CYBER READINESS HAS NEVER BEEN MORE CRITICAL

InfoSecurity PROFESSIONAL

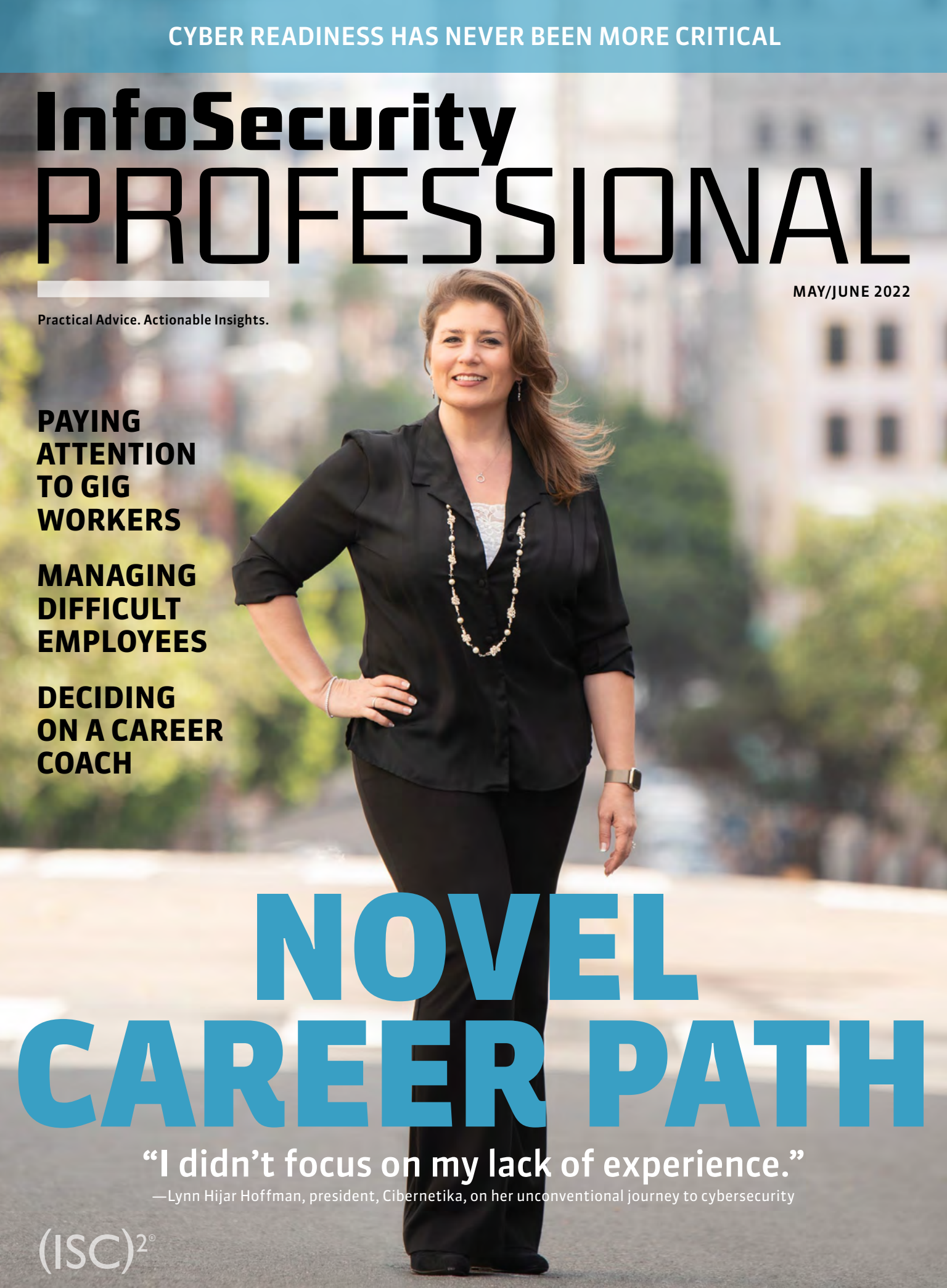
MAY/JUNE 2022

Practical Advice. Actionable Insights.

PAYING ATTENTION TO GIG WORKERS

MANAGING DIFFICULT EMPLOYEES

DECIDING ON A CAREER COACH



NOVEL CAREER PATH

"I didn't focus on my lack of experience."

—Lynn Hijar Hoffman, president, Cibernetika, on her unconventional journey to cybersecurity

(ISC)²

How Does Your Infrastructure Look To An Adversary?

Can you identify all of the internet-accessible devices on your network?

Or your supply chain's networks?

Do you know if those assets have critical vulnerabilities?

At LookingGlass, we help organizations reduce their cyber risk across their extended attack surface and empower them to find, focus, and defend against the threats that matter to their organization.

Learn more at www.lookingglasscyber.com

LOOKINGGLASS

CONTENTS ▪ MAY/JUNE 2022 ▪ VOLUME 15 - ISSUE 3

Tips for handling Negative Nancy, Egotistical Eddie, Crisis Charlie and other challenging employees.

PAGE 31

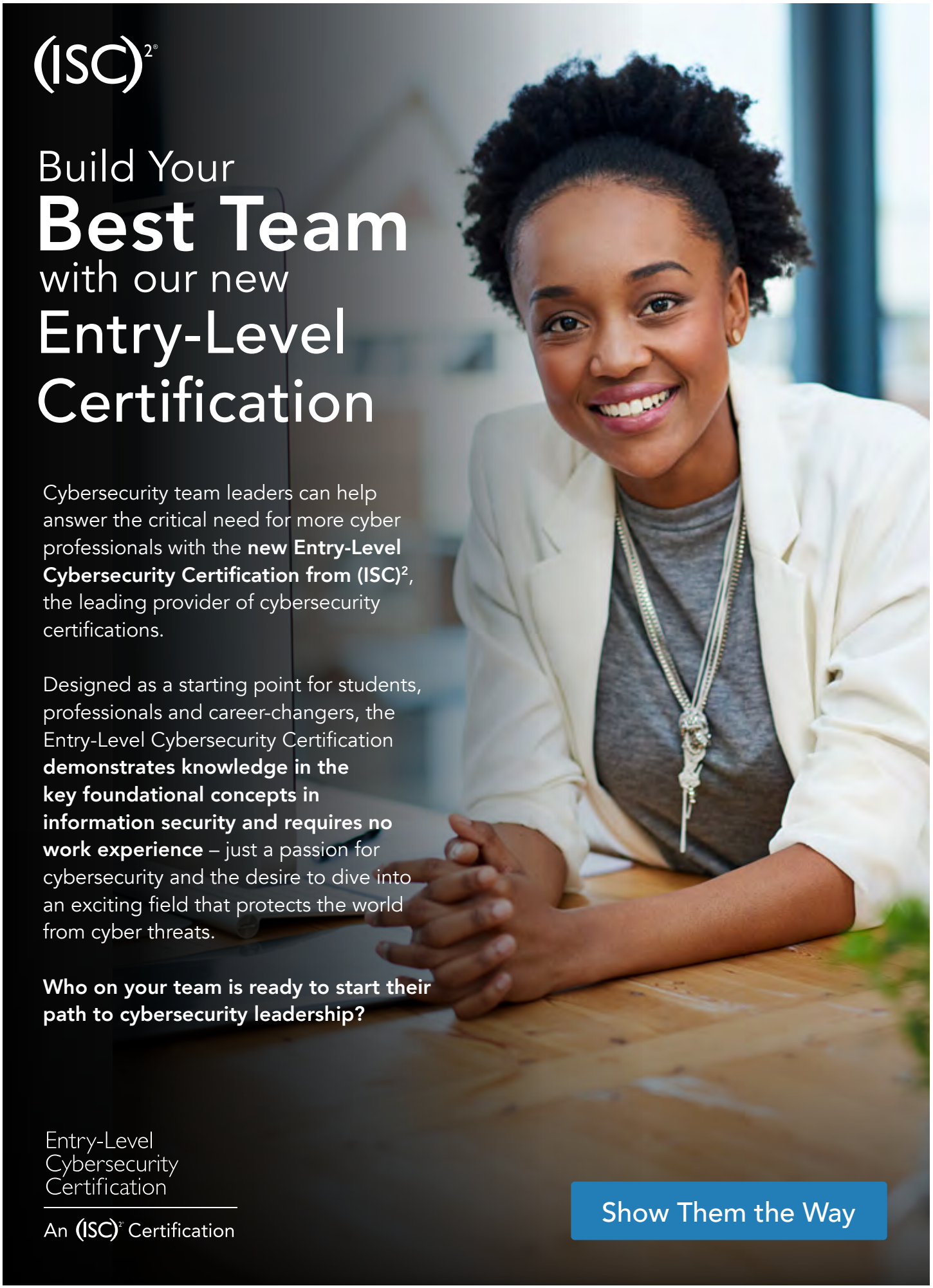
FEATURES

Cover photograph by Tim King

Illustration (above) by Jan Feindt

Page 27 illustration (right) by Peter and Maria Hoey

DEPARTMENTS


(ISC)²
Build Your
Best Team
with our new
Entry-Level
Certification
Cybersecurity team leaders can help answer the critical need for more cyber professionals with the **new Entry-Level Cybersecurity Certification from (ISC)²**, the leading provider of cybersecurity certifications.
Designed as a starting point for students, professionals and career-changers, the Entry-Level Cybersecurity Certification **demonstrates knowledge in the key foundational concepts in information security and requires no work experience** – just a passion for cybersecurity and the desire to dive into an exciting field that protects the world from cyber threats.
Who on your team is ready to start their path to cybersecurity leadership?
Entry-Level
Cybersecurity
Certification
An (ISC)² Certification
Show Them the Way

EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

What's Old is New Again (And That's a Good Thing)

IT'S NOT OFTEN you meet a CISO of a major corporation with her own IMDb page. Or learn how a humanitarian mission in Papua New Guinea still informs a security team leader's decision-making at an international conglomerate. Then there's the ISSO who once worked for the National Basketball Association—and Jennifer Lopez's production company.

These are some of the cybersecurity professionals highlighted in our cover story on successful practitioners with an unconventional career past. All have a natural curiosity about how things work and a desire to show those who believed in them that faith was not misplaced.

In writing the feature article, I thought back to when I first began chronicling the information security industry and most people weren't professionally trained. Few colleges offered courses, let alone actual degrees, in IT security, which meant that those who wanted to specialize in it were largely self-taught or mentored. Organizations like (ISC)² played a significant role in raising information security's profile—and professionalism. The CISSP remains the gold standard employers seek in candidates, who follow a code of ethics. Specialized (ISC)² certifications like the CCSP are gaining ground as the industry metamorphizes to meet today's evolving organizational needs and operating models.

(ISC)² continues to shape the industry by providing more opportunities for pursuers to demonstrate baseline skills with a new certification for entry-level professionals (see Field Notes for the latest on the pilot program). This should help alleviate one of the biggest barriers to entry and help convince hiring managers these job candidates are qualified despite their lack of experience.

I remember interviewing the great Dan Geer 20 (!) years ago about the changing profession. He worried that if there was only one path to becoming an information security professional, the industry itself would suffer from a lack of what he called a "hybrid vigor." It was the diversity of previous professions, backgrounds, experiences and educations that he considered a then-emerging industry's greatest strength.

Today we see a similar push for diversity and inclusion to improve the profession writ large. Sure, anytime we're asked to do things differently, we can expect some rough patches before everything smooths out. Those of us who push through initial resistance become more resilient. So do the companies and communities they serve. ●

Photograph by Louise Roup

Anne Saita lives and works in San Diego. She can be reached at asaita@isc2.org.

CONTRIBUTORS

This issue we showcase a chapter on managing difficult employees from a security management book written by veteran journalist **Mark Tarallo**, whose work most recently has appeared in Dark Reading, *Highbrow Magazine* and *HR Magazine*. You can learn more about what inspired Mark to write the book in a Q&A that follows his article.

Astrid Harders is again contributing a great piece involving today's workforces. This time she alerts us to a difficulty of managing still-remote employees working two or more jobs while on the clock for just one. Her piece is inspired by a lively Reddit thread in which someone created a script that brought his primary workday down to well under a half hour.

Both subjects for this issue's cover story, "The Path Less Taken," were photographed by **Tim King**. Based in San Diego and San Francisco, Tim's roster of clients includes the *Los Angeles Times*, Huffington Post, *The Wall Street Journal* and more. Beyond Tim's passion for photography, his interests include creating unique interior designs and world travel.

Illustrators **Peter Hoey** and **Maria Hoey** collaborated on this issue's illustration for "Hidden Gigs Among Us." In 2021, the siblings illustrated the article "Infection Control." Their other clients include *The New York Times*, *Rolling Stone* and *Time*.

Berlin, Germany-based illustrator **Jan Feindt** adds lots of attitude to author Mark Tarallo's profiles of those with unfavorable workplace behaviors in "Managing Difficult Employees." Jan's notable clients include *The New York Times*, *Rolling Stone* and *Time*.

What Are Your INDUSTRY PEERS Saying About CLOUD SECURITY?

To stay ahead of emerging trends, arm yourself with the 2022 Cloud Security Report. Sponsored by (ISC)², this comprehensive survey explores how organizations are responding to evolving threats. Download your copy of the report and learn:

- The latest cloud security trends and challenges
- How organizations are responding to security threats in the cloud
- What tools and best practices cybersecurity leaders are considering in their move to the cloud

Get the Report

"CCSP was just named "The Next Big Thing" by Certification Magazine!"

CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

InfoSecurity PROFESSIONAL
Practical Advice. Actionable Insights.

(ISC)² INSPIRING A SAFE AND SECURE CYBER WORLD

isc2.org community.isc2.org

READ. QUIZ. EARN.

Earn Two CPE Credits for Reading This Issue and Taking the Online Quiz

In order to earn the two CPE credits, you must pass the issue quiz. Please provide your name and (ISC)² member number so that we can award the two CPE credits to your account. This typically takes up to 15 business days to be added to your account.

https://www.isc2.org/InfoSecurity-Professional/Magazine-Archive/Quiz/May-June-2022

Learn about more opportunities to earn CPE credits at https://www.isc2.org/Membership/CPE-Opportunities

ADVERTISER INDEX

For information about advertising in this publication, please contact Vendor Sponsorship: Lisa Pettograsso, lpettograsso@isc2.org.

Cyber Readiness Has Never Been More Critical

BY ZACH TUDOR, CISSP

The past few months have been intense as the entire world watched the Russian invasion of Ukraine unfold. Regardless of where you live and work, no one is unaffected by the ramifications of a conflict of this magnitude, which has shaken up international trade markets and added additional pressure to financial systems and inflation, while the COVID-19 pandemic lingers.

Zach Tudor, CISSP, is the (ISC)² Board of Directors chairperson. He can be reached at ztudor@isc2.org.

As I mentioned in our March 21 Inside (ISC)² webcast, our hearts go out to all of the people in Ukraine and the surrounding region who have been impacted by this tragic conflict. Loss of life and the safety of those in harm's way are top of mind. To a lesser extent, when it comes to our members in the region, (ISC)² is making sure that AMF payments and CPE obligations that cannot be met will be paused and revisited with members at a later date when circumstances permit, in accordance with the (ISC)² hardship policy. These members should not have any concerns about their membership status with much bigger priorities in mind.

We continue to monitor for further escalation of cyber aggressions as well. As the physical bombardments continue, the U.S. Department of Homeland Security warned in January that anti-Western cybercriminal groups are expected to target U.S. critical infrastructure. U.S. President Biden also released a statement in late March urging private sector organizations that own and operate critical infrastructure to harden their cyber defenses and for businesses to take responsibility for protecting our shared cyber environment.

This is a unique time that calls for a new level of cyber preparedness. As CEO Clar Rosso wrote in her LinkedIn post on the topic back in early March, "Preparedness and vigilance is our best course forward, given the unpredictability of the current climate." To that end, (ISC)² published a cyber preparedness tips guide to remind organizations of the baseline best practices they should follow to shore up common vulnerabilities and maintain a state of readiness. I hope you'll read it and share it with your colleagues.

The (ISC)² team also wanted to hear directly from its members around the world what their top concerns were when it comes to the cyber fallout from the invasion of Ukraine. Among a host of thoughtful responses, critical infrastructure and supply chains polled as the top concern among (ISC)² members, according to responses from 269 practitioners representing 41 countries and 33 industries. You can read all about these results on the (ISC)² blog here.

The conversation also continued in the (ISC)² Think Tank webinar channel with an event called The Fallout: The Russia/Ukraine Conflict and Its Impact on Cybersecurity, where (ISC)² CISO Jon France, CISSP, was joined by two experienced members to discuss the cyber risks facing organizations in this current landscape and how to limit that risk.

As we navigate this evolving situation, (ISC)² depends on the expertise of our member-led advisory councils around the world to address emerging issues like the invasion of Ukraine. The organization works with these councils to up-level their insights so it can support its more than 168,000 members as they harden their defenses and quickly identify and respond if and when an attack does occur.

If you have ideas or experiences that you think would be useful to share with your fellow members and colleagues, please join in the Ukraine cyber threat discussions happening in the (ISC)² Community.

On behalf of the (ISC)² Board of Directors, thank you for all that you are doing to inspire a safe and secure cyber world. ●

(ISC)²

The Latest TRENDS and INSIGHTS in IT Security

How do your perceptions, priorities and security posture stack up against those of your peers? The ninth annual Cyberthreat Defense Report is now available. Get an in-depth look at how IT security professionals perceive – and plan to defend against – cyber threats.

THE RESEARCH REVEALS:

- A record 85% of organizations suffered from a successful cyberattack last year
- The vast majority (84%) of organizations are experiencing an IT security skills shortfall
- Nearly all respondents (99%) agreed that achieving a cybersecurity certification would help their careers; the top choices were cloud security, software security, and security administration

Use the 2022 findings to benchmark where your organization stands.

Get the Report

2022 Cyberthreat Defense Report - Sponsored by (ISC)²

FIELD NOTES

A ROUNDUP OF WHAT'S HAPPENING IN (ISC)² COMMUNITIES

The Time for Cybersecurity Attorneys is Now

BY SCOTT M. GIORDANO, ESQ., CISSP, CCSP

HOW MANY TIMES have you (or someone on your team) asked your organization's attorney any of the following questions:

- "Can we legally pay ransom to the hackers?"
- "If we're ISO 27k certified, are we compliant with [given regulation or contract]?"
- "What kind of liability are we exposed to if there's a breach?"
- "If our data is encrypted, is it still considered sensitive?"
- "If I remove someone's name from a record, doesn't that de-identify it?"
- "If we document this gap in security, can it be used against us?"
- "Do these controls qualify as 'reasonable' security?"

These are not easy questions to answer; they require a deep understanding of the context in which they are asked, and include jurisdictional, operational, and (in the case of multinational matters) political nuances. If fact, the list of legal questions related to the disciplines of cybersecurity and data privacy is nearly endless.

Moreover, their growth has been dramatic since the advent of cloud computing a decade ago. This phenomenon has resulted in a tremendous demand for attorneys with acumen in those two disciplines but with few candidates to fill them; this mirrors the larger problem of finding candidates for just about all types of open cybersecurity positions.

THERE MUST BE A BETTER WAY

In cybersecurity, a career path often starts with a basic skill in a sub-discipline (such as penetration testing or an IT position), adds related skills, and evolves into something deeper, such as security architect. This is often driven by technological advances (mobile devices, cloud, social media) and the current threat environment.

During this journey, professionals typically reach natural breakpoints where obtaining a technical certification is needed to advance their careers. These certifications are usually obtained on the person's own time and expense, through their employer, or some combination of the two.

There is no equivalent path for attorneys. I started a law practice in 2003 that focused on cybersecurity, privacy, and electronic discovery. I taught at a local law school while studying cybersecurity in graduate school. I immersed myself in the disciplines, learned from many great colleagues and instructors, and spent as much time studying for the CISSP as I did for the bar exam. I passed on the first try, and this certification has been enormously enriching, professionally and personally. This was a particularly arduous path, however; there must be a better way.

It is time the legal profession acknowledges that it has to adopt a new discipline that is a combination of cybersecurity and data privacy—*data protection*. Attorneys must understand both fields in order to faithfully serve their clients.

NEXT STEPS

It is time the legal profession acknowledges that it has to adopt a new discipline that is a combination of cybersecurity and data privacy—*data protection*. Attorneys must understand both fields in order to faithfully serve their clients.

I propose putting together a working group of stakeholders to identify the key subject areas important to such a practice. This would not be limited to attorneys; it would include multidisciplinary personnel globally. I hope, in particular, that attorneys who are considering sitting for the CISSP will participate. We will produce a report that we can present to (ISC)² at the 2022 Security Congress this October outlining our recommendations. Please connect with me on LinkedIn and let's get the ball rolling.

Pilot Program for New Entry-Level Cert Ends This Month

THE (ISC)² PILOT certification program for first-time cybersecurity career pursuers ends this month. Anyone currently or expecting to enroll in the new program's test run can take the exam by May 31.

The new certification is designed to demonstrate to hiring managers that those who pass the exam have a demonstrable understanding of basic cybersecurity concepts and have an aptitude to learn. It will reinforce confidence that they are equipped for entry-level cybersecurity roles despite the lack of three to five years of experience normally required by other qualifications. The goal is to ease some of the frustrations new college graduates or those transitioning from another field experience when competing in the labor market.

(ISC)² Security Congress 2022—Vegas *and* Virtual

(ISC)² SECURITY CONGRESS turns the spotlight on cutting-edge collaboration and learning for thousands of cybersecurity professionals from all over the world, October 10-12, 2022, at Caesars Palace Las Vegas and virtually.

Watch for upcoming announcements about star keynote speakers, hundreds of educational sessions, and Vegas-style networking events planned for in-person attendees and virtually.

Key highlights will include:

- Star keynotes
- 100+ educational sessions on the hottest cyber topics
- CPE credit opportunities
- Exclusive (ISC)² networking

Getty Images

- Career guidance and resources
- And much more

Register now for $200 off the All Access Pass with Early Bird Savings*.

**Early Bird Savings end September 16, 2022.*

Updates to CISSP CAT Exam Start June 1

BEGINNING JUNE 1, additional pretest items and time will be added to the CISSP exam for the Computerized Adaptive Testing (CAT) format.

The current CISSP CAT exam contains 25 pretest (unscored) items. The addition of 25 more items brings the total count to 50 pretest items. With these added items, the minimum and maximum number of items candidates will need to respond to during the exam will increase from 100-150 to 125-175. To allow for these additional items, the maximum exam administration time will increase from three to four hours.

Pretest items enable (ISC)² to continue expanding our item bank to strengthen the integrity and security of the CISSP for all those who earn the certification. The additional 25 pretest items will be evaluated for inclusion as operational (scored) items in future exams. The pretest items will be indistinguishable from operational (scored) items and should be considered carefully to select the best possible answer. Responses to pretest items will not impact scores or the pass/fail result of the examination.

There are no other changes to the content, including domains and domain weights, for the CISSP exam. All policies regarding exam rescheduling remain in effect.

For more information, visit www.isc2.org/notice/CISSP-Exam-Length or contact our Exam Administration team at examadministration@isc2.org.

Russia-Ukraine War and Its Impact on Cybersecurity

THE PAST SEVERAL MONTHS have had cybersecurity professionals re-evaluating their cyberattack readiness, especially when it comes to protecting industrial control systems and critical infrastructure.

In March, weeks into Russia's war in Ukraine, (ISC)² polled more than 260 (ISC)²-certified cybersecurity professionals from 41 countries, including Ukraine and the Russian Federation. They represent 33 different industries, with the most in financial services, followed by IT services and healthcare. Not surprisingly, cybersecurity professionals all over the world are concerned about a rash of new threats emerging from the conflict, including ransomware, data-wiping malware, Zero Days and DDoS attacks.

Among other insights, as outlined in a March blog post:

- The top concern across the board was the immediate threat to critical infrastructure and essential supply chains that would put lives at risk anywhere in the world. "Critical infrastructure may be attacked by DDoS, affecting the availability of systems and causing inconvenience to citizens in terms of water, electricity and travel," said one respondent from China.
- In addition to being concerned about how attacks could shut down critical functions of society, respondents were also concerned about the level of preparedness that exists to combat such attacks. "I am worried that few companies have a sufficient incident response system," said one IT services manager in Japan.
- While critical infrastructure and supply chains are of primary concern, cybersecurity professionals also worry about threats to businesses and how their customers could be impacted financially.
- "Cyber warfare is now a reality and is equally important along with traditional warfare. Hence, having both attack and defense strategies in line with traditional warfare to maintain one's national sovereignty is a must," said a respondent from India.
- While a member from Ghana said, "My biggest concern is the potential for cyberattacks to become a 'legitimate' weapon in modern day warfare."
- Some respondents foresaw the possibility of non-related attacks taking advantage of the worldwide attention on Ukraine to sneak by undetected. One Japanese respondent said their top concern is "phishing scams disguised as donation requests." While an MSSP IT services manager in the Netherlands remarked, "If ever Zero Days and managing/protecting against abusing them was important, this period will probably prove we need to up our game there."

What's clear is that cyber professionals everywhere are concerned about the ramifications of the invasion. Even as cyber threats are weighed, some respondents sent a reminder that it's important not to lose sight of the fact that human lives are at stake in Ukraine.

One Taiwanese cyber professional in the education field indicated the top concern right now is for "human rights."

Meanwhile, a respondent from Ukraine summed up their feelings on cyber threats by simply saying, "Right now all our services are under physical attack, so cyber-attacks in comparison with physical [destruction] of our infrastructure and people [takes] second place." This sentiment was also echoed by a Russian Federation professional, who when asked the same question about their top concern summed it up by saying, "People's lives."

Read the (ISC)² Cyber Preparedness Guide today by visiting "Steeling For Disruptive Cybersecurity Attacks on Business and Infrastructure." ●

Getty Images

New SECURE Summits—Virtual and In-Person Opportunities

THE ONE-DAY, IN-PERSON (ISC)² SECURE Summit series continues with SECURE Singapore on July 14, alongside three additional events held virtually throughout the second half of 2022.

The first in the series—an in-person SECURE London—took place in April. These events tailor content to host regions and this year cover topics including government cybersecurity, Zero Trust, ransomware, cloud security and quantum computing. The SECURE Summits are open to both (ISC)² members and non-members in every stage of their careers.

The 2022 SECURE Events will take place on the following dates:

- June 15 – SECURE North America
- July 14 – SECURE Singapore
- November 10 – SECURE Asia-Pacific
- December 8 – SECURE UK & Europe
- December 9 – SECURE Washington, D.C.

For more information on SECURE Summit series and to register, please visit https://www.isc2.org/Events. ●

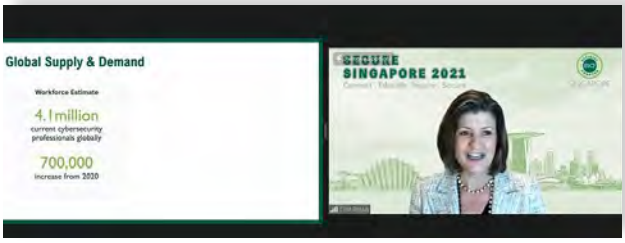
CHAPTER SPOTLIGHT

(ISC)² Singapore Chapter 'Rises Above' to Draw Attendees to Virtual Event

WITH A THEME OF "Rising Above and Staying Resilient Against Future Threats," the Singapore (ISC)² Chapter drew more than 180 attendees to a 6.5-hour virtual event. Among the speakers were David Koh, chief executive of the Cyber Security Agency (CSA) of Singapore, and (ISC)² CEO Clar Rosso.

Event highlights included:

- The Singapore Cybersecurity Strategy address was given by Yik Jia Wei, director - strategy & planning from CSA.
- Sessions covered artificial intelligence, cyber insurance, regulatory trends, supply chain risk management, ransomware and cloud security.
- A panel moderated by Melvin Leong and featuring Victor Yeo, S.C. Leung, Neha Malhotra and Andre Shori discussed risks related to emerging technologies such as AI, blockchain, IoT, operational technology and 5G.
- Conference moderators Paolo Miranda and Anthony Lim kept enthusiasm levels high all day.
- A fun Kahoot quiz capped off the program.



(ISC)² SECURE Singapore is scheduled for July 14 at the Shangri-La Singapore hotel. Learn more about the event, including how to register, at https://www.isc2.org/Events/SECURE-Singapore.

Interested in starting an (ISC)² Chapter in your local community? Visit https://www.isc2.org/chapters/start-chapter for requirements, process, and all other relevant information.

(ISC)²

SECURITY CONGRESS

SAVE $200 with Early Bird Through Sept. 16, 2022

OCT 10 -12 LAS VEGAS CAESARS PALACE

(ISC)² Security Congress turns the spotlight on cutting-edge collaboration and learning. Join thousands of cybersecurity professionals from all over the world, October 10-12, 2022, at Caesars Palace Las Vegas and virtually.

It's Going to Be a Game-Changer!

- Star Keynotes
- 100+ Sessions on the Hottest Topics
- CPE Credit Opportunities
- Exclusive (ISC)² Networking
- Career Guidance and Resources
- Industry-leading Exhibitors and Sponsors

Register Now

Congress.isc2.org | #ISC2Congress

Who's to Blame if MFA Fails to Work?

BY IAN RIFKIN, CISSP

While multi-factor authentication (MFA) use has increased significantly during the pandemic, its adoption could still be higher, given its benefits. So why aren't more users adopting this stronger method of authentication? And who is really to blame when they don't?

Ian Rifkin, CISSP, is a strategic technology leader with expertise in web and cloud technologies. He currently is director of data and systems integration at Brandeis University and has a master's degree in information technology management.

MFA requires multiple factors as part of the authentication process. Authentication without MFA (e.g., password-based authentication) only uses one factor, while MFA uses two or more: something you know (e.g., password), something you have (e.g., a phone or security key), and/or something you are (e.g., biometrics). Security professionals agree that MFA significantly increases account security. Failure to adopt MFA makes it easier for hackers to compromise accounts.

MFA, much like password security policies, is dependent on the specific site/service implementation. Organizations do not implement MFA in the same manner everywhere; instead, it's up to users to figure it out.

As a technology, MFA has been around for many years. In fact, nearly 20 years ago when I was playing the online multiplayer role-playing game Final Fantasy XI, I had a hardware token to use as my second factor. The initial problem wasn't adoption from users; the problem then was adoption by organizations. That was the first hurdle of MFA adoption. People couldn't use it if the sites/applications they were logging into didn't offer it.

Fortunately, in the years since, MFA options have become more common. Yet, sadly, MFA still is not a given. According to a Gartner analysis: "By 2023, 60% of large and global enterprises, and 80% of MSEs, will deploy MFA capabilities consolidated with access management or similar tools, which is an increase from 10% and 25%, respectively, today."

GETTING PEOPLE TO ENABLE MFA

When the relationship isn't employer/employee or school/student and is instead business/customer, we are quick to blame the user/customer for low MFA adoption rates.

We don't hear about poor adoption rates with setting passwords. That's because businesses require their users to set passwords (and, increasingly, complex ones more difficult to crack).

Some people shift the blame from users to security professionals, sending mixed messages about the benefits of specific MFA implementation options, particularly the effectiveness of SMS texts that high-profile bloggers and sites like CNET have discouraged in articles on the subject.

Are they wrong? No. SMS-based MFA is not as safe as an authentication app or a physical security key due to inherent risks like SIM swapping and a general understanding that text messaging wasn't built to be a robust authentication platform. Nonetheless, some feel that presenting SMS MFA as unsafe might be detrimental to MFA adoption in general and consequently are blaming the security professionals attempting to teach best practices.

'REQUIRE THE RIGHT THING'

It's not a question of telling users to do the right thing—it's up to us to tell businesses

to require the right thing.

If a provider doesn't offer MFA, there's nothing the user can do. If it offers MFA but doesn't promote it during sign-up, is it the user's responsibility to navigate deep into their account settings to see if this service has implemented MFA or updated its options? If the provider offers only MFA using SMS, should the user decline, based on criticism of this approach? Even if the user signs up for MFA with a non-SMS option, the provider may still give an SMS fallback option that the user can't opt out of.

A better approach would be for the security community to pressure organizations, not end users, to require the right thing. Organizations should implement, not just offer, appropriate MFA options. That means either requiring MFA or least prompting users to set up MFA during and periodically after sign-up.

Microsoft's David Weston once tweeted: "Optional security nearly always means low volume." If we want the security MFA provides, it cannot be a hidden feature that you need to know the secret to unlock. MFA needs to be part of regular processes, whether a user is an employee, customer or contractor. It is our responsibility as security professionals to make this happen. ●

For a longer version of this article, visit "Multi-Factor Authentication: Who's to Blame if It Doesn't Work as Intended?"

(ISC)²

SECURE SUMMITS

Make plans now to attend this exciting new event series in 2022.

Register today and join your peers for a collaborative deep dive into the most current cybersecurity issues impacting organizations in your local and regional markets. You'll come back inspired with new ideas and solutions from a diversity of perspectives.

Each SECURE Summit features:

- Expert Presentations
- Exclusive Networking
- CPE Credits
- Exhibit Hall

IN-PERSON SUMMITS:

- SECURE Singapore
  Thursday, July 14
  Shangri-La Singapore
- SECURE Washington, D.C.
  Wednesday, December 9
  Renaissance Washington, DC Downtown Hotel

LIVE VIRTUAL SUMMITS:

- SECURE North America
  Wednesday, June 15
- SECURE Asia-Pacific
  Thursday, November 10
- SECURE UK & Europe
  Thursday, December 8

LEARN MORE AND REGISTER AT
www.isc2.org/events

INTERESTED IN SPONSORING? EMAIL US FOR MORE INFORMATION.

Upskilling: The Not-So-Secret Ingredient to Staff Retention

BY DEBORAH JOHNSON

The COVID-19 pandemic, ensuing "Great Resignation" and perennial shortage of talent has technology and cybersecurity managers scrambling to keep valuable employees. One way is through upskilling.

The potential reward of upskilling is reflected in a recent survey by PwC which says 93% of the responding CEOs who had implemented advanced upskilling programs reported increased productivity, an improvement in talent acquisition and retention, and a more resilient workforce.

"Reskilling people or moving people into new roles is always one of the most cost-effective things to do," Oakland-based HR analyst Josh Bersin recently told me. He lays out the savings on his website: "The cost of recruiting a midcareer software engineer can be $30,000 or more, including recruitment fees, advertising and recruiting technology. By contrast, the cost to train and reskill an internal employee may be $20,000 or less."

Upskilling has another benefit, Bersin adds. "It improves retention because some of those people [getting new skills] might say, 'Well, this is something I've always wanted to do and now I don't have to leave this company.'"

There are many avenues to upskill, from online programs to on-site seminars, even mentoring.

The personal relationship created by mentoring can be the key to successful upskilling, maintains Amanda Schnieders, senior marketing manager at Chronus, a mentoring software platform. "People talking to other people get the chance to actually learn [by] building rapport and support within an organization," she told me. "That kind of personal connection to the subject matter helps it stick in their mind long after the conversation. It may stick around longer than a training session they attended or a webinar they watched."

Mackenzie Hoy, a customer success manager at Chronus, says company management must first develop a mentorship plan. "Making the best mentor/mentee matches requires well-defined programmatic goals set by the organization. These goals are typically the answer to questions like 'What changes do we want to see in our organization?'

"Once you have these answers," she continues, "programs can then take it down to the individual level to see what would produce a great pairing, and match individuals based on shared areas of learning (on the mentee side) and areas of expertise (on the mentor side)."

A successful pairing requires managers know their team members, asserts Bersin, the HR analyst. "Every CEO or every head of tech should think: 'Who do we have who is a really high potential person, really smart, who could move into this role?' And then, "Who's the counterpart person who could mentor them?'"

While corporate success may be the goal, position upskilling as career-building, warns Hoy. "Jack and Jane sitting at their desks are thinking, 'Well, the company is benefiting, but what do I get out of it?' This comes with communicating the benefits to those individuals." That can include potential promotions, pay raises and a sense of "taking care of our own," she adds. ●

Photograph by Louise Roup

Deborah Johnson lives and works in San Diego. She can be reached at djohnson@twirlingtigermedia.com.

Map your way to the cloud with Official (ISC)² Training

As organizations rapidly shift to a cloud-based paradigm, demand for professionals skilled in secure cloud migration and operations has never been higher. For a competitive advantage, IT and cybersecurity professionals like you are earning the (ISC)² Certified Cloud Security Professional (CCSP), the highest standard for cloud security expertise.

Choose your training path

We'll help guide you to certification with three flexible (ISC)² Official Training options.

Self-Paced
Online learning at your own pace

Online Instructor-Led
Virtual learning with a live instructor

Classroom-Based
Focused in-person learning

Start on Your Path

THE PATH LESS TAKEN

BY ANNE SAITA

"I don't want clones of myself working on my team; I want to see different backgrounds that will look at a problem through different lenses."

—Jessica Sica, CISSP, CISO, Petco

(ISC)² members share how their unconventional resumes shaped the successful cybersecurity professionals they are now

WHEN JESSICA SICA stood to turn in her CISSP exam, heads turned.

"I was the first one up, and everyone kind of stared at me," she recalled almost 15 years later. "I've just always been a good test-taker, I guess. But, yeah, I got some funny looks."

Imagine those test-takers' expressions if they knew the first to finish also was a film-maker, writing and helping produce documentaries about a range of subjects, such as autism, elephants and hunger. By the time she became a Certified Information Security Specialist Professional (CISSP), Sica was running her own trail race company, creating websites from scratch and would soon be writing for a sports blog.

All the while she continued converting a natural curiosity and attraction to rules and procedures into a successful cybersecurity career, moving from admin to IT help desk to network engineer to security to her current position as chief information security officer (CISO) for Petco, a 30,000-employee publicly traded pet wellness and health company.

PHOTOGRAPH BY TIM KING

Earlier this year she received a bachelor's degree in information systems and business analytics from Colorado State Global Campus, again defying the conventional path of a formal education first and entry-level job—let alone executive title—later.

But it's that unconventional career path that Sica sees as a key strength.

"It's not common to be both creative and technical," she says. "Right now, I'm not as technical as I used to be, but I still find creative solutions to problems. I think it's important to be able to look at issues from different angles—see them from store employees' or marketing groups' perspectives, not just the CISO's."

"I think it's important to be able to look at issues from different angles—see them from store employees' or marketing groups' perspectives, not just the CISO's."

—Jessica Sica, CISSP, CISO, Petco

DIFFERENT PERSPECTIVES

Lynn Hijar Hoffman agrees that those who come from non-technical backgrounds add a different dimension to the prevention of cyberattacks and their painful damages.

Hijar Hoffman is president of a San Diego-based boutique cybersecurity company called Cibernetika that she founded after years working in international business, primarily as an importer/exporter consultant at the city's World Trade Center. She also did a stint in diplomacy and military relations for a former mayor of San Diego, one the largest cities in the U.S.

Her path to cybersecurity began after the defacement of a website she created for an online platform she built for her import/export clients. Working with the website host's cybersecurity services to restore the site, she became interested in how to counter the threats cybercriminals posed.

Like Sica, she spent a lot of time self-studying technical aspects of IT security. Eventually her husband convinced her to apply to a new master's program in cybersecurity at the University of San Diego. "I loved it and continued to get more and more involved in projects. When the program was over, my husband encouraged me to take the CISSP exam."

Hijar Hoffman, who grew up in Mexico City and has lived her adult life in the U.S., lacked the five years of experience to become a CISSP, so she took the (ISC)^2 test in 2017 as an Associate before earning her certification in 2020.

"Honestly, I didn't focus on my lack of experience. Instead, I put on blinders and ignored some challenges while concentrating on overcoming some others," Hijar Hoffman explained about the work required to transition to security. "There were moments when I wondered why I got into this. But, I really liked doing this and there were plenty of good times to help balance the challenging ones."

DIVERSE BACKGROUNDS PAY DIVIDENDS

The cybersecurity profession is undergoing its own transformation, broadening pipelines to lure more qualified professionals into an industry with ongoing global workforce shortages. This longstanding gap has helped bad actors gain ground with increasingly sophisticated attack methods, such as spear phishing and ransomware-as-a-service.

Organizations like (ISC)^2 have taken up the cause with programs to help the less experienced more easily land an entry-level security position. Earlier this year, (ISC)^2 began piloting a certification program for recent graduates and relative newcomers, with domains and exam questions based on member feedback. The Center for Cyber Safety and Education has awarded millions of dollars in scholarships to those seeking a cybersecurity degree.

At the same time, (ISC)^2 is helping seasoned CISSPs move up the career ladder into more influential roles with webinars, courses, conferences and networking opportunities. One reason employers want to hire CISSPs is because the certification demonstrates both technical and business acumen. Continuous education for recertification assures companies these professionals remain on top of their fields long after their initial exam pass.

Widening the net of candidates is designed to attract adults with backgrounds traditionally not considered an easy fit for IT security. As part of a global push for greater diversity and

A DIFFERENT PATH TO **CYBERSECURITY**

TROY FINE, CISSP

Customer Success, Compliance Adviser for Drata, which specializes in compliance automation and continuous control monitoring

Years in cybersecurity: 8

Past occupation[s] outside the cyber realm:
SOX IT auditor

How difficult was it to transition to cybersecurity?
Initially it was tough, as I was coming from a CPA background, so I didn't have the baseline knowledge taught to me as part of a university program or on-the-job training. I mostly taught myself by performing audits and through constant research. However, I quickly realized that my knowledge of auditing concepts could serve me well. Through auditing, I was able to ask questions that allowed me to learn how cybersecurity controls were being implemented at many organizations. I was able to see the controls in action through supporting evidence. As I continued to perform audits and research, the transition became a thing of the past.

Most important skills developed from that earlier occupation:
- Risk assessment and risk management
- Control testing to evidence the operation of cybersecurity controls
- Interviewing control owners to perform walk-through of controls

Most relevant experience that continues to pay dividends with current role:
My auditing experiences.

Best advice for hiring managers when evaluating job candidates:
Ask how they learn about cybersecurity and stay up to date on emerging topics in cybersecurity. Ask what cybersecurity topics they are currently learning about.

Suggestions for cybersecurity teams/security operations centers who incorporate professionals with a less linear career path:
Hire for attitude and the passion for learning cybersecurity.

Words of wisdom, based on your own unique background:
Even if you don't have the ability to bring on entry-level personnel, give back to the cybersecurity community by mentoring others.

inclusion, more enterprises are bringing on team members with unconventional backgrounds in business, the arts, social sciences and humanities. Here again, (ISC)^2 is leading efforts through programs like the Associates program, and DEI Resource Center for hiring managers and team leaders.

Both Sica and Hijar Hoffman are among those who turned to cybersecurity later in life.

Sica benefited from learning cybersecurity skills while on the job, looking for internal opportunities to gain talents. "I think it's easier to move from one area to another within a company instead of starting at another company altogether," she said.

When she joined Petco, she let her manager know her career goals and how she intended to achieve them. (One reason everyone should give careful consideration to the ubiquitous interview question: Where do you see yourself in three to five years?) By following through on that plan and demonstrating leadership and management skills earned in previous roles, she was offered the CISO job around the time her boss was promoted to chief technology officer (CTO).

A DIFFERENT PATH TO **CYBERSECURITY**

JAMES COLLINS, CISSP

Senior Cybersecurity Consultant for a Big Four accounting firm

Years in cybersecurity: 7

Past occupation[s] outside the cyber realm:
Customer support and business analysis

How difficult was it to transition to cybersecurity?
The transition wasn't difficult, but you need to invest the time to learn key concepts and a lot of new content. This is challenging when you have a full-time job.

Most important skills developed from that earlier occupation:

- Communicating with stakeholders over the phone and via email
- Knowledge of basic project management concepts from my time as a business analyst
- Troubleshooting IT systems and software

Most relevant experience that continues to pay dividends with current role:
Communicating with stakeholders is essential for everyday activities within my role. Being able to see other points of view and communicate them was a skill I learned during my time in customer support. I still receive compliments from clients on how well I manage situations and convey key messages.

Best advice for hiring managers when evaluating job candidates:
Never judge a book by its cover. Yes, it's a cliché, but the senior manager who hired me confessed years later that he wasn't sure I was suitable for the role. But as a result of an excellent interview, he was willing to hire me anyway.

Suggestions for cybersecurity teams/ security operations centers who incorporate professionals with a less linear career path:
Simply because professionals with a less linear career path may not be aware of the day-to-day operations of a security operations center, doesn't mean they can't learn. Teach them the very basics and I believe they will re-use their already honed skills in new ways and to excellent effect.

Words of wisdom, based on your own unique background:
Don't let the world of cybersecurity intimidate you from joining it. We all started our learning somewhere. I joined the world of cybersecurity consulting as an experienced hire but had the level of experience in that area of a new graduate. I'm so glad I did since it enabled me to learn so much. The experience and skills you will gain will stay with you for a lifetime.

Sica was in her new position six months when the pandemic pushed Petco's workforce to go remote. That made it more challenging for people to get to know her and she, them. Sica made sure to always be on camera during video conferences and periodic leadership meetings, including board meetings.

"People need to know who you are, and that you're really there," she notes.

Bilingual Hijar Hoffman experienced typical initial struggles as a startup founder but eventually found her footing by leveraging her previous international business experience to gain clients. "Businesses in a lot of countries aren't as fortunate to have the kind of resources we have here in the U.S. to secure their businesses. There's a need out there that we can help with," she said.

In addition to running her company, Hijar Hoffman now teaches two cybersecurity

A DIFFERENT PATH TO **CYBERSECURITY**

DAMION GREEN

ISSO, General Dynamics IT

Years in cybersecurity: 7

Past occupation[s] outside the cyber realm:
Worked for Sony Entertainment (Indomitable Entertainment, Enticement Entertainment); Jennifer Lopez (JLE Enterprises); NBA

How difficult was it to transition to cybersecurity?
In my first job at Raytheon, I felt like I was drowning for the first couple of months. The people I worked with were great though. I'd worked with one of them at the local NBA B team, so we had a solid connection and he was super supportive.

Most important skills developed from that earlier occupation:
- Double check everything
- Ability to accept when you failed, admit it, fix it
- Not to be too judgmental of other people making mistakes; help them if you can

Most relevant experience that continues to pay dividends with current role:
The ability to concisely discern a problem and communicate that.

Best advice for hiring managers when evaluating job candidates:
I was hired into my first job because I built video editing computers. I wasn't super interested in tech, though I did like making a fast computer. Just because someone isn't broadly interested in "all things tech" doesn't mean they don't have that spark or the ability for that interest to grow.

Suggestions for cybersecurity teams/ security operations centers who incorporate professionals with a less linear career path:
There are a lot of abilities outside raw technical knowledge that are harder to gain. Attention to detail, communication, seeing flaws in a plan or in your own performance fall outside a certification, but they are more important than the immediate technical problems you face day to day.

Words of wisdom, based on your own unique background:
The desire to improve yourself is hard to prove and hard to see on a resume, but it's really important for any professional who wishes to grow.

Also: Be honest, with other people and with yourself. If you job requires you to not be honest, get another job. Success is more than the amount of money you make, it's the ability to choose good projects and good people to work with.

engineering courses at her alma mater. "I really like seeing different perspectives from students in online discussions on any given topic. I learn as they do about different approaches to the challenges we currently face."

ADVICE ON SKILLS DEVELOPMENT

Both women believe the strongest job candidate for a cybersecurity position may not be the most technically adept. Though technical skills are important, they also can be learned if someone has the aptitude and can-do attitude. What's harder to acquire—and perhaps convey—is genuine passion for the work and mission.

A DIFFERENT PATH TO **CYBERSECURITY**

SAM BERGER, CISSP

Senior Technical Director, AT&T (Telecommunication)

Years in cybersecurity: 16

Past occupation[s] outside the cyber realm:
Electrical engineer and vocational teacher in Germany; development work in Papua New Guinea; high school teacher; electrical infrastructure builder for several church stations and small business manager

How difficult was it to transition to cybersecurity?
Very difficult, not because of the subject, but because of life circumstances.

I'm trained as an electrical engineer and vocational teacher and worked in Papua New Guinea for eight years. When coming back to Germany, I didn't get a job as a teacher, so after six months of being unemployed, I managed to get a 12-month training opportunity as a system and network administrator. Those 18 months were tough, where I had little money to feed my family. I joined AT&T in 1999 and worked in customer operations for six years until I joined the Chief Security Office, where I now lead a team of security professionals in EMEA.

Most important skills developed from that earlier occupation:
- Cross-cultural communication
- Leadership in a cross-cultural environment
- Language skills

Most relevant experience that continues to pay dividends with current role:
When we first came to Papua New Guinea, a woman from a neighboring village visited to us one morning and emptied half her bag of garden fruits she was carrying to the market. We realized that she actually gave us half of the income she was about to get for a week. We knew we had to accept the gift in order not to embarrass her, but we didn't feel at ease. Our oversea boxes with our belongings had just arrived, so we went into the house to look for something in return. We gave her a couple of T-shirts and other small things, but she didn't want to take it until we almost forced it onto her. However, we realized something was wrong.

A local mentor later told us that in Papua New Guinea you give someone a gift when you want to start a relationship. If the receiving party accepts it and can stand the tension that they are in someone's debt, that is signal that they are interested in that relationship. (There will be a chance to help the giver at some later date.) If you give something back immediately, you signal that you do not want to be in debt with that particular person; hence, you do not want a closer relationship. Though we wanted to be kind and generous we had actually done the wrong thing. I learned the importance of understanding a culture (we later made up for our faux pas and actually had a good relationship with that family).

Best advice for hiring managers when evaluating job candidates:
Be aware and appreciate of cultural differences when evaluating the responses and values of others.

Suggestions for cybersecurity teams/ security operations centers who incorporate professionals with a less linear career path:
People not "growing up" in cybersecurity usually have some broader experience in life, having worked in other sectors where business cultures might have been different. They might bring to the team an outsider view and diversity that can add value to the creativity and productivity of a team.

Words of wisdom, based on your own unique background:
Never take anything for granted.

"I have brought in people who weren't as experienced," Sica said. "But they understood how security supports the business. They have to have that business acumen in a big company like Petco, so they take the business into consideration when making decisions."

Hijar Hoffman believes technical skills are more important for some security jobs than others. "If you need a pen tester, you need someone with strong programming skills no matter what," she said. "But when it comes to other areas, I think a lot of hiring managers aren't looking beyond cybersecurity skills. And that's a shame because a lot of us come with other skills that perhaps employers don't even consider."

Sica believes that diversity and inclusion are highly valued at Petco, and not necessarily in terms of gender, race and ethnicities. "I think diverse teams make very valuable teams because different experiences allow you to look at problems differently," she said. "I don't want clones of myself working on my team; I want to see different backgrounds that will look at a problem through different lenses."

Hijar Hoffman encourages newcomers to network. "I know it's tough in this area for a lot of people who just don't like to do it," she said. "A lot of people that are attracted to this field prefer to be behind a computer screen."

After becoming an (ISC)² Associate and then a CISSP, she joined the (ISC)² San Diego Chapter and now serves on its board. Chapter meetings and events continue to provide opportunities for new business, she added.

Both women also encourage others who want to transition to a new career to stay the course even when adversities arise. Instead of downplaying non-technical skills—like business and communications—acquired through prior experiences, highlight them to hiring managers who understand their value.

"I think people who go by the book today have a harder time getting into security than someone who stands out a little more," Sica explained. " Not just by having more certifications, but by having done something other people haven't."

Anne Saita is editor-in-chief of *InfoSecurity Professional*.

HIDDEN GIGS AMONG US

What to do about employees working for other companies while on the clock for yours

BY ASTRID HARDERS

WHAT IF JOB DESCRIPTIONS included the *exact* amount of time an employee is expected to spend doing *actual* work? What if the time in pointless meetings doesn't count? How many hours per day would your job description state?

For an IT engineer who rose to Reddit and *Newsweek* fame back in January (but remains nameless/unidentified), his work time at his home office desk clocked in at an enviable 10 minutes per day. In those daily 10 minutes, this guy got everything done he was asked to do. The law firm that had hired him to migrate digital court evidence onto a cloud was getting what they needed, and everyone was happy.

ILLUSTRATION BY PETER AND MARIA HOEY

How did this dream scenario come about? The IT engineer automated his job by writing a script that performed his responsibilities for him. At the end of the day, he would simply sit at his computer to make sure everything ran smoothly. The rest of the day was wide open to play video games and work on a side project. The IT engineer got a digital standing ovation from many, many Reddit users.

But is this guy a hero or putting himself and his employer at risk? What led to a situation in which someone could get paid close to $90,000 a year working only 10 minutes daily without a drop in productivity?

Like many remote workers during the past two years of the pandemic, this IT engineer's best allied circumstance was the home office. In early 2020, when millions of people all around the world switched to working from home, bosses lost much of their surveilling control. Sure, we all had a seemingly endless carousel of Zoom meetings to sign into, and some organizations already used software to monitor computer activity, but was that really the same as being a few desks away from those in charge?

"Maybe they are not being compensated with what they are looking for, or they're in a rut with their current job thinking, 'I can do it with my eyes closed.'"

—Joey V. Price, CEO, Jumpstart

For some industries the move to remote, distributed working might have been a positive, more productive shift. But for others, remote work simply meant employees could get away with a lot more. In fact, some workers discovered that being remote presented a golden opportunity to start a side hustle. Perhaps a freelance gig that generated extra income. Or, even better, a complete second full-time job to double the existing salary. *The Wall Street Journal* reported that white-collar workers in banking, tech and insurance devised all sorts of resourceful tactics—having two laptops; connecting external microphones to mute themselves without colleagues being alerted; color-coding browser windows for each job; childcare, burnout and home device malfunction excuses—to juggle two jobs without bosses knowing. As with the IT engineer, questions arise: Are these folks heroes sticking it to a system that wasn't valuing them enough anyway? Or are they causing more problems for us all?

According to Joey V. Price, CEO of Jumpstart, a company that provides small business and startup HR outsourcing and managed HR services, it's necessary to identify why exactly people are taking on secondary jobs.

"If I were to guess—the research isn't out there yet because it's such a new phenomenon—I would suspect it's one of two things: either pay or boredom," Price said. "Maybe they are not being compensated with what they are looking for, or they're in a rut with their current job thinking, 'I can do it with my eyes closed.'"

Whether for the pay or the hunt for something stimulating, before getting on the secondary job wagon, make sure it's safe to do so.

STRATEGIZE YOUR DOUBLE-DIPPING

How can people who double-dip in their career make sure they're not shooting themselves in the foot?

Matthew L. Berman, a partner of Valli Kane & Vagnini LLP, an employee rights attorney firm in New York, sees the possible conditions at play: "The side hustle question depends on a number of factors, one of them being fraud. If the employee is being paid on an hourly basis, he cannot sell the same hour to two different employers. It's different when you're a salary person who is paid for performing certain services."

So, if you're a contractor, make sure you're not double billing the same hour of work to two different employers. But, if you're a salaried worker, you might be OK, as long as you get your tasks done.

There are obvious cases where employees are just digging their own work grave. For example,

when you engage in a side hustle or a secondary job with a competitor to your primary job. Berman explained: "If I work for Coca-Cola, I can't also be working for Pepsi. They're competing with each other. I'm being blatantly disloyal against my employer at Coca-Cola when I do stuff for Pepsi."

But what if your secondary gig is not with a competitor? Are there dangers to avoid?

"One way to get around that is to ask for permission. If they give you permission, you are in the clear and on the right side of the law," said Berman. "Of course, getting permission could be challenging. The company may tell you, 'We don't want an open relationship, we don't swing that way.'"

The safest and first step if you're contemplating a secondary job is to carefully read your current contract. Does it mention anything related to non-competitor clauses? Does it include exclusivity clauses? How does it land in terms of antitrust law? If you are not sure, it's best to seek professional counsel. It might seem exaggerated, but an expert can advise you on what you can and what you shouldn't lawfully do when seeking secondary employment.

"One way to get around that is to ask for permission. If they give you permission, you are in the clear and on the right side of the law."

—Matthew L. Berman, partner, Valli Kane & Vagnini LLP

COMPANIES BEWARE

On the flipside, how can organizations best prepare to handle employees double-booking their time?

"It's handled case by case," Price explained. "I would start with your employee handbook. What does it say about moonlighting, additional jobs, even non-competes or non-disclosures?" And depending on what a company's employee handbook says, it might be time to update clauses and rules now that COVID-19 and remote work have changed the physical and virtual workplace.

"The next thing I would do," according to Price, "is check with your company values. Are you comfortable with individuals holding two jobs? If so, what does that look like? How do you make sure people are successful?"

Once again, COVID-19 has turned equations upside down. Is it possible for employees to be successful at two jobs at the same time? Does your organization believe a person can fully deliver when focusing on two separate full-time roles?

"The other thing I would do is have a conversation with that individual," Price recommended. "Say, 'What's your plan?' Because you can work on weekends, you can work evenings, but it's risky to do that."

Companies of all sizes might have to think beyond re-educating their managers and HR departments. With the two-hidden-gig economy, there may be serious legal ramifications.

Let's go back to that IT engineer and his side project he worked on while on the clock with that law firm. What if this side project, as a Reddit user suggested, turns into a successful money-making operation? Could the law firm, once it realizes what the IT engineer was doing, be entitled to a share of the side project's monetary gains?

According to Berman, "If an employee has an employment agreement with their employer, it is not uncommon to have something called an assignment of invention clause in there, especially with tech workers—and they may not realize that it's in there when they sign it. It says anything that you invent or create while you are our employee, working on our time, we own. So, if our IT specialist's contract had one of those clauses, the law firm could open that technology and say to him, 'We don't need you anymore. We're keeping the invention and we'll have one of our staff work with it. Thanks for improving our efficiency so much. Bye!'"

Regardless of the minutiae of each case, the fact everyone can agree on is that the two-gig economy exists and is gaining momentum. So, we might as well get used to it.

“We’re going to have to reckon more and more with the relationship that humans have with technology in the pursuit of fulfilling their job duties. We’re going to have to challenge everything.”

—Matthew L. Berman, partner, Valli Kane & Vagnini LLP

“In the IT specialist’s case—and I don’t have all the context—butI think he’s brilliant. He is the kind of person who could start a company and be very successful because he figured that out,” said Price. More generally, he added, “we’re going to have to reckon more and more with the relationship that humans have with technology in the pursuit of fulfilling their job duties. We’re going to have to challenge everything.”

As Berman put it: “Instead of telling someone, ‘You’re getting eight hours of work done in 10 minutes? You’re fired!’ They could say, ‘Wow! What else could you do with that [script]?’”

ASTRID HARDERS is a Miami-based freelance writer who previously wrote the cover story on the security threats surrounding remote workers in the January/February 2021 issue.

MANAGING difficult EMPLOYEES

We may no longer meet as much in person, but that doesn't mean we won't face workers struggling to get by—or get along

BY MARK TARALLO

ILLUSTRATION BY JAN FEINDT

PROBLEM EMPLOYEES. Difficult staffers. Team members in need of behavioral modification and attitude adjustment. They may be uncooperative, overly negative, excessively distracted or simply hard to work with. They usually require a special approach.

There is no one silver bullet solution or scripted spiel that can suddenly make a difficult team member easy to work with. But there are numerous strategies, covering various parts of the process, that can be very helpful. As a manager, sometimes you may have to deal with difficult behaviors that stem from well-entrenched personal qualities, and so you need to be creative in your use of personal strategies and management tools.

PRE-QUALIFYING

The first piece of guidance here is simple: Don't let a team member reach the point where they become a problem employee. This entails a sustained effort on your part, and the effort starts during the hiring process.

A good place to begin is by following this guideline: Hire not only for the right skill set, but for the right qualities and attitude.

To do this, look for indications of emotional intelligence when learning about candidates during the recruiting and interviewing process. Those indications can include relationship management skills, self-awareness, social awareness, empathy, altruism and an amenable personality.

A good place to begin is by following this guideline: Hire not only for the right skill set, but for the right qualities and attitude.

Once the new hire begins, continue the effort during the onboarding process. Initiate conversations with the new hire on responsibilities, expectations, and other topics that will make their role clear. Encourage questions to help build their understanding of the position.

Once onboarding is finished, these regular conversations should continue, perhaps a 10-minute informal chat every few weeks or so. These chats are helpful for several reasons. They allow each party to provide feedback. If signs of unproductive behavior in the workplace are starting to crop up, they can be discussed before they have time to solidify. Moreover, the new team member can let you know how they feel about their assignments and role, and any adjustments that can be explored.

These chats also allow you, as a manager, to repeatedly emphasize how the team member's role is tied to the success of the organization, which can go a long way toward maintaining the staffer's sense of mission.

And these conversations also allow you to gauge the team member's alignment with the organization. Through active listening, you can learn about the staffer on a deeper level: their sense of mission, values, life goals, and involvement in the community. It is these types of discussions that show team members that you care about them as an individual and as a team member.

Once you gain this deeper knowledge about a team member, you can better understand how their values align with the company's mission, and the ways in which they feel most connected with the organization. This alignment of values is the best environment in which to build trust and connection. When that happens, the staffer is much more likely to be engaged and professionally fulfilled, and much less likely to become a difficult or problem employee.

PROFESSIONAL OBJECTIVITY

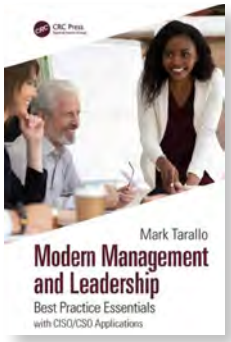
Of course, some managers, such as those newly hired or promoted, take over a department that is already staffed. In those cases, you may find yourself face-to-face with a difficult employee, with no previous opportunity to work with them at the point of hire or immediately after.

In these situations, you should strive to be as self-aware as possible when approaching any problems. Ask yourself, "Are my behaviors or actions making this problem worse?" Try to answer that question as honestly as possible.

Here are a few examples how managers may make the problem worse.

- Some managers may sense problems with a staffer's behavior or attitude and become frustrated, but never take concrete actions to address it, and the problem worsens.
- Sometimes, a manager assumes that the team member knows there is a problem, and so the manager becomes more and more frustrated because they feel that the staffer is knowingly continuing to transgress. This could lead to a blow-up on the manager's part that is neither professional nor managerially sound.
- In other cases, managers devote a tremendous amount of extra attention and time to difficult employees, and this runs the risk of rewarding bad behavior.

So, besides self-awareness, strive for maximum fairness in your approach. If you are looking



This article is an excerpt from *Modern Management and Leadership: Best Practice Essentials with CISO/CSO Applications* (2022, CRC Press) by Mark Tarallo.

A Q&A WITH THE AUTHOR **MARK TARALLO**

What was happening in the IT world that made you write a book on security leadership?
Security professionals were continuing to be promoted into managerial and leadership positions without having comprehensive training or education in those practices. Many IT managers were learning day-to-day management tasks through trial and error. Other professionals were thrust into leadership positions without any deep guidance on what it means to lead people.

Given this situation, a publishing company editor, who believed that the security space needed more leadership and management guidance, approached me about writing a book. And I think most would agree that information security has become ever more crucial to organizational survival, so the importance of security leadership continues to grow.

Although the CISO/CSO position is relatively new compared to other chief executives like CTO and CIO, it's been around long enough to have built up credibility and influence. What can cybersecurity leaders do now to gain the same stature as a CTO or CIO within an organization?
They can demonstrate, through their words and deeds, that their knowledge base stretches beyond IT and security. They can show they understand the organization's mission, business objectives and operations, as well as the concerns of the stakeholders. They can offer guidance on how information security can address and improve all of these.

Most C-suite executives are usually responsible for leading their department's staff. The current pandemic is the perfect time for the CISO/CSO to share with other leaders their effective initiatives regarding talent development, employee engagement, coaching and other crucial management functions which the book provides guidance on. The best way to build stature as a leader is to ensure that those whom you lead are thriving.

You wrote this book at the start of the pandemic. What has changed since then that makes the lessons even more relevant?
The pandemic brought new and heightened challenges to the IT security profession, involving developments such as increased remote work, the "infodemic" of spreading disinformation, and various attempts by bad actors to use the COVID-19 crisis to exploit security vulnerabilities.

But as a life-and-death public health crisis, the pandemic also accelerated the already increasing focus on the "human side" of management and leadership. However technical and complex the work becomes, IT security work is conducted by humans who value meaningful work and make mistakes, not by robots. So much of the guidance in the book—including topics like protecting staff from burnout, self-management for leaders and ensuring staff understands how their work makes a difference—has become even more relevant.

Cybersecurity professionals encounter differences of opinions and actions when dealing with a major event, such as a data breach that exposes private information. What one main thing should a CISO do to show true leadership during such a crisis?
Communicate effectively. In practice, this has several components. One important piece is empathetic listening. As you say, there will be different views and pieces of advice expressed in these situations. Leaders should do their best to communicate that the various concerns are being heard and that actions moving forward will take those concerns into consideration.

Another is to ensure communications are accurate and unifying. Sometime when a breach occurs, leaders send out messages to staff that sound like blame-shifting: Here's how you guys have been careless with security, and now we are all paying the price. Instead, leaders should communicate honestly in describing why the breach is serious and what needs to be done moving forward, but also reinforce the unifying belief that the quality and talents of the staff make recovery an encouraging prospect and a learning opportunity, especially if everyone pulls together as a team.

Not all great employees make great managers, and not all great managers make great CISOs. If you were hiring, what would you ask a management or CISO candidate to help determine if they are up for the role?
I would ask a few questions about their leadership style, their core management concepts or philosophy and their goals as a leader. Here, any answers should reflect inherent professional respect for team members. One red flag would be a philosophy that suggests: I make sure to always keep on my people so they don't goof off and skirt their responsibilities.

I would be encouraged if the candidate's answers reflected a desire to achieve win-win outcomes. In other words, the manager strives to lead in such a way to facilitate strong performance from staff, which benefits the organization, while also having a focus on the staff's development and professional growth, which benefits each employee and their respective careers.

into a problematic situation with a team member, make sure it does not veer into witch hunt territory. Do not leap to conclusions, and be as open to input as possible. Facts are facts, but they can change, so be as objective as possible.

Maintaining professional respect is also key. Your meetings with staffers should never have the tone of a parent–child scolding session, but rather an adult-to-adult constructive conversation between two intelligent professionals.

Overall, it is usually best to take a positive and optimistic stance during the discussion and focus on future improvement. For example, you may clearly state: "What I would like to do here is for us to find a way forward." Solicit the team member's ideas on this, as well as offering your own.

Your meetings with staffers should never have the tone of a parent–child scolding session, but rather an adult-to-adult constructive conversation between two intelligent professionals.

It is also a good practice to strive for agreement and feedback from your team member. If certain procedures or policies were breached, you should state those and then check for understanding.

In such cases, it is important to remember that any actions that can be interpreted as discriminatory, or as harassment, can lead to civil action by employees. Hence, proper documentation, which can show that the employee was not singled out for special treatment, is important. Seeking cooperation in documentation is often advisable; if you are documenting the meeting, you may ask the employee to agree with the documentation.

RE-ENGAGEMENT

In some cases, a team member's problematic behavior and attitude is a manifestation of a deeper underlying issue: lack of engagement with their job.

This possibility is often worth discussing with the staffer. Sometimes, an honest and supportive conversation will reveal a truth—the team member is simply not in the right job. That is an unpleasant thought for some, especially longtime employees who are at a loss for what they would do if they left their current job.

But if that is the case and it is acknowledged, a manager can then work with the employee on some potentially productive activities.

For example, you can help the team member frame a vision for a future career. This may give him or her the impetus to resign and find a job that they would be more aligned with. Or, they may see new value in the current position (perhaps with a few adjustments) as a stepping stone on the way to their desired career destination.

However, in many cases, a staffer's lack of engagement is not because they are an inherently poor match for the job; the deeper reasons that drove them to enter the profession are likely still valid. Somewhere along the way, the connection was lost. Often, that's because the staffer is not seeing clear evidence of why his or her work is crucial to the organization and its mission, and how that mission is important to the larger world.

This is because evidence of this importance and value can be obscured in different ways. Day-to-day repetition can make work seem negatively formulaic. Overwork can compel staffers to focus, above anything else, on keeping their heads above water. Sometimes, concepts like mission and purpose are given lip service, but never explicitly expressed or explored. Once the connection is lost, it's a rare staffer that will flat-out ask management, "Can you show me why my work matters?"

But here you can take the initiative and, through exploratory discussion, help your team member regain perspective on their contributions and value, to the organization and beyond. You can point out where the connection is, in a way that could re-inspire them.

BEHAVIORAL SPECIFICS

Every team member is unique, distinctive. Nonetheless, there are certain types of difficult behaviors and attitudes that occur in many workplaces. Below are examples of some common difficult workplace behaviors, based on conversations with workplace issue experts as well as

a review of published HR literature. Each thumbnail sketch is followed by some best-practice advice on how managers should deal with each one.

Negative Nancy

Nancy naysays projects and assignments. Shoots down the new ideas of others. Often predicts doom. Frequently makes comments such as, "We tried that before, and it never works." "This project is turning into a complete disaster." "There's just no way we can meet a deadline like that."

Sometimes, negativity is used by an employee as a badge of intelligence. Critics often seem like authorities, so naysaying a project can be an attempt by an employee to try to highlight their expertise and their range of professional experience. The manager, then, should strive to redirect that expertise in a more positive direction.

If the pattern of negativity becomes disruptive, you may want to have a conversation about this pattern and invite Nancy to take a different tack. In doing this, use a factual approach when noting behavior patterns such as Nancy's tendency to criticize when new ideas are proposed at staff meetings. You may also explain how past failures may be the result of timing issues, not problems inherent to the idea.

Finally, you can encourage and coach Nancy on changing her focus so that the project is improved and not obliterated. For example, you can ask Nancy what success looks like to her. Have her paint a picture of success, and ask her what she would do differently to avoid the incidents of the past.

Egotistical Eddie

Eddie acts condescendingly. He dominates discussion at staff meetings. He resents being asked to do mundane but necessary tasks. His immense self-regard alienates coworkers.

While prima donna behavior can be frustrating for other staffers to deal with, a manager should be careful to keep the focus on business factors, and not on irritating personal characteristics, when discussing issues with Eddie. So, avoid saying things like: "You obviously think you're all that, and it is annoying to other team members."

Instead, focus on how Eddie's specific actions may be hurting staff productivity. For example, you might discuss how Eddie's domination of staff meeting discussions hinders others from contributing ideas—and that makes for a diminished output from the team on the whole. It is also good practice to make clear to Eddie that his team-hindering actions do not negate his own valued contributions and skills, which are an asset to the team. Emphasize that the goal is to create a positive workplace where everybody, including Eddie, can contribute and everybody feels comfortable.

Crisis Charlie

Charlie's life circumstances frequently interrupt his work life: long personal phone conversations in the office, mood swings, and oversharing about relationship issues to other employees. His life events, like his divorces, can affect performance for weeks.

Here a manager should tread very carefully. Personal crises can come in clusters—an employee may need to help care for elderly ailing parents, which can schedule disruptions and economic stress, which in turn can cause marital stress and possibly separation, which can cause stress for the children. It's also possible that mood swings and oversharing may reflect medical issues, which is all the more reason for a manager to be careful.

At the same time, a manager can make a huge contribution to a team member's career and well-being by being supportive in troubled times. In sensitive one-on-one conversations with the employee, you should be able to begin to gauge the level of the problem.

These conversations, although delicate, can afford you an opportunity for you to gain a deeper understanding of an employee's life context—the challenges they face outside of the workplace that may affect their performance at work. It may also be an opportunity for you to highlight the organization's employee assistance program or other resources the company may have to help.

Focus on being supportive but still candid. It is appropriate to discuss how a staffer's demeanor may affect others on the staff, especially since the employee may be unaware of this, but discussions should be nonthreatening and considerate. Inform human resources about the situation as well.

Challenging Cathy

Cathy thrives on taking on authority. She will often challenge a manager's directives and be privately critical of decisions by upper management. She is frequently derisive of "company men."

In many cases, thoughtful criticism of operations can lead to greater innovation and efficiency. A manager may coach Cathy to help make her presentation and style more palatable, but still offer constructive suggestions that lead to improvements.

When doing this, try to coach Cathy to be less attacking and avoid being cutting or derisive in her questions. You can also help her reframe her questions to be more what-oriented or how-oriented, which can help people focus on the issue and be less defensive.

Why Everyone Needs a Coach

BY MICHAEL HANNA, CISSP

American businessman Bob Nardelli once said, "I absolutely believe that people, unless coached, never reach their maximum capabilities."

That's why I firmly believe that, as leaders, we must be willing to receive coaching and develop to our greatest ability. Doing so means that we may contribute to the positive improvement of our teams' *personal and professional* lives. Just like the mind and body must align for optimal performance, so should the personal and professional components of our lives. By examining Maslow's Hierarchy of Needs or Existence, Relatedness, and Growth theory of needs, human beings cannot reach their optimal levels (top of the pyramid) if they are stuck worried about lower levels like physiological, safety, social or esteem needs.

U.S. football hall of famer Tom Landry, both a player and head coach Super Bowl champion as well as a World War II Army officer, describes a coach as "someone who tells you what you don't want to hear, who has you see what you don't want to see, so you can be who you have always known you could be."

That's one of the most succinct definitions you will find about coaching. Occasionally, we place self-imposed limits on who we think we can be, but we need to encourage and guide those we coach to see past those limits—ourselves included. Here are a few of my coaching tips:

Tip 1: Ask yourself: What's the end-game? Determine optimal or best outcomes, personally and professionally. Coaching sessions do not need to only be restricted to professional development because people care about other areas of their lives, and these other areas impact performance.

Sure, sometimes there are "fires" we need to put out, but sometimes work can be set aside to make a team better.

Tip 2: Your time is not worth more than someone else's time. If you set up a coaching session, do not repeatedly cancel or postpone that session because you are busy. Sure, sometimes there are "fires" we need to put out, but sometimes work can be set aside to make a team better. In a year or two, you might not remember the instances you repeatedly rescheduled a session, but that other person will *always* remember that you thought they were not important enough.

Tip 3: Take various personality tests to self-inventory your strengths, weaknesses, motivations and likely behaviors. For example, taking and understanding my Enneagram type helped me better understand myself so that I could better coach the team around me.

Coaching and developing our teams must be a top priority as cybersecurity leaders. Give some of these tips a try, share your coaching tips with the (ISC)² Community, and don't curb your excitement of better understanding yourself after taking your Enneagram test. •

Dr. Michael Hanna is a leader and a university professor within the field of information technology and cybersecurity. He specializes in developing high-performing teams, artificial intelligence and cybersecurity. You can reach him on LinkedIn at Michael Hanna. The views expressed here are solely those of the author, and do not necessarily reflect those of the Department of the Navy, Department of Defense or the United States government.

Accuracy. Actionability. Timeliness. Scalability.

At BlueVoyant, we recognize that effective cybersecurity requires active prevention and defense across both your organization and supply chain. Our proprietary data, analytics and technology, coupled with deep expertise, works as a force multiplier to secure your full ecosystem.

Digital Risk Protection Platform

BlueVoyant provides organizations with real-time visibility of digital threats by continuously monitoring domains and websites, social media, apps in official and unofficial stores, deep & dark web, instant messaging and open-source – allowing for quick and effective breach mitigation.

BlueVoyant's extensive global coverage, data science, and analyst expertise enables identification of malicious "look-alike" attacks, live phishing pages, and more. A competitive differentiator, we have an unmatched ability to take action on your behalf to eliminate threats to your brand, employees, and customers.

BlueVoyant's new eBook, "Digital Risk Protection: From Reactive to Proactive Security Posture," addresses the following:

- Common cyberattacks used by today's threat actors
- Recent changes to the threat landscape based on the increasing popularity of hybrid work models
- The advantage of leveraging a Digital Risk Protection (DRP) solution to establish visibility and establish a proactive approach to security

Learn more at www.bluevoyant.com
Download the DRP eBook: http://www2.bluevoyant.com/DRP-ebook-ismag