SECURITY AT THE SPEED OF BUSINESS | SUMMER 2020

CSO
FROM IDG

CSO50 AWARDS 2020

CISO Rising

Breach concerns, data privacy regulations and new responsibilities for managing risk are **elevating the security leadership role.**

BY JAIKUMAR VIJAYAN

CSOonline.com

Congratulations to the 2020 Hall of Fame Inductees and Award Winners!

Tempered

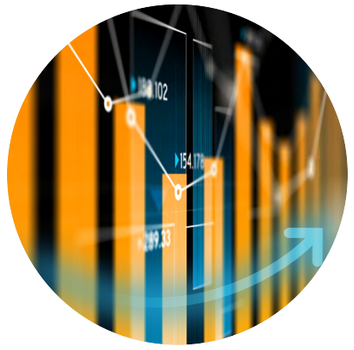
zero trust network solutions

protect, connect & be invisible

Most network environments connect first and secure later. Attacks are when, not if. You always need more firewalls, VPNs, VLANs, ACLs, SSH keys — but you're never really secure. We've found an infinitely better way to keep it all safe. Airwall makes connected things invisible and protects against network-based cyber attacks — at any scale. Join us and be invisible.

Learn more at www.tempered.io

Inside



[COVER STORY]

CISO Rising

11 Breach concerns, data privacy regulations and new responsibilities for managing risk are **elevating the security leadership role.** **BY JAIKUMAR VIJAYAN**

» 14 CSO50 award winners | 17 CSO's Hall of Fame

CSO
FROM IDG

EDITORIAL

EXECUTIVE EDITOR
Amy Bennett

ART DIRECTOR
April Montgomery

SENIOR EDITOR
Michael Nadeau

SENIOR WRITERS
Lucian Constantin, JM Porup, Dan Swinhoe

CSO EVENTS

SVP/PUBLISHER
Bob Bragdon

IDG COMMUNICATIONS, INC.

PRESIDENT
Kumaran Ramanathan

US PRESIDENT
Charles Lee

FOUNDER
Patrick J. McGovern (1937-2014)

FOLLOW US ON ...

Twitter | twitter.com/csoonline
Facebook | www.facebook.com/CSOonline
LinkedIn | www.linkedin.com/company/csoonline

CONTACT US
www.csoonline.com/about/contactus.html

BRIAN STAUFFER / MICROSTOCKHUB / SUPPACHOK_NUTHEP / WHYFRAMESTUDIO / GETTY IMAGES

5 tips *for* SCALING a security organization

How to prepare your SOC for mergers, new business innovation and a constantly changing and growing attack surface. **BY STACY COLLETT**

WITHIN THE SPAN of six months in 2017, CISO Eric Schlesinger watched his company Polaris Alpha balloon from 150 employees to 1,500 workers after three companies merged and three more were acquired. Schlesinger faced several daunting challenges, starting with being a prime target for cyberattacks because the company provides mission solutions to defense, intelligence and security customers, including the federal government.

"Part of that rapid IT integration comes with inherent risks.

MICROSTOCKHUB / SUPPACHOK NUTHEP / GETTY IMAGES

When it goes so fast, sometimes security wasn't necessarily keeping up with the pace of IT," says Schlesinger. How could he take six different companies, with six different networks and security teams, and create a single, dedicated security function that could partner and scale as the Polaris Alpha network was being scaled out?

> We realized early on that **tools were just part of the investment,** but not the ones driving our security.
>
> — **ERIC SCHLESINGER,** CISO, POLARIS ALPHA

Like most small to midsize firms, the acquired companies had relied on investments in tools for their cybersecurity. But integrating multiple tools from six companies wasn't going to work.

"We realized early on that tools were just part of the investment, but not the ones driving our security," Schlesinger says. "It needed to be based on the people, methodologies, workforce and processes that would allow us to scale from 500 to 1,500 people, and now to the 15,000 people we have today with Parsons acquiring us [in May 2019]."

You need a strategy

Schlesinger spent the first months wrapping his arms around the new organizations. Did he have the right people? What tools did those organizations have, and could they be repurposed?

Next, the company's integrated network security team adopted a standard U.S. Department of Defense (DoD)/Defense Information Systems Agency (DISA) model and applied it to the processes the company uses to defend its corporate network. "It creates a workforce structure that is clear on how that ecosystem has to work, and gives individuals a very clearly defined purpose and clearly defined procedures and workflows," he says.

While this megamerger represents an extreme case of scaling a security organization, most organizations still need the ability to scale security quickly, and not just due to M&A, new business innovation or new ways of interfacing with customers.

"We're in a very highly interconnected world with a vast, constantly changing and growing attack surface, which makes the scope and scale of what you're trying to do from a cyber standpoint ever-growing," says Emily Mossburg, principal, Cyber Risk Services Leadership Team, Deloitte & Touche.

CISOs and security consultants offer the following tips for organizing your security operation to scale.

1 Create a 'battle rhythm'

The adoption of the DoD model created a "battle rhythm" for Schlesinger's team and shifted its work from reactive to proactive. The joint security operations center (SOC) now has four quadrants—Protect, Detect, Respond and Sustain—with two full-time network defenders assigned to each one.

In the Protect quadrant, analysts handle risk assessments and vulnerability management.

Analysts on the Detect team look for indicators of compromise via alerts or by manually checking logs, looking for anything out of the ordinary.

"Within the first 15 minutes, if [Detect team analysts] believe it's something bigger that needs to be responded to, then they send it over to Respond team," Schlesinger says. The goal is to move the compromise up the security chain quickly so the Detect team can continue looking for additional problems. Respond analysts then take all necessary actions to stop the threat.

Finally, the engineers on the Sustain team support those three functions and ensure that all the tools and infrastructure are maintained and running.

2 Pare down tools

Kevin Richards was Accenture's global lead of security strategy when he helped reorganize and scale the security operations at a pharmaceutical company that acquired another pharmaceutical company, which had been spun off from a third pharma that still had ties with some of its services.

Complexity is the enemy of good security, says Richards, who is now executive vice president of strategic cyber readiness and response at Booz Allen Hamilton. "We all agreed that we can't have three SIEMs and four antiviruses and three different identity management products," but each organization had its own vendor preferences. "We wanted common, global, simple, so when we got down to two to three competing products, we just got in a room and had to pick."

The combined team eliminated almost 60 percent of the security tools it used—and freed up more than $1 million from multiple, redundant licenses, Richards says.

3 Repurpose people

As part of the acquisition, the parent pharma created a new hierarchy that would align better to the new business, which created a lot of new product areas and regions. It also gave Richards the opportunity to revamp the security team for the future—without losing any cybersecurity staff, except for one of the two CISOs.

"Everyone got assimilated in, but they weren't necessarily in the same role," Richards says. For example, "We didn't need two heads of SecOps, so one took on an architecture role and one took more of an operational role."

They also created some new roles, including a cyber innovation lead "who plays with new technologies and figures out how we could leverage those in our new construct," Richards says.

> We're in a very **highly interconnected** world with a **vast, constantly changing and growing attack surface.**
>
> — **EMILY MOSSBURG,** PRINCIPAL, CYBER RISK SERVICES LEADERSHIP TEAM, DELOITTE & TOUCHE

> **We don't want to be the 'business prevention department,' just saying no,** but educating people and supporting the needs of the business.
>
> — **ERIC SCHLESINGER,** CISO, POLARIS ALPHA

4 Consider outsourcing

The growing breadth and scope of cybersecurity can often outpace the capabilities of many organizations. Those companies should consider new channels for closing security gaps, including third-party security providers, Mossburg says.

"Just like many organizations decided they didn't necessarily want to maintain all of their networks and infrastructure, I think we're starting to see that same awakening around cyber," Mossburg says.

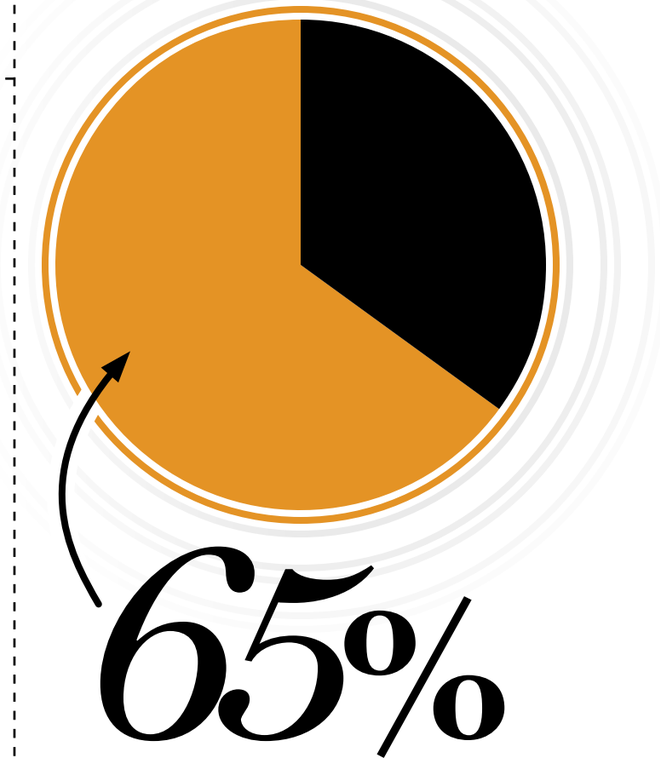
A 2019 Deloitte survey on the future of cyber shows that organizations are willing to rely on third parties to help address security gaps. Nearly two-thirds of CISOs (65%) outsourced 21 to 30 percent of their cyber operations.

5 Involve the entire organization

To detect and stop cyberattacks as they grow, the security organization needs the rest of the enterprise to help. "It cannot operate by itself," Mossburg says. "Educate, train and drive awareness and some level of accountability related to these risks outside the boundaries of the [security] organization."

All of these steps require a healthy relationship between security and the business, Schlesinger says. "Sometimes you have to isolate the team because they're dealing with sensitive information, but we are a customer service organization. We don't want to be the 'business prevention department,' just saying no, but educating people and supporting the needs of the business," Schlesinger says. "Tools come and go. Invest in people." ◆

STACY COLLETT *is a regular contributor to CSO.*



Is *your* **MSP** an **insider threat?**

Managed service providers and managed security service providers are attracting attention from attackers, who see them as a gateway to access their clients' networks. Here's how to minimize the risk.

BY LUCIAN CONSTANTIN

A GROWING NUMBER of managed service providers from around the world are being targeted and compromised by hackers. Such breaches can have a serious impact on their customers' business, as compromised MSPs can serve as launchpads into their clients' corporate networks. MSP compromises highlight why it's important for organizations to consider the risk they pose and be ready to block threats coming through trusted business partners.

In November 2019, a ransomware attack hit IT services firm

METAMORWORKS / GETTY IMAGES

Everis, a subsidiary of NTT and one of the largest MSPs in Spain. Based on internal communications leaked on Twitter, the company directed employees to shut down their computers and decided to cut the network links between its offices and its clients.

The attack directly impacted Everis's customers who relied on the company to manage various aspects of their IT infrastructure, and some of them started internal investigations into whether they were infected with ransomware themselves.

The malware program that hit Everis encrypted files using the .3v3r1s ransomware, and the ransom note warned the company against making the incident public. This suggests the MSP was not just a random victim in an indiscriminate attack, but that hackers chose it on purpose and customized the ransomware for the attack.

MSPs under attack

Attacks against MSPs and managed security service providers (MSSPs) ramped up in 2019 with a first wave of attacks in February by GandCrab ransomware pushers who exploited a known vulnerability in a plug-in that integrated ConnectWise with Kaseya, two platforms used by MSPs to manage systems.

In June, another string of attacks hit MSPs and deployed Sodinokibi ransomware through the Webroot Management Console, another tool popular with MSPs. The incident prompted Webroot, a cybersecurity company, to send a letter to customers and force the use of two-factor authentication.

In October, security firm Armor published a report listing 13 MSPs and cloud-based service providers that were hit by ransomware in 2019. In many cases, the incidents resulted in ransomware infections on customers' networks, affecting educational institutions, law firms, healthcare organizations, real estate brokers and more.

More than ransomware

While most of the MSP compromises so far have been leveraged to deploy ransomware, this is not the only type of threat that MSP customers are exposed to. State-sponsored cyberespionage groups could also use this technique to reach their targets and so could sophisticated cybercriminal groups like Carbanak or FIN7, whose modus operandi involves compromising networks, moving laterally to critical systems, learning internal workflows over an extended period of time and then stealing money or credit card data from organizations.

The 2013 network breach at Target, which resulted in over 40 million payment card details being compromised, started with hackers using credentials stolen from a heating, ventilation and air conditioning supplier that had access to the company's system through a portal. While that was not the first breach that resulted from a supply-chain compromise, it was the one that put this threat vector on the map.

In the years that followed, there were many incidents where hackers compromised organizations after breaching their partners or software suppliers. The NotPetya ransomware outbreak in 2017 started in Ukraine through a poisoned update for a popular tax accounting program called MeDoc.

Even when MSP attacks don't result in compromised systems or networks downstream, they can still cause downtime and impact customer business if the MSP is forced to temporarily shut down its normal operations.

Limiting the damage

According to Verizon's 2019 Data Breach Investigations Report, over

a third of breaches were caused by insiders. Attacks through trusted partners that have legitimate access into your infrastructure qualify as insider threats.

"Mitigating this threat is, of course, difficult as most supply chain threats are," says Ioan Constantin, cybersecurity expert at telecommunications provider Orange Romania, which also offers managed security operations center solutions for businesses. "Enterprises trust MSSPs and MSPs with their data and, at the same time, avoid operational overhead by sourcing most of the traditional mitigation techniques through this supply chain—think things like pentesting, monitoring and training.

"Learning from the [tactics, techniques and procedures] of some of the attacks against MSPs and MSSPs, there are some takeaways for enterprises to better protect against upstream compromises in their security supply chain," Constantin says. **Those takeaways include:**

- Secure remote access
- Enforce least privilege policies for access to resources
- Review and update service-level agreements with service providers
- Audit and improve policies regarding external access to your resources from consultants, vendors or service providers
- Regularly scan for and address vulnerabilities
- Communicate with and train your employees and other users

Constantin says the last item is probably the most important aspect of cyber threat mitigation. "Awareness is key, as always, to better security irrespective of the supply chain."

According to well-known hacker, author and penetration tester Jayson Street, the first thing organizations should do to prevent attackers abusing legitimate connections into their network is to isolate them. "I firmly believe that segmentation is the number one thing all companies should be doing when it comes to having anyone connecting into their internal network via the internet," says Street, who currently serves as vice president of InfoSec at SphereNY. "Each vendor, MSP, MSSP, etc., should be isolated once they're in the company network, and any communication to internal sources should be strictly controlled and monitored."

> **Awareness is key, as always,** to better security, irrespective of the supply chain.
>
> — IOAN CONSTANTIN, CYBERSECURITY EXPERT, ORANGE ROMANIA

Many of the typical recommendations for mitigating insider threats from employees or preventing lateral movement from threat actors apply to partners as well as MSPs. This includes making sure they are using unique credentials that are sufficiently strong and rotated frequently, enabling two-factor authentication, restricting access to the assets they need to manage or the information they need to do their job, monitoring their connections and movement inside the network and having systems in place that are capable of flagging unusual behavior and policy violations. ◆

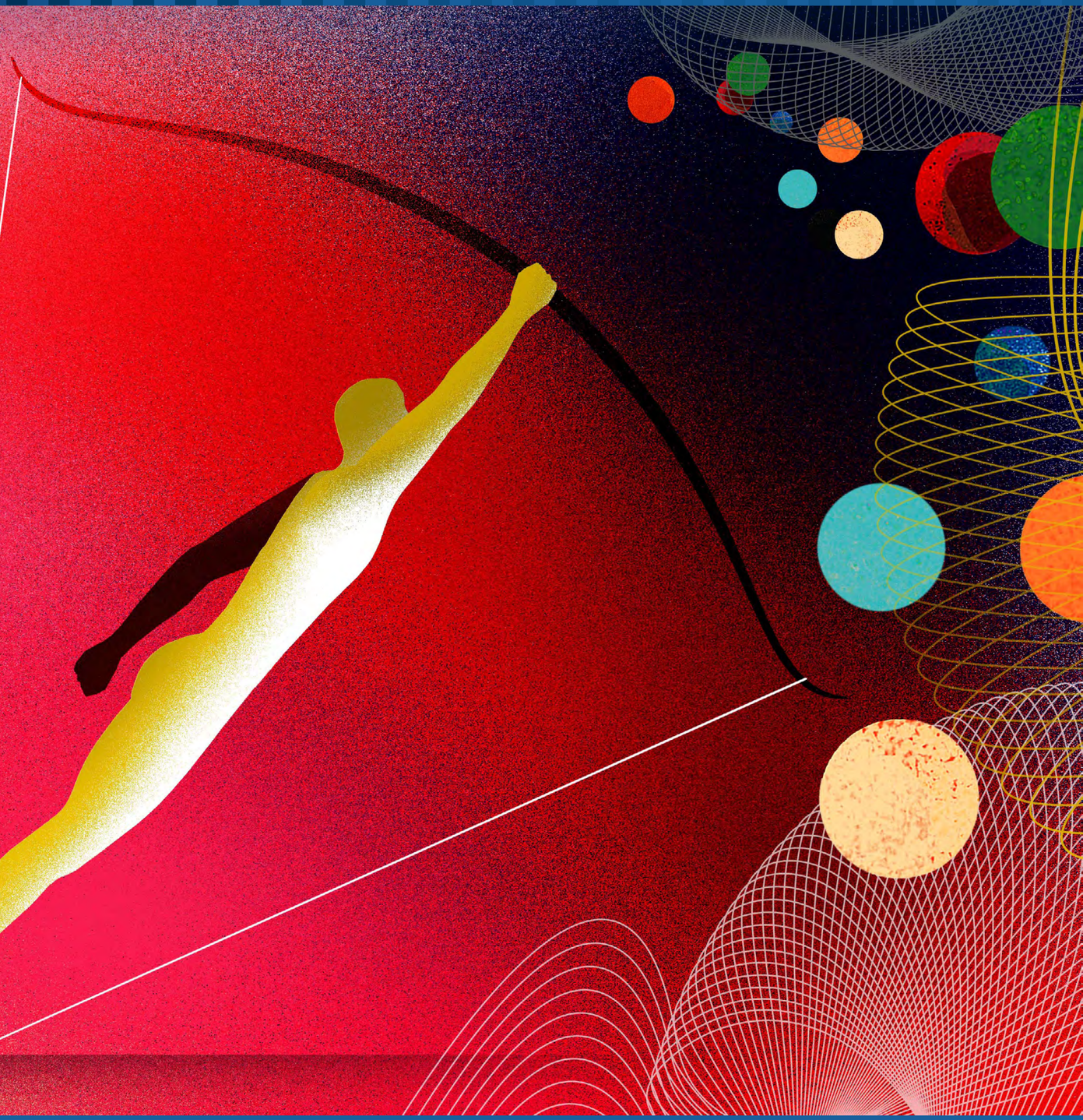
LUCIAN CONSTANTIN *is a senior writer with CSO.*

CSO50 AWARDS 2020

CISO Rising

Breach concerns, data privacy regulations and new responsibilities for managing risk are **elevating the security leadership role.**

BY JAIKUMAR VIJAYAN



BRIAN STAUFFER ILLUSTRATION

TIMOTHY YOUNGBLOOD'S responsibilities as CISO at McDonald's Corp. are broad, influential and a lot different from what most executives like him were tasked with a few years ago.

As the fast-food giant's chief security executive, Youngblood's role is as much about protecting the McDonald's brand globally as it is about facilitating and supporting business initiatives and goals. He reports to senior leadership, has board-level visibility and accountability and a voice in key business decisions at his company.

"Ten to 15 years ago, the CISO role was more of a unicorn role," Youngblood says. "Few companies had CISOs or even knew what a CISO was."

If security leadership existed, it typically reported into a vice president of infrastructure or similar role and was constricted to operational activity around things like access control, Youngblood says. These days, CISOs are not only asked to report to boards, but also to be on them. "Because of the headlines of the day, most boards want to speak with security leadership before they talk with CIOs."

CISOs at the center

The CISO role is evolving rapidly in part because of changing expectations around data privacy and protection.

Organizations that experience data breaches can incur huge costs and brand damage. Equifax's 2017 data breach cost the company $381 million in breach compensation. In addition, the U.S. Federal Trade Commission forced the company to commit to spending at least $1 billion on security improvements over the next five years.

Statutes like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are adding to the pressure by requiring organizations to implement new and far more granular controls over customer and consumer data. Data breaches resulting from vulnerabilities in the supply chain and among third parties are exposing companies to new liabilities and forcing them to respond.

> **Ten to 15 years ago, the CISO role was more of a unicorn role.** Few companies had CISOs or even knew what a CISO was.
>
> — TIMOTHY YOUNGBLOOD, CISO, MCDONALD'S CORP.

CISOs are in the middle of a lot of this change and are increasingly being vested with the responsibility for building privacy risk programs and managing third party risk and vendor controls. For many, these are new domains with which they have had little experience or little prior art to draw from, says Expel CISO Bruce Potter, who served as senior technical adviser to members of President Obama's Commission on Enhancing National Cybersecurity.

"It's a very different environment I think than what CISOs are used to," Potter says. "In a lot of

MCDONALD'S CORP.

ways, we are building a plane as we are going down the runaway."

New capabilities needed

Many organizations, for instance, are finding themselves having to implement new capabilities for data mapping and tracking data flows so they can comply with GDPR and CCPA requirements that allow consumers more control over their personal data. Few have the capability because until now they weren't required to know where individual data elements existed across the enterprise, Potter says.

Similarly, the data minimization requirements under these statutes run directly counter to the data mining and data analytics initiatives many organizations have implemented in recent years, Potter says. "You had CTOs and CIOs going out and gathering as much data as they could and putting it into data warehouses and making the business smarter," he adds. "Nobody really thought about the privacy ramifications because there was no hammer."

Third-party risk management and vendor control are other areas that are elevating the importance and visibility of the CISO. A good and growing chunk of a CISO's responsibilities these days is vetting vendor products and services for their organizations. Many recent breaches have resulted from attacks exploiting vulnerabilities in partner networks, and the security organization is increasingly being tasked with identifying and weeding out potential issues.

> In a lot of ways, we are **building a plane** as we are **going down the runaway.**
>
> — **BRUCE POTTER,** CISO, EXPEL

Youngblood, for instance, was very much in the middle of three recent technology acquisitions at McDonalds. "The CISO role has changed dramatically to be an arbiter of what companies it is OK to do business with," Potter says. Some of the security organizations that he interacts with these days spend as much as 40 percent of their time managing third-party risk. "It puts them in line with purchasing and other things with which they were not historically aligned," he says.

A burgeoning business role

In navigating such waters, CISOs are becoming more visible and influential across the enterprise. From being confined to a largely operational and technical role, security leaders for the first time are finding themselves being invited into a broader and more influential role at a growing number of companies.

Chief security executives are getting more opportunity to influence, partner and support change across the business, says Jason Haward-Grau, CISO of PAS Global and former chief security executive at Hungarian oil company MOL Group. "I think many CISOs across industries feel that expectation from their colleagues, peers and their own sense of personal drive."

The changing environment is requiring CISOs to think differently about their roles. Where previously it was good enough to have operational and technical capabilities, these days CISOs have to be able to demonstrate business acumen and show how security is creating value and opportunity.

[Continued on page 15 ...]

CSO50 WINNERS 2020

This year's class of CSO50 award winners raise the bar on security innovation. While delivering **business value** and demonstrating **thought leadership** are the metrics on which they are measured, the greater value is in the **peer-to-peer sharing** of ideas, approaches and best practices across a range of industries and company sizes.

- Aaron's Inc.
- Adobe
- ADP
- AFLAC
- Amity University, Uttar Pradesh
- Amrock
- Banco MUFG Brasil S.A.
- Bechtel Global Corporation
- BNY Mellon | Pershing
- Brigham Young University
- Centers for Medicare and Medicaid Services + Center for Consumer Information and Insurance Oversight
- City of Gainesville + Gainesville Regional Utilities
- City of Greensboro
- Coast Capital Savings
- CPS Energy
- Eaton County Central Dispatch
- Equifax
- Expedia Group
- Forever Living Products
- Frame.io
- Genpact
- HD Supply
- Health Care Service Corp.
- HMS
- Horizon Blue Cross
- Blue Shield of New Jersey
- HP
- ICON Clinical Research
- Kansas State University
- Legendary Entertainment
- Metropolitan Washington Airports Authority
- Microsoft
- NCR
- ND Information Technology Department
- O.F. Mossberg & Sons
- PayPal
- Penn Medicine
- Peraton
- PPD
- Prudential Financial
- Q2 Software
- Regeneron Pharmaceuticals
- SAP SE
- Saudi Aramco
- Skyworks Solutions
- St. Louis Cardinals
- Texas Dow Employee Credit Union
- TVS Motor Co.
- United Nations International Computing Centre
- Visa
- Webster Bank

[Continued from page 13 ...]

CISOs need to be able to work with business leaders, the C-suite and the board; understand business requirements; be an enabler of new initiatives; and be an arbitrator among different business functions—for example, information technology (IT) and operational technology (OT). "CISOs now need to understand not just security, risk and compliance, but also the nuances of the potential consequences and impacts on their business, their customers and now the supplier base," Haward-Grau says.

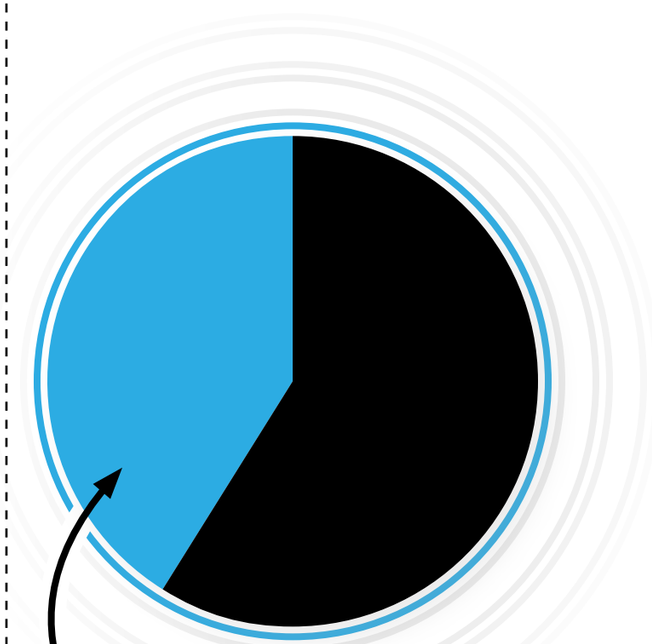
CISO to CIRO

The rapidly changing profile of the CISO has lent urgency to long-standing questions about reporting structures for the role. Traditionally, CISOs have reported up to the CIO, CTO or in some cases infrastructure leaders because the role has primarily been viewed as being operational and technical in nature.

> **CISOs now need to understand not just security, risk and compliance,** but also the nuances of the potential consequences and impacts on their business, their customers and now the supplier base.
>
> — **JASON HAWARD-GRAU,** CISO, PAS GLOBAL

Many have argued for some time that to really influence risk and drive change, the role of the CISO needs to be separated from IT because of the conflicting interests. While CIOs are typically measured against and rewarded for keeping systems up and installing new technology, CISOs are focused on protecting corporate assets and reducing the risk footprint.

In recent years, there has been a movement toward separating security governance from operations. Some CISOs have begun reporting to CEOs, CFOs, COOs and even general counsels. The overwhelming majority (41 percent, according to CIO.com's 2020 State of the CIO report) continues to report to CIOs because of the operational expectations for the role in areas like managing network security, Youngblood says. "If those operational duties are moved to other leadership, you will start to see



41%

of CISOs **continue to report to CIOs**

> If those **operational duties** are moved to other leadership, you will start to see more of a **governance and strategic focus** of CISOs.
>
> — **TIMOTHY YOUNGBLOOD,** CISO, MCDONALD'S CORP.

more of a governance and strategic focus of CISOs," he says.

Many of the security functions that CISOs are responsible for are being integrated into the technology that organizations purchase. Most network routers and edge devices, for instance, already have integrated security capabilities and can be managed by infrastructure and operational groups, Youngblood says. Identity management similarly is becoming more turnkey, highly operational and highly repeatable and something that an infrastructure team can handle. The more CISOs can divest themselves of these responsibilities, the better they can assume a true governance role, he says.

The natural progression is for a CISO to move to more of a chief information risk officer (CIRO) role that works closely with finance, strategy, operations and other groups. Expect to see policy management functions move to the CIRO role as well, Youngblood says. "We currently see this role being created more in the financial services industry, but it is coming more into other industries," he says. ◆

JAIKUMAR VIJAYAN *is a regular contributor to CSO.*

CSO HALL of FAME 2020

HONOREES

TIM CALLAHAN
SVP, Global CISO, Aflac

JIM ROUTH
Head of Enterprise Information Risk Management, MassMutual

GREGORY WOOD
SVP, Technology Risk Management & Security, The Walt Disney Company

KATHY ORNER
VP, Chief Risk Officer, CWT

JAMIL FARSHCHI
CISO, Equifax

CSO's Hall of Fame celebrates outstanding personal achievement in IT, honoring the technology executives who, along with significant accomplishments in the field of IT, have all demonstrated **substantial business impact** and **technology vision** within one or more organizations.

DAVE ESTLICK
CISO, Chipotle Mexican Grill

EMILY HEATH
Chief Trust & Security Officer, DocuSign

BRAD MAIORINO
CISO, Thomson Reuters

TIMOTHY YOUNGBLOOD
Corporate VP, CISO, McDonald's

MICHAEL ASSANTE*
SANS Institute, Center for Strategic and International Studies
** awarded posthumously*

SECURING THE PROMISE

Aflac is proud to recognize Tim Callahan, Aflac global chief security officer, for being inducted into the CSO Hall of Fame. Aflac's Global Security team is also being recognized with a CSO50 award for Keeping Our Ducks in a Row: Aflac's Cybersecurity Assurance Program.

We are committed to giving customers and partners the most secure experience possible. We promise to be here for our policyholders when they need us most by offering benefits that can **help with expenses health insurance doesn't cover.**

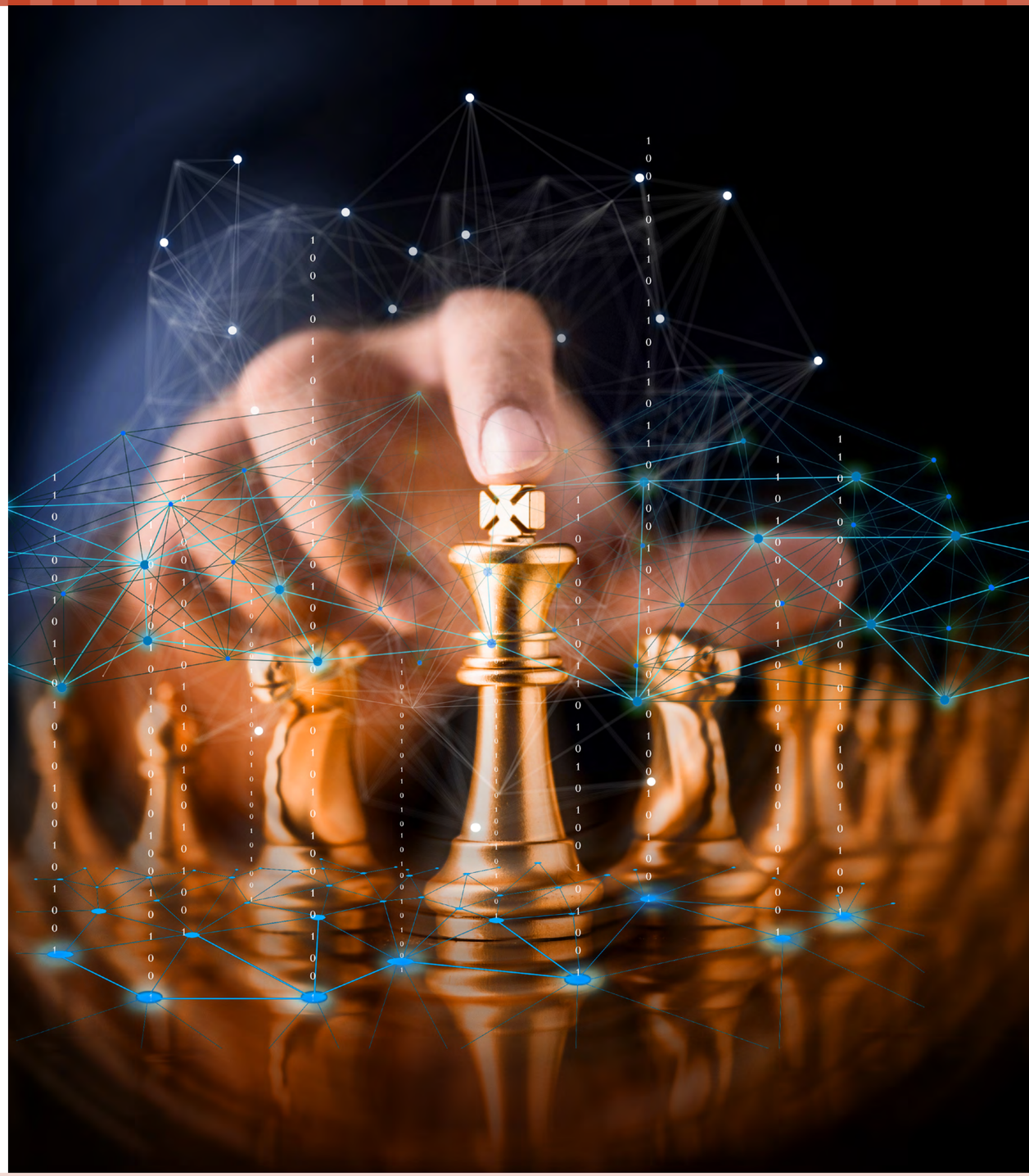
Get to know us at aflac.com.

Aflac®

Gamifying security training

How Penn Medicine's Penn Test challenge builds infosec skills and drives employee engagement. **BY JM PORUP**

FROM THE OUTSIDE, a career in cybersecurity seems pretty damn sexy—all those hoodies and green Matrix characters streaming past in the background wherever you go, popping boxen, zero-days and exploits, APTs and hackers, oh my. The reality on the inside, of course, can seem more like accounting. The sometimes boring drudgery of security operations can be a drum beat of digital paper shuffling, SIEM alerts to wade through, security audits to perform, GRC (governance, risk and compliance) to manage.



WHYFRAMESTUDIO / GETTY IMAGES

Keeping things a little spicy is key to employee acquisition and retention in a tight job market, and pushing your blue team to think more like an attacker pays dividends in an improved organizational security posture, according to Penn Medicine's Seth Fogie, director of information security, who launched and manages the organization's biweekly Penn Test security challenge for in-house security staff—a project that earned Penn Medicine a CSO50 award.

For 90 minutes every other week, the 35- to 40-person security department, including security engineering, security operations and information assurance, come together for a short capture-the-flag (CTF) competition. Fogie says he chooses real-world scenarios that could (and do) happen on their networks, so that employees are immediately empowered to go forth and seek out that vulnerability on their networks.

"A lot of people come into the security program out of college, or maybe from the infrastructure teams, but have never really been exposed to security skills, where you're looking for vulnerabilities, looking for how bad guys break in," Fogie tells CSO. "The whole concept of the Penn Test security challenge is a focus on teaching our staff how to break stuff and how bad guys do it, so we can build our systems better."

Even recent college grads with a degree in computer science often lack the hands-on skills required to secure real-world networks, he says, making realistic CTFs a great way to both train and motivate them. "Ninety-nine percent of people out of college have never dealt with network file shares (NFS)—how it works, how you configure it," he says. "The infrastructure team might know it exists, but half the time doesn't know how to secure it."

The emphasis on real-world scenarios that the infosec team is likely to discover on its own networks is key to the program's success, he says. Many CTFs rely on fun but unrealistic mind-bending puzzles that don't look anything like a real-world vulnerability that is likely to be exploited by an attacker. Keeping it real helps defenders think like attackers.

The goal isn't to turn every employee into a threat hunter, he says, but to give them perspective on their existing work, whether that's in security engineering or performing GRC audits. "Learning the finer details of how some of these attack scenarios are carried out ... helps build a more well-rounded security professional."

Unlike, say, sending his employees to take a SANS course or other training class, which is expensive in terms of both time and money

"The whole concept of the **Penn Test security challenge** is a focus on teaching our staff how to break stuff and how bad guys do it, so we can build our systems better.

— SETH FOGIE,
DIRECTOR OF INFORMATION SECURITY, PENN MEDICINE

PENN MEDICINE

and limited to classroom exercises, employees finish the Penn Test CTF and immediately return to their desk, where a massive network awaits to apply what they learn in each biweekly session.

Protecting medical applications

In addition to the many network security issues Penn Medicine shares with any organization, Fogie says the healthcare-specific concerns that worry him right now aren't medical devices, but rather patient data and how it's being used. "While medical device security is definitely a popular subject in the media, when it comes to healthcare organizations, there is a larger field of exploration that hasn't been touched yet, and that's medical applications."

There's a lot of innovation in the medical application space, he says, including traditional client-server applications, web apps and mobile apps, all used in varying ways to provide basic healthcare services, and often built and deployed without security front and center.

Securing those applications requires curious and motivated breakers with the right set of skills—the kinds of skills Fogie says the Penn Test security challenge offers.

"I think this is something that needs to be prioritized by managers," Fogie says. "Carving out time for this kind of activity … has had nothing but positive impact on those that are involved in these activities." ◆

JM PORUP *is a senior writer at CSO.*

Resources

SPONSORED BY: Tempered

DOWNLOAD HERE

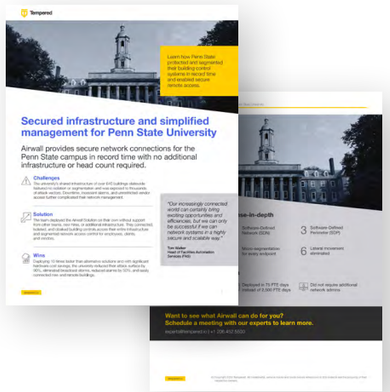
Airwall: A Revolution in Secure Networking

■ **Airwall makes 'things' on a network invisible and protects against cyber-attacks.** A comprehensive solution that is exceptionally effective at protecting critical physical infrastructure, while still allowing secure remote access.

DOWNLOAD HERE

Micro-segmentation Mistakes: How to Avoid Them

■ You don't need to compromise security or budget to protect critical infrastructure: **This guide is designed to help you avoid the most common pitfalls organizations make when implementing micro-segmentation.**



DOWNLOAD HERE

PSU: Secured Infrastructure, Simplified Management

■ Airwall provides secure network connections for Penn State University in record time with no additional infrastructure or head count. **Learn how they protected and segmented their building control systems and enabled secure remote access.**

DOWNLOAD HERE

Case Study: Great Lakes Water Authority

■ **Learn how Great Lakes Water Authority enabled a secure connection to remote sites and protected its critical infrastructure.** Airwall Solution provides remote access and simplified management for one of the largest control systems in the U.S.

DOWNLOAD HERE

Five-Star Casino Resort has a Sure Bet on a Secure Network

■ Airwall provides network security and simplified management for billion-dollar luxury entertainment complexes. **Learn how a five-star casino resort enabled secure remote access and protected its facilities with invisibility and micro-segmentation.**