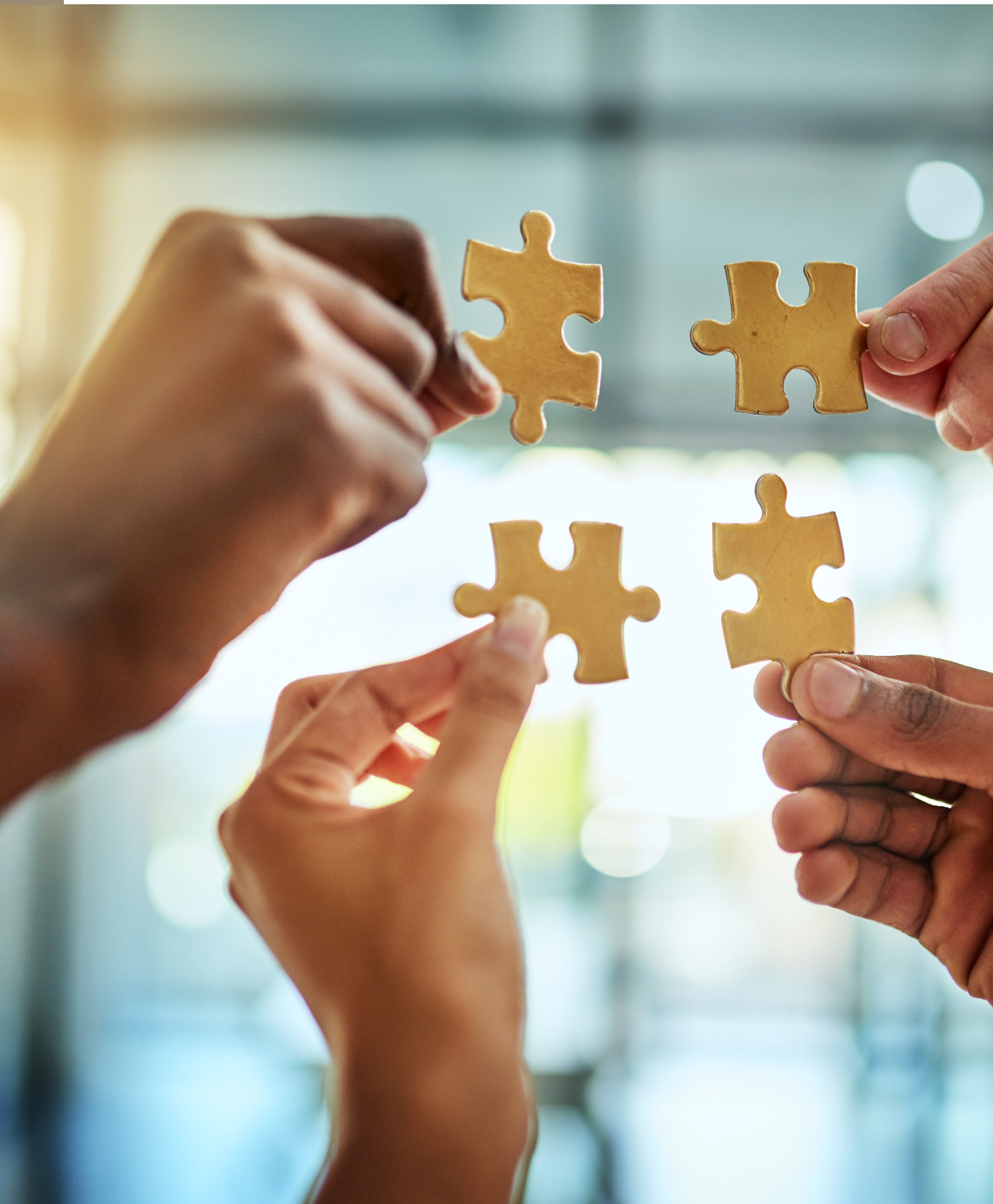
CSO CENTER®
FOR LEADERSHIP
& DEVELOPMENT
ASIS International

EXECUTIVE SUMMARY

2021 Leadership Series

ASIS INTERNATIONAL
Advancing Security Worldwide®



About the CSO Center for Leadership and Development

The ASIS International CSO Center for Leadership and Development is a membership community exclusively for chief security officers and their deputies. The CSO Center provides curated benefits for senior security executives from leading global organizations and offers member-exclusive opportunities to network, share information, and collaborate to shape strategy and solve everyday challenges. Gain access to members-only discussion groups, virtual and in-person networking events, executive education sessions, benchmarking surveys, a digital resource library, and other valuable benefits.

Membership is reserved for the most senior security executives from large corporations, non-profits, governmental agencies, and public entities that meet certain revenue requirements. Applications to join must be submitted online and include a job description, employment affirmation, and an organization chart.

About the CSO Center Leadership Series

The CSO Center Leadership Series is an exclusive, invitation-only virtual experience for CSO Center members, bringing together the global community of chief security officers and their deputies to explore a wide variety of critical issues and compare approaches and strategies to best prepare for an uncertain future.

This three-part leadership series focused on the role strong partnerships can play as a force multiplier in CSO success. It is now available on-demand for CSO Center members. Visit *csocenter.org* for more details.

This CSO Center Leadership Series Executive Summary was compiled with the assistance of ASIS International staff, including CSO Center Director Carla Lochiatto, IOM, CAE, and *Security Management* Assistant Editor Sara Mosqueda. The Leadership Series was made possible by CSO Center volunteers, panelists, and moderators who generously shared their time and expertise, and it was sponsored by AlertEnterprise and Brivo.

csocenter.org

A Multidisciplinary Approach to Threat Assessment in a Post-2020 World

A lack of awareness into issues affecting employees—from anxiety to financial pressures to dissatisfaction with a toxic manager—can ultimately leave the door open to sabotage, reputational damage, or insider threats.

Executive-level leaders leverage partnerships with other departments, monitor the evolving security landscape, and manage effective communications. From a CSO's point of view, having a wide spectrum of partners available to share resources, ideas, and lessons learned can be invaluable. During the 2021 CSO Center Leadership Series, panelists discussed the value of partnerships—internal, external, and governmental—and what they mean to threat assessments and risk management in 2021 and beyond.

A significant part of building a comprehensive risk management program involves maintaining healthy relationships with other departments, notably human resources. This has become increasingly important since much of the workforce shifted to remote work in response to the COVID-19 pandemic, which altered much of the security landscape.

Greater importance now lies in heading off and mitigating insider threats. According to panelist Diana Concannon, dean for the California School of Forensic Studies and co-vice chair of the ASIS Extremism and Political Instability Community, the most common types of insider threats involve negligence, criminal intent, and third-party theft of privileged credentials.

Studies and surveys indicated that during the last year, people who were working from home faced unique pressures that increased anxiety, such as substance abuse and intimate partner violence, she said. A lack of awareness about issues affecting employees—both during and outside of work hours—can ultimately evolve into sabotage or other forms of insider attacks.

"Anxiety, depression, and substance misuse are specifically associated with compromised functioning and, particularly, specific research shows it's associated with compromised ethical decision making," Concannon said. "They're also associated with increased hostility, which is correlated with malicious insider threats."

Leaders can counter these anxieties by various means, starting with understanding which employees are at risk. A variety of different resources or efforts can help identify anxieties, dissatisfaction, or disturbing behavior.

Organizations or departments can implement behavioral threat assessments and wellness initiatives, while managers can perform remote check-ins with employees to assess their wellbeing and discuss any challenges.

Another consequence of the rise of remote work is employees' growing intolerance of toxic workplace cultures or managers, according to Nick Schacht, chief global development officer for the Society for Human Resource Management (SHRM).

Of those who voluntarily resign, Schacht said that 60 percent are leaving a manager, not the company. "They leave because they don't like their boss," he said. "If we can focus on making better bosses...not only do we increase retention, but we improve the culture and reduce the vulnerability to insider threat."

Schacht also recommended that security leaders remember or re-learn how to listen to staff, keeping an ear out for not only signs of anxiety, but also for frustrations or dissatisfaction with the organization.

Equally important is communicating safety initiatives and efforts to improve an organization's culture. Given how 2020 also featured substantial social justice campaigns that were also reflected in workplaces, Schacht further stressed the significance of teaching and encouraging employees and leaders to effectively communicate to build an effective solution instead of barriers.

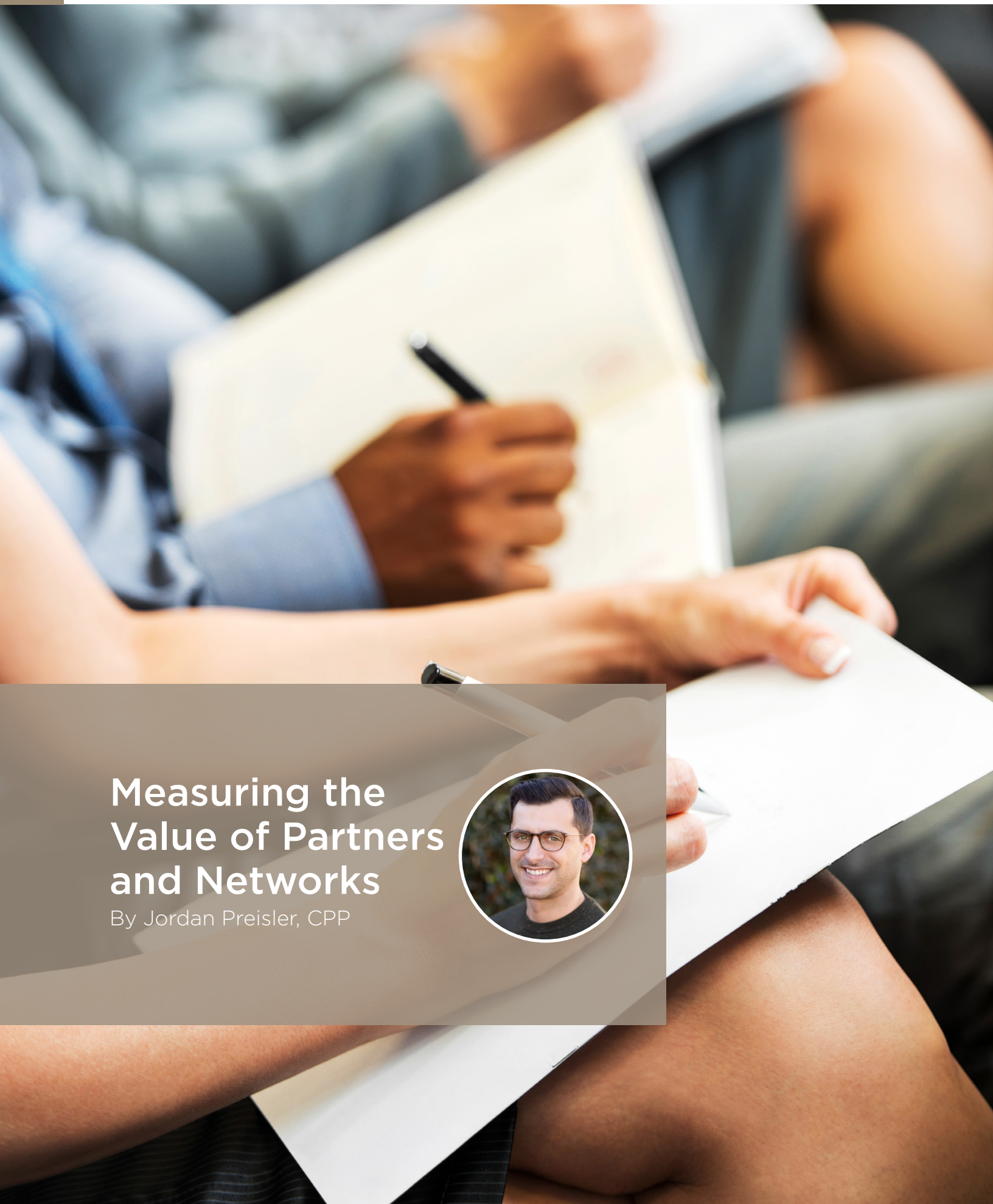
"There has to be an increasing push on... teaching people how to disagree without being disagreeable, how to confront without being confrontational, and really accept a range of beliefs in the workplace as long as we respect each other," Schacht said. "If you've got a workplace that you're going to, for example, allow people to wear rainbow t-shirts, you have to be ok with people wearing MAGA hats, and you have to allow people to respect that. This culture of safety then is based in part on a culture of respect for people."

THE STATE OF WORKPLACE EMOTION

For many all over the world, anxiety rates in the workplace have significantly risen within the past year. In Gallup's *State of the Global Workplace 2021 Report*, a survey of the impacts of the COVID-19 pandemic found that employees were reporting high levels of worry, stress, anger, and sadness in 2020 compared to the year before.

An estimated 43 percent of employees were stressed, and 24 percent felt anger during a lot of their workday—a record high from the past 11 years.

A sense of disrespect or a lack of respect also increased from 2019, Gallup found. "Globally, 14 percent of employees say they were not treated with respect during all of the previous day," according to the report. "This item includes experiences inside and outside the workplace. Lack of respect in the workplace correlates highly with employee perceptions of discrimination or harassment."



Measuring the Value of Partners and Networks

By Jordan Preisler, CPP

The theme of this year's CSO Center Leadership Series is building better partnerships, and as senior leaders we have an outsized influence on the creation of strong partnerships inside and outside our organizations.

It's been said that physical security, human resources, IT, and other similar cost centers are the horizontals that support a company's profitable verticals, and we build the strongest possible foundation for our company's success by working closely together.

In the last year, whether it's been temperature screening, contact tracing, or return-to-office planning, none of these vital initiatives could have been rolled out effectively without a concerted effort between physical security organizations and our internal partners. Established relationships ensured physical security had a seat at the table and a voice in the strategic conversations that led to the procurement of novel technologies and the creation of new processes that our physical security teams were later tasked with operationalizing.

Strong partnerships help us keep everyone safe, including our security teams operating in the field. As the conversation with our speakers made clear, the value of internal partnerships can also be quantified in their ability to influence on our behalf throughout the company. They can preemptively answer questions and calm the concerns of partners that may sit outside our spheres of influence. Simultaneously, they can help us to consider security-forward issues from perspectives we may not have in the past. These partnerships pave the way for our proposed solutions to be more holistic in nature, and in turn this means they are often approved by leadership more quickly and adopted across the business with less pushback.

At first, every company and every physical security organization struggled to adapt to the pandemic environment. We had to apply existing processes that had never been implemented, establish best practices to fill in gaps where policies didn't yet exist, and engage new technologies to solve problems we had never considered.

For many of us, this is where our external partnership with the CSO Center has proven its value and where its membership has shined. Through our Leadership Series, monthly Huddles, and peer-to-peer networking, physical security and partner executives have selflessly shared what worked for them so we could more quickly implement the right solutions—as well as what didn't, so we could learn from one another's mistakes.

The value created by partnerships can be calculated as savings in time, money, and increased safety and security. While it's often hard to calculate return on investment in our field, it's easy to see it here: whether our partnerships are internal or external, working together always makes us better at what we do.

Jordan Preisler, CPP
Vice President, Security Operations & Process Excellence, NBCUniversal
CSO Center Host, 2021 Leadership Series

ALERT ENTERPRISE
PHYSICAL | LOGICAL SECURITY CONVERGENCE

The 2021 CSO Center Leadership Series was sponsored by AlertEnterprise.

Opening your company's doors has never been so complicated—*or important.*

What we mean is, your employees and network of partners need fast, simple access to the doors, floors, folders, and databases where they work—but you also have to keep those same physical and digital spaces secure against constant cyber–physical threats.

What if you could bring together your HR, IT, and physical security teams (and systems) for one coordinated approach to workplace access—automating policy enforcement while also strengthening security and productivity? That's exactly what we can help you do with cyber–physical solutions that integrate with your existing systems. Here's what it looks like:

A human-centered employee experience

- Self-service for access inquiries
- Automated access across the employee lifecycle
- Workspaces where everyone feels confident and supported

A secure, productive work environment

- Greater productivity across every department
- Fewer manual requests for physical security
- Coordinated threat detection and response practices from a single source of truth

Stronger financial results

- Eliminate redundancies
- Unlock efficiencies
- Simplify compliance

Start today with AlertEnterprise.

We're ready when you are. Let's chat about how we can secure your digital transformation. Contact us today.

LET'S GET STARTED

alertenterprise.com

Strengthening Agency Assets Through Governmental and Federal Insights

After building bridges between internal partners, it's time to turn your attention to the possibilities embedded in force-multiplying public–private partnerships.

"Economic security is national security," said moderator Rich Mason at the beginning of this CSO Center Leadership Series session. By building and supporting bridges across the public and private sectors, CSOs have the opportunity to leverage government knowledge and expertise while sharing threat information and private-sector efficiencies. By helping to secure the private sector, Mason explained, government agencies foster a more stable environment for national security, growth, and advancement.

Today's CSO must be a chief bridge builder—not only with departments within an organization, but also with external entities.

During this panel, security leaders with experience in both the private and public sectors explored the challenges and demands of improving an organization's overall security and resiliency, especially through partnerships with external groups.

Representing the public sector, Karinda Washington, acting assistant secretary of Partnership and Engagement for the U.S. Department of Homeland Security (DHS), noted that for federal employees looking to cultivate and maintain partnerships with for-profit and non-public organizations, one of the biggest hurdles is the potential of an ethical dilemma. When seeking partnerships, Washington's department is aware that a successful venture is reliant on "whether our legal division believes that we can actually partner without implicating some type of conflict of interest or financial interest of a for-profit entity in working with government."

A goal for the department is in figuring out how to better partner with non-public groups, especially those with a focus on the national security space.

According to Bradford Willke, senior advisor for the U.S. Cybersecurity and Infrastructure Security Agency (CISA), part of DHS, once a partnership is established, achieving both collective and collaborative security will require accessibility to each other and an understanding of where divisional labor will be; whereas a lack of awareness or knowledge about available resources and capabilities can hamper an organization, especially during an incident like the

ransomware attack on Colonial Pipeline earlier this year.

One step in the direction of more effective partnerships—at least from CISA's point of view—is breaking down preexisting barriers and avoiding building new ones when it comes to different aspects of security.

"There's risk in doing that," said Scott Breor, associated director for security programs for CISA's Infrastructure Security Division. However, CISA offers resources and training that can serve as a force multiplier for organizations, including cyber and physical risk notifications, one-day workshops and webinars on emerging threats or trends, guidance around drone response, and a new insider threat guide. Breor also noted that relevant ASIS materials could be beneficial for public or private entities.

At the DHS, a pilot program called Exemplar assists in bridging gaps between public and private groups. Through this training program, GS-11 through GS-15 employees in the science, technology, engineering, and mathematics (STEM) fields at CISA and the Science and Technology Directorate are detailed out to for-profit private sector entities to train, bringing private-sector expertise back to DHS to help improve program efficiency and develop best practices.

Conversely, Washington said, through the DHS Loaned Executive Program, executive-level private-sector talent can join forces with DHS to partner on specific projects over the course of a year, sharing their unique, specialized skill sets with the government and provide "fresh eyes" on old problems.

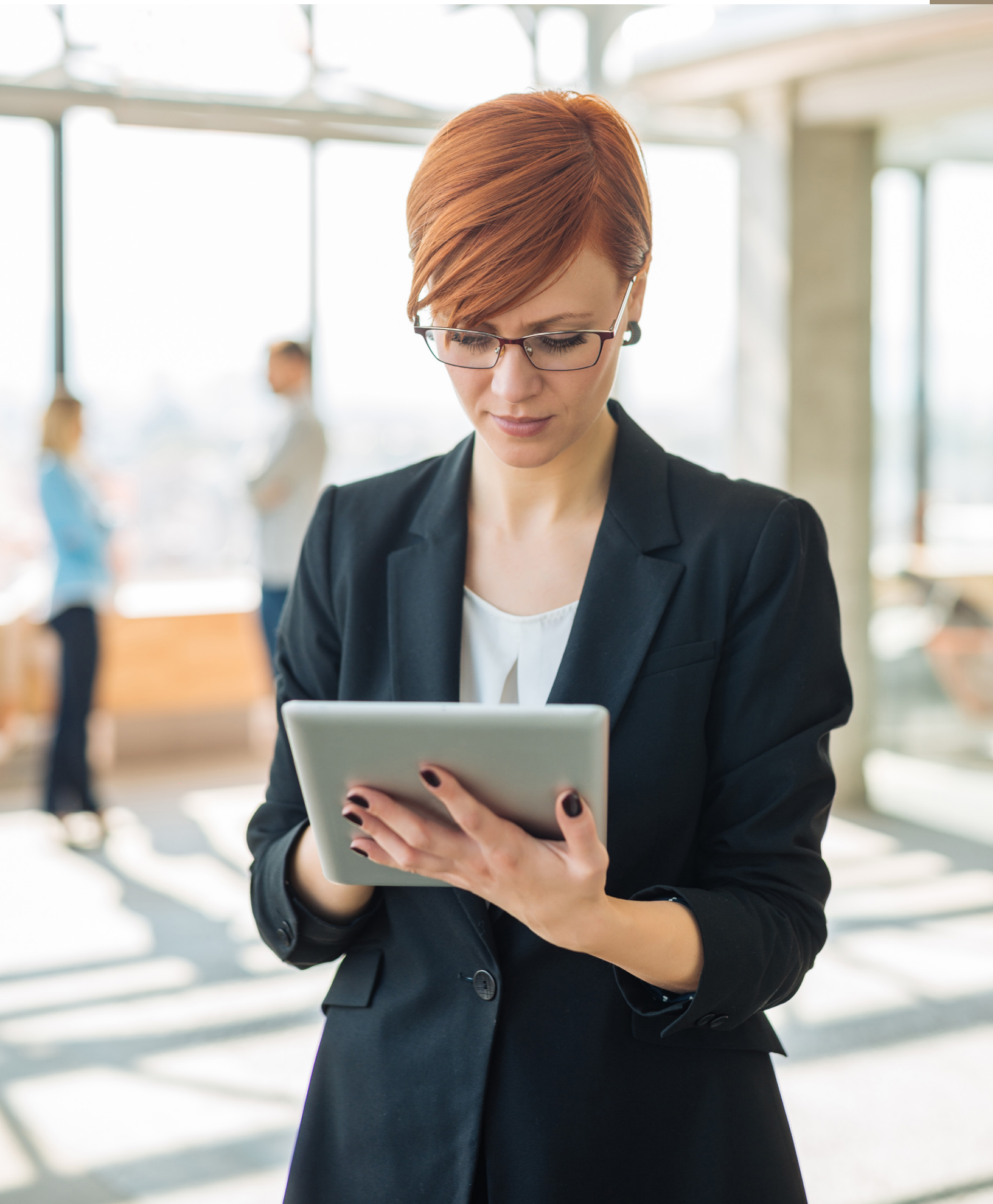
RESOURCES

CSOs are welcome to contact Karinda Washington with questions about resources or a potential partnership, as she has made her contact information available to the CSO Center.

Karinda.Washington@hq.dhs.gov

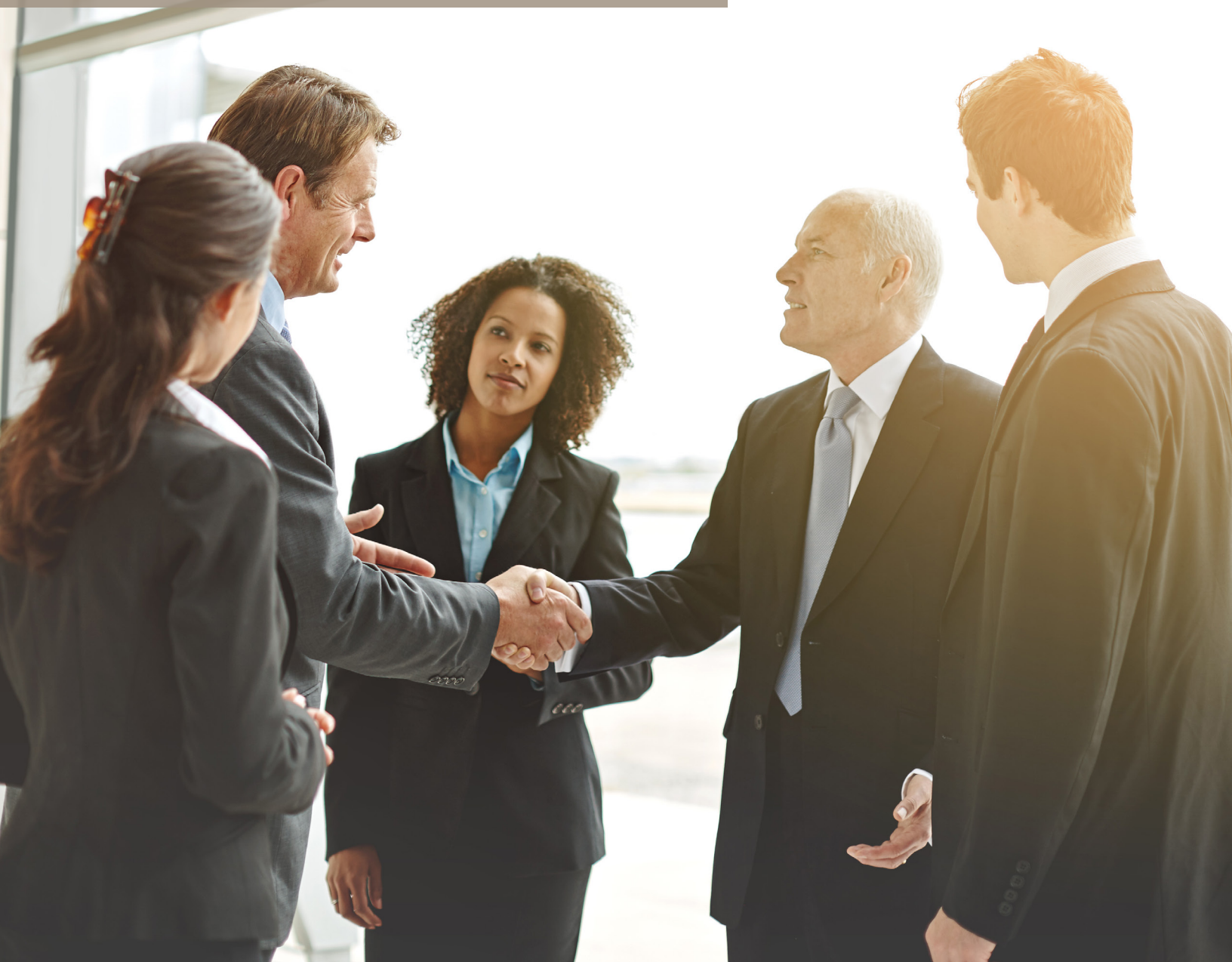
Some of the resources referenced and shared during the session are listed below.

- White House: *www.whitehouse.gov*
  - o Memorandum on Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships
- U.S. Department of Homeland Security: *www.dhs.gov*
  - o Exemplar program
  - o Loaned Executive Program
- Cybersecurity Infrastructure Security Agency (CISA): *www.cisa.gov*
  - o Chemical Facility Anti-Terrorism Standards (CFATS)
  - o Workplace Violence (An assessment tool will be available by the end of Q3 2021.)
  - o Unmanned Aircraft Systems
  - o Sector Coordinating Councils
  - o Regions
  - o Protective Security Advisors



Together We Stand

By Avril Eklund, CPP



"We need that constant flow of information—in both directions—for all of us to be successful."

Helen Keller said, "Alone we can do so little; together we can do so much." This one quote summarizes my experience as a chief security officer. Partnerships—internal and external—are truly the cornerstone of our success. During my experience building new security teams (which we all know is like building a plane that's already left the runway) I have often relied on partnerships to fill gaps in my resources.

Forging strong partnerships with agencies like OSAC and Infragard provided direct channels for the intelligence needed to be aware of current threats and those on the horizon. I have leveraged the Cybersecurity and Infrastructure Security Agency (CISA) Protective Service Advisor program to conduct security assessments of critical facilities and used their findings to bolster my risk assessments and support my resource requests.

I have relied heavily on the ASIS CSO Center to connect with other security leaders individually and as a group, and I have been thrilled to find so many fellow security practitioners ready and willing to share benchmarking data, standards and policies, best practices, and most importantly their lessons learned. These resources can serve as force multipliers for small teams like mine that have a global footprint to manage with limited resources and funding.

The true value in strategic partnerships is that they are mutually beneficial. We share information, knowledge, and perspective—helping each other grow and develop on an individual, company, or agency level. But the strength and success of these relationships add to the credibility and success of the security industry as a whole. No matter how successful your team is, the right partnership can take your team—and the security profession—to even greater heights.

Whether it's internal stakeholders like human resources that have a stake in the same game as you or external agencies like the U.S. Department of Homeland Security that play on the same field but a slightly different sport, we need to partner effectively and often.

What resonated most from the CSO Center Leadership Series session on external partnerships was right from Richard Mason's introduction: "The benefits of shared knowledge, experience, recommendations, and resources from trustworthy stakeholders such as DHS and CISA can help CSOs ensure they have an effective threat posture while keeping other organizations and government entities informed about emerging risks to the private sector."

We need that constant flow of information—in both directions—for all of us to be successful. Even together, we may not foresee and mitigate every risk or threat, but we'll definitely fail if we try to go it alone.

Avril Eklund, CPP
Head of Global Workplace Security and Safety, GitHub

Brivo Is Reinventing the Future of Security

The 2021 CSO Center Leadership Series was sponsored by Brivo.

Brivo is the global leader in mobile, cloud-based access control for commercial real estate, multifamily residential, and large distributed enterprises. Our comprehensive product ecosystem and open API provide businesses with powerful digital tools to increase security automation, elevate employee and tenant experience, and improve the safety of all people and assets in the built environment. Having created the category more than 20 years ago, our building access platform is now the digital foundation for the largest collection of customer facilities in the world, trusted by more than 25 million users occupying over 300 million square feet of secured space in 42 countries.

Our dedication to simply better security means providing the best technology and support to property owners, managers, and tenants as they look for more from buildings where they live, work, and play. Our comprehensive product suite includes access control, smart readers, touchless mobile credentials, visitor management, occupancy monitoring, health and safety features, and integrated video surveillance, smart locks, and intercoms. Valued for its simple installation, high-reliability backbone, and rich API partner network, Brivo also has the longest track record of cybersecurity audits and privacy protections in the industry.

Brivo is privately held and headquartered in Bethesda, Maryland.

WANT TO LEARN MORE?

www.brivo.com

Keeping Pace with Outside Threats Through Strong External Partnerships

Now that you've shored up internal relationships and partnerships with federal resources, shift your focus over to external partnerships, which can help improve awareness and responsiveness to external threats.

"Even just one conversation can open your mind and really provide a whole list of new possibilities for operational steps to improve a security posture," said Jack Donohue, board member for the Network Contagion Research Institute, during the third session of the 2021 CSO Center Leadership Series.

During this session, which is available on-demand to members of the CSO Center, industry thought leaders emphasized how connections to CSOs and subject matter experts outside of one's respective company—as well as in completely different industries—can widely improve a company's security posture. Whether it's about sharing intelligence, methods, expertise, or analytics, these relationships can improve threat awareness and responsiveness to crises, Donohue said.

Having allies in other environments, departments, or companies allows security leaders to remain focused on the mission while maintaining a radar for developing threats that lie beyond the horizon. Marene Allison, vice president and chief information security officer for Johnson & Johnson, knows that it is impossible for a single person to be omniscient; however, creating and maintaining relationships with peers and experts outside of an organization can mitigate and diminish potential blind spots as new perspectives help peel back the layers of risk.

"You'll be surprised," Allison said. "Sometimes a very minute communication with your peers will give you nuggets. And when you peel back the onion, you'll go, 'Crap, there's a dinosaur in there! Let's go fix it.' But you wouldn't know otherwise and it's only those relationships that are so very important that give you the intel that you need."

Donohue echoed the value in such conversations, noting that anecdotes and case studies from people beyond someone's bubble can be valuable. While he usually communicates with CISOs, he also tries to speak with and listen to insurance companies and other stakeholders. "The fact is that you don't have to speak to that many to get a very good idea of their perspective," Donohue said.

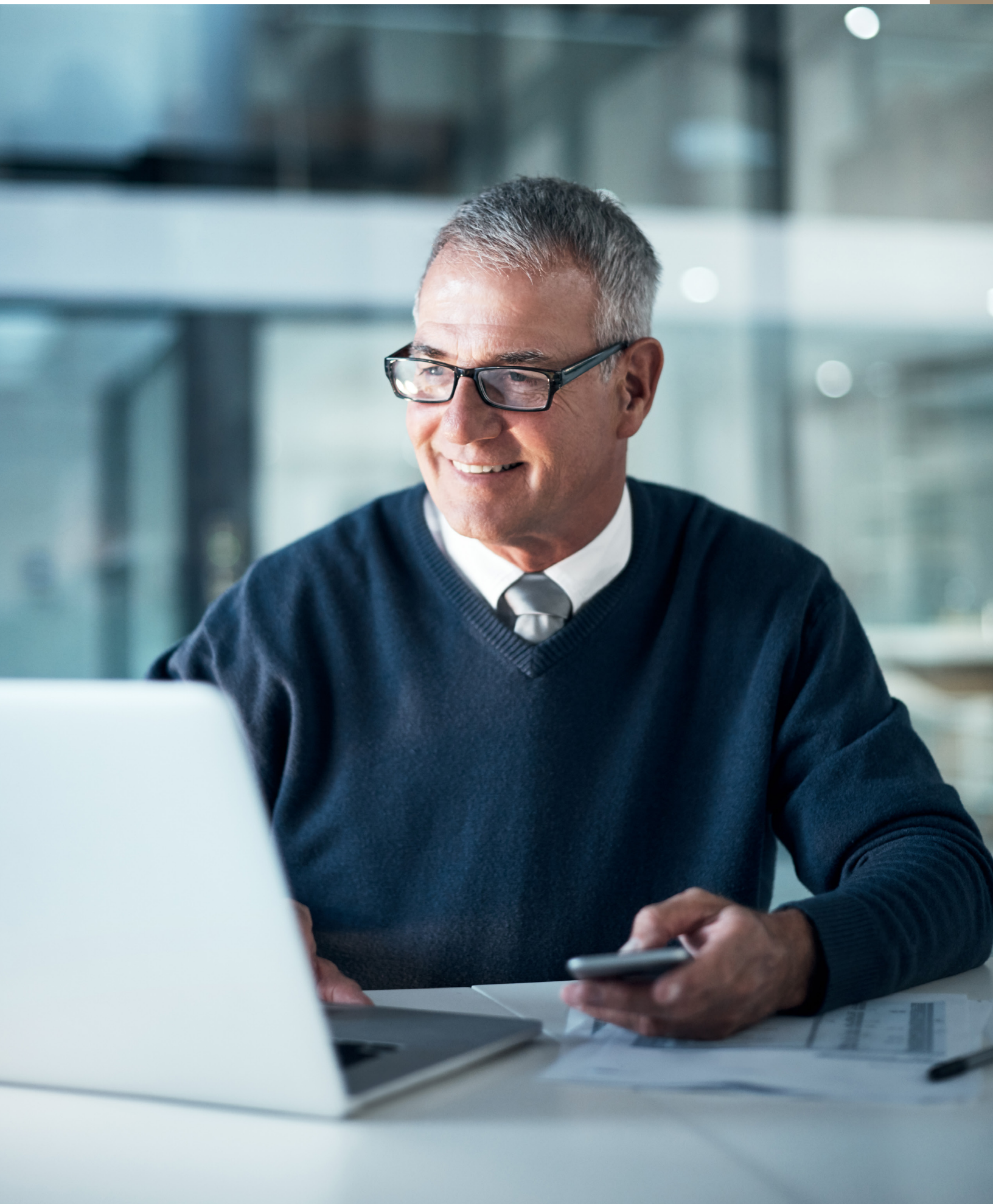
"Sometimes a very minute communication with your peers will give you nuggets. And when you peel back the onion, you'll go, 'Crap, there's a dinosaur in there! Let's go fix it.'"

David Forscey, managing director for Aspen Digital's Cybersecurity Group, noted that careful networking can benefit companies as they try to fortify against systemic risk. He encouraged CSOs to consider their respective supply chains when reaching out to peers in other companies and sectors. Specifically, ask others if there is a cloud-based software or a common dependency they share and evaluate how secure it may or may not be, he said.

Although this is already a common consideration for companies in the power sector and banking, he said this kind of risk assessment is lacking in several other industries. "I think it's a real problem," Forscey said.

Beyond engaging with other companies and external peers, Forscey also recommended connecting with think tanks. According to him, think tanks "are always looking for something like 30 CSOs to come to them" with a big problem to research and address. Think tanks want to be able to approach foundations and submit grant requests for research that has real-world applications and can improve business operations.

This in turn, allows CSOs to save their businesses money by outsourcing problem-solving endeavors, as well as saving the security department time and effort by farming out another burden.



Keeping Pace

By Lisa Oliveri, CPP, PCI

Perhaps now more than ever, partnerships matter.

As fellow CSO Center member Jordan Preisler, CPP, highlighted in his summary of the first session of the CSO Center Leadership Series (see page 6), strong partnerships help security professionals keep everyone safe. During the pandemic, many CSOs reported that their budgets have not increased—despite a growing list of threats and complications in an evolving operational environment.

As a security professional working in the non-governmental organization (NGO) sector, this resonates with me. NGOs typically have very limited staffing and security budgets (if they are fortunate to have a budget at all), so we rely on our partners, associations, and networks to obtain trustworthy information, ask relevant questions, and share diverse perspectives and lessons learned that can help us all anticipate, avoid, or respond to security issues more adeptly.

During the last session of this CSO Center Leadership Series, the panel discussed how security professionals stay updated on trends, policies, and best practices when there is so much information, misinformation, and disinformation to navigate despite limits on CSOs' time and competing priorities.

David Forscey from the Aspen Institute put it nicely when he recommended that people should speak with others outside of their "bubble" and pay attention to anecdotes that are shared—these can be good indicators of what others in the industry may be facing. Additionally, by convening leaders, scholars, and other diverse, nonpartisan thought leaders, innovative and practical ideas can provoke actions to address some of the world's most complex problems.

Jack Donohue explained how the Network Contagion Research Institute was founded as a not-for-profit organization that seeks to explore safe ways to audit, reveal challenges, devise solutions, and create transparency in partnerships with social media platforms, public safety organizations, and government agencies. Particularly with the increase of disinformation campaigns that impugn a particular product (such as a COVID-19 vaccine) and the companies that make said products, the ability for CSOs to access consistent and quantifiable information from politically neutral, multidisciplinary subject matter experts is invaluable.

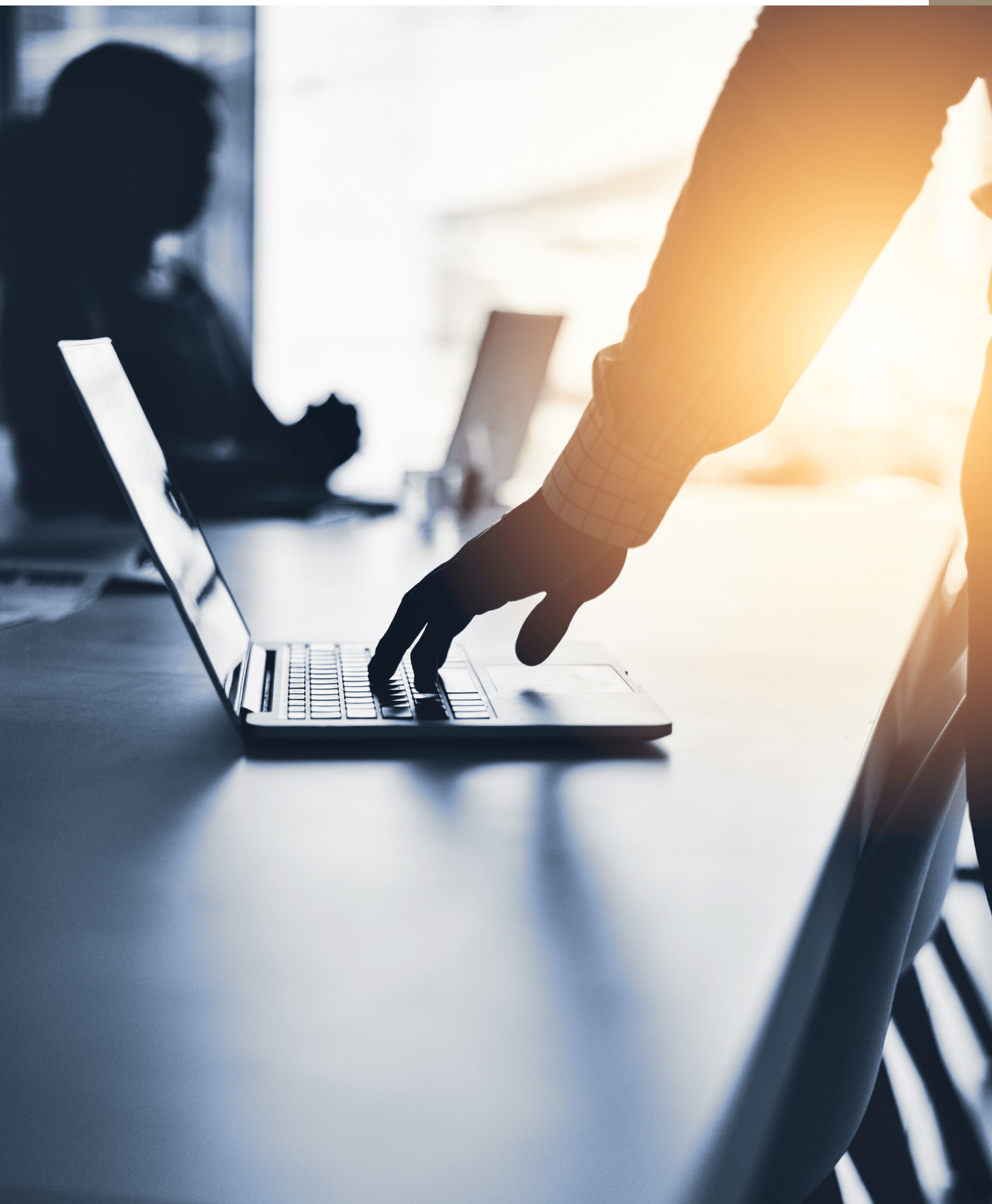
One of the most fascinating parts of the session was when Marene Allison shared her experience as a CISO working for Johnson & Johnson (J&J) when the decision was made to produce a COVID-19 vaccine. Marene explained how she navigated a drastically changing threat landscape and how critical it was for her to convene and consult with internal stakeholders and external contacts that she had developed throughout her career to help strategize communication on a global scale and facilitate working with various governments. Additionally, Marene highlighted how she and her team needed to approach disinformation related to J&J's vaccine and how they worked with their partners to learn from the past about how to manage information around a regulated product.

"One of the most fascinating parts of the session was when Marene Allison shared her experience as a CISO working for Johnson & Johnson (J&J) when the decision was made to produce a COVID-19 vaccine."

All panelists—as well as moderator Rich Mason—agreed about the value of engaging external stakeholders, partners, and think tanks to help CSOs stay on pace with outside threats or even get ahead of the curve.

I would encourage all CSO Center members to take the time to review these sessions as they are full of insight and practical steps that strengthen our networks and organizational response to crises.

Lisa Oliveri, CPP, PCI
Director of Global Safety and Security, EDC
CSO Center Host, 2021 Leadership Series



Continue the Conversation
Become a CSO Center Member

By joining the CSO Center, you'll be connected to leading chief security officers and their deputies from premier global organizations. Leverage the global network and exclusive resources the CSO Center provides members which include CSO Center members-only discussion groups, in-person and virtual networking events, benchmarking surveys, professional development, and much more. Align yourself with this well-respected community of security executives, raise your profile, and help position yourself for success.

The Value of CSO Center Membership, as Seen by Security Leaders

"The CSO Center provides me an invaluable resource to create meaningful relationships with other security executives. I frequently leverage these relationships to benchmark and glean advice on how they are facing the evolving challenges we face on a regular basis. Having access to this outstanding network as a resource for my executive toolbox regularly pays off and it allows me to be a better leader within my company."

Mark Landry, Senior Manager of Corporate Strategic Security, FedEx Freight, Inc.

"What I find most valuable, thus far, as a member of the CSO Center are the opportunities to hear from and interact with others in the security industry, especially in these times of 'distancing' and restrictions on in-person gatherings and travel. Hearing from others during the weekly CSO Huddles who are faced with similar decision points has been eye opening. I especially appreciate the ground rules established for these forums which have resulted in extreme candor and trust from all participants."

Frazier R. Thompson, IV, Global Security Operations Manager, International Paper

Huddle Up

CSO Center members can join regular Huddles—members-only, real-time discussion groups where you can share your challenges, successes, and questions with peers across the world. Huddle participants contribute to snap polls to benchmark their goals, viewpoints, and programs against other CSOs and move the conversation forward.

What department is your closest partner at your organization?

47% HR

0% Sales/Marketing

13% Travel

20% Facilities

20% Other

What are your biggest leadership challenges? *(Multiple responses allowed)*

17% Building a High-Performing Team

11% Identifying and Retaining Top Talent

50% Gaining Buy-In from the C-Suite

78% Demonstrating the ROI of Security Programs

11% Other

What leadership areas do you want to develop in yourself? *(Multiple responses allowed)*

42% Managing Difficult Conversations

17% Building a Personal Brand

25% Improving Emotional Intelligence and Its Application

83% Creating Strategic Initiatives

Learn more about the CSO Center for Leadership & Development at *csocenter.org*

Polls conducted in a CSO Center Huddle on 6 May 2021

To learn more about the ASIS International
CSO Center for Leadership and Development visit *csocenter.org*
or email CSO Center Center Director
Carla Lochiatto, IOM, CAE, at *csocenter@asisonline.org*

The CSO Center and ASIS International
thank our 2021 CSO Center Leadership Series Sponsors.

www.alertenterprise.com

www.brivo.com

Printed in the United States of America