WHAT MEMBERS CAN EXPECT IN 2022

InfoSecurity PROFESSIONAL

NOVEMBER/DECEMBER 2021

In Zero, We Trust

+

Healthcare Security

Grief and Incident Response

(ISC)² An (ISC)² Publication

Find Out

What Professionals are Reporting About CLOUD SECURITY

Did you know that **96%** of organizations are moderately to extremely concerned about cloud security? Or that **39%** of organizations indicated lack of qualified staff is their biggest cloud security concern?

The 2021 Cloud Security Report, sponsored by (ISC)², explores the challenges organizations are facing and how they are responding to security threats in the cloud and continuous shortfall of qualified staff.

Download the 2021 Cloud Security Report and find out what else professionals are reporting.

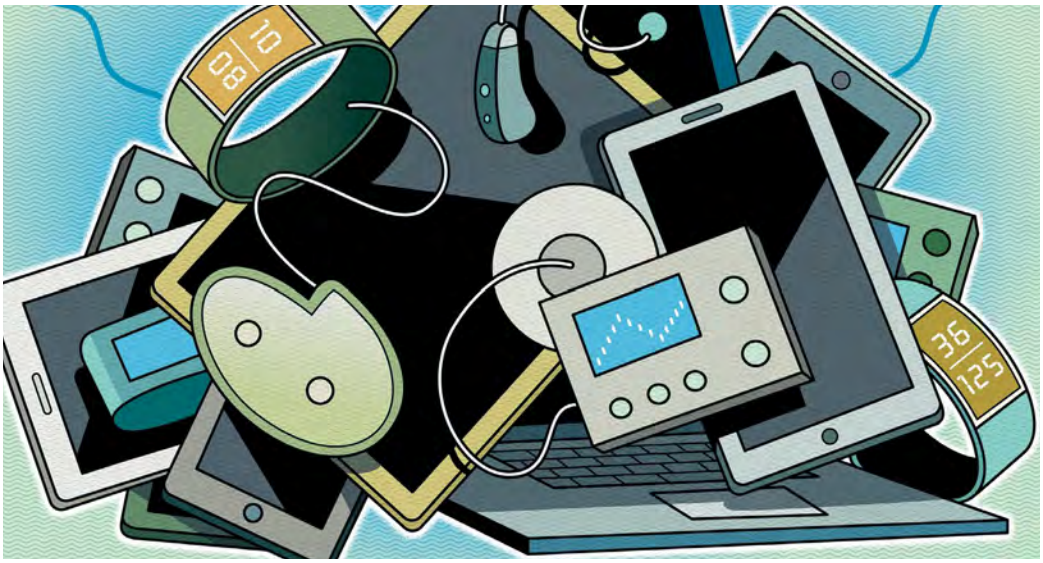
Get the Report

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

CCSP® Certified Cloud Security Professional

An (ISC)² Certification

CONTENTS ▪ NOVEMBER/DECEMBER 2021 ▪ VOLUME 14 - ISSUE 6



Protected Health Information at risk.

PAGE 25

FEATURES

Cover image by John Kuczala

Illustration (above) by Peter and Maria Hoey

Illustration (right) by Ard Su

DEPARTMENTS

EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

Seeing How We Work Through a Different Lens

EARLY IN MY JOURNALISM CAREER, I covered a murder trial in Highland County, Virginia. It took hours of white-knuckled driving up and around winding, narrow mountain roads to reach "Little Switzerland," as the state's least populated county was called. The rural outpost was then home to psychiatrist Elisabeth Kübler-Ross, who chose the agrarian area as her full-time retreat.

I remember asking locals during courtroom lulls how they felt being neighbors with a woman whose work with the dying was so widely known. Not everyone was a fan, especially after Kübler-Ross announced plans to open a hospice center for children with AIDS. Several years after my visit, arsonists torched Kübler-Ross's log cabin and killed her prized llama. If running her out of town was the goal, it worked. She moved to Scottsdale, Arizona, where she remained until her death in 2004.

I thought of that trip to tiny Head Waters, Virginia, after reading CISSP Marc Muher's piece in this issue comparing Kübler-Ross's Five Stages of Grief to a common framework for incident response. It's novel, for sure. But so is Muher, who studied Kübler-Ross's work while earning a master's degree in social work. He then worked with people with disabilities, convicted juveniles in both wilderness incarceration and residential treatment programs. Eventually, he left the field for a career in cybersecurity.

Not everyone would be able to see similarities in grieving a huge loss and responding to a cyber incident, but Muher did because his experiences differ from most (ISC)² members. This is among the reasons why we should all consider adding job candidates with nontraditional backgrounds to security operations teams. They see the world of threats and vulnerabilities from new perspectives; they introduce workflow tweaks that make everyone more productive.

If you transitioned to cybersecurity from a completely different field—film, international studies, social sciences, art, music, nursing, medicine, law, humanities, retail, wilderness training, etc.—I'd love to hear from you. Tell me your story at asaita@isc2.org. I want to know not just how you made the transition, but how that transition made you into the professional you are now. Was it difficult? Surprisingly easy? How has your unconventional journey to cybersecurity helped you? Hurt you? I really want to learn more from you. And something tells me others do too. ●

Photograph by Louise Roup

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

CONTRIBUTORS

This issue's Editor's Note highlights contributor **Marc Muher**, a former clinical social worker who is now a CISSP currently working in information security for a large municipality. He combines models from both former and current professions for a great piece on grief and incident response.

Another CISSP, **Michael Pinhorn** in the U.K., looks at what it takes to actually implement Zero Trust, an article inspired by his own research into one of the hottest topics this year. Michael heads Information Security Governance, Risk and Compliance for the University of Oxford's Information Security Team. That said, he admits: "I won't feel like a security expert until I can stop my 12-year-old from working around all my parental controls."

Las Vegas freelance writer **Shawna McAlearney** is inspired by what she learns at the annual Black Hat conference, which for years now has featured sessions demonstrating the vulnerability of implantable medical devices. IMDs open her feature focused on healthcare security.

Siblings **Peter Hoey** and **Maria Hoey** created this issue's illustration for "Infection Control." They have collaborated on work appearing not only in *InfoSecurity Professional*, but also in notable publications such as *Time*, *Rolling Stone*, *The New York Times*, *Print*, *Mother Jones* and more.

Ard Su, illustrator for "Coping with Loss," is based in New York. She graduated from Maryland Institute College of Art in 2020 with an MA in illustration. Her clients include *The New Yorker*, *The New York Times*, *The Washington Post* and more.

Global Cybersecurity Trends

and Insights You Need to Know Now

How do your perceptions and security posture stack up against those of your peers? Learn the latest trends and insights inside CyberEdge Group's Cyberthreat Defense Report, sponsored by (ISC)².

Based on a survey of participants representing 17 countries and 19 industries, the report provides an in-depth look at how cybersecurity professionals perceive and defend against cyberthreats. The research reveals:

87%

of organizations are experiencing a shortfall of skilled cybersecurity personnel.

The typical enterprise cybersecurity budget increased 4% last year, but the rate of budget growth slowed for the first time in years.

57%

of ransomware victims paid ransoms last year, encouraging bad actors to increase their attacks.

Download the report and use the 2021 findings to benchmark where your organization stands.

Get the Report

InfoSecurity PROFESSIONAL
An (ISC)² Publication

(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/Nov-Dec-2021

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.

CCSP: The Solution to Your Cloud Security Challenges

Are you confident in your organization's cloud security posture? Cloud computing skills gaps have nearly doubled in the past 3 years, leaving businesses around the globe challenged by a lack of staff expertise. For a competitive advantage, they increasingly look to (ISC)² and the CCSP.

Download our white paper for 10 reasons why you should invest in CCSP team training and certification. You'll quickly learn how to better defend against cyberattacks – and find the silver lining in the cloud.

Ready to Command the Cloud?

Get Your Copy

CERTIFICATION MAGAZINE
2021 TOP CERTS
CCSP
CISSP
(ISC)²
THE NEXT BIG THING

CCSP was named ***"The Next Big Thing"*** by Certification Magazine

Growth and Engagement in 2022

BY TARA WISNIEWSKI

This has been a year of immense change for (ISC)². We continued to operate through a global pandemic, our CEO completed her first full year with the association and our executive management team has grown. As we build out new and exciting capabilities that will set the stage for an extension of (ISC)²'s impact and influence around the world, I want to share with you the vision for what that will look like in 2022.

Tara Wisniewski is the EVP of Advocacy, Global Markets and Member Engagement at (ISC)². She can be reached at twisniewski@isc2.org.

While our goal continues to be to advocate for our members and the cybersecurity profession, we're examining what that means in practice, and formulating plans to become more involved in geopolitical discussions on the workforce shortage, security standards and regulatory compliance. Not only do we need a seat at the table, but we want many seats at multiple tables. (ISC)² has the power to be a convener and catalyst for the dialogue that is needed at this moment in history.

This effort is in recognition of the fact that while our member base is truly global in scope (you hail from more than 175 countries), (ISC)² is a lean organization and has traditionally been U.S.-focused by necessity. Cybersecurity is borderless, as are the attacks our organizations face, and the discussions about how to meet these challenges are happening on a global level. We are committed to driving these collaborations. As such, we will be expanding our profile and engaging with leaders across regions to make our members' voices heard. You will start to see progress on this front next year, and we are excited to represent you in a much more global capacity.

We will also step up our member engagement efforts to provide strong value to our members while inviting more talent into the profession to reinforce the work you are doing to inspire a safe and secure cyber world. Because of the vast member network you are part of, we are designing new ways to enable you and others to tap into knowledge and resources that will help you thrive and feel supported by your cyber community. This will create opportunities for younger professionals to build their careers while opening avenues for those who want to pass on their expertise.

We will also step up our member engagement efforts to provide strong value to our members while inviting more talent into the profession to reinforce the work you are doing to inspire a safe and secure cyber world.

We're also adding resources to the Center for Cyber Safety and Education to amplify the services it currently offers and expand the portfolio of programs within it. While the Center has traditionally been focused on providing cyber safety lessons to elementary aged students, there is a clear opportunity to make it a more nimble and agile part of our organization. Over the next few months we will work to redesign the Center and launch enhanced and new programs in 2022 that will enable greater reach and impact in our mission to inspire a safe and secure cyber world.

There's never been a time where more opportunities were available to us to make a global impact on cybersecurity. We look forward to sharing updates on our progress with you in the new year. •

Cybersecurity is Only as **STRONG** as its WEAKEST Link

The cybersecurity of your organization can be thought of as a chain. And every chain is only as strong as its weakest link. How strong are the links in your organization's cybersecurity?

Stronger Cybersecurity Starts with CISSP

CISSP certification arms your employees with the expertise to design, engineer, implement and run a premier information security program. Make your people your greatest strength and protection. Certify them with CISSP.

CISSP®
Certified Information Systems Security Professional
An (ISC)² Certification

Get The Definitive Guide for Cybersecurity and Business Prosperity

Become CISSP Strong

Voted Best Professional Certification at the 2021 SC Magazine Awards and "**The Next Big Thing**" by Certification Magazine.

SC awards 2021 WINNER

CERTIFICATION MAGAZINE
2021 TOP CERT
CISSP
(ISC)²
THE NEXT BIG THING

FIELD NOTES

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

Evaluating Your Cloud Service Provider

BY VINCENT MUTONGI, CISSP

SINCE THE ADVENT of cloud computing, enterprises have struggled with choosing the best cloud service provider based on their unique needs. Some organizations have tended to play it safe by signing up for "hybrid cloud" architecture where critical workloads hosting sensitive and critical data (e.g., databases, etc.) are left on-premises while less critical applications are migrated to the cloud. Others have gone all-in on either private or public clouds. Then there are differentiators among cloud providers themselves.

With so many options and providers, how can CISOs, CTOs and other IT managers choose the best cloud service provider for their needs? Here are some important evaluation criteria.

Shared Security Responsibility

Before engaging a cloud service provider, IT managers need to determine who will be responsible for their workloads. That's why it's prudent for organizations to read and understand a contract's Shared Security Responsibility model—how it applies to an IT manager's environment and how it meets specific use cases—before signing on with a cloud service provider.

Cloud Service Level Agreements (SLAs)

A service level agreement (SLA) is a contract that guides cloud performance and is negotiated by both the cloud services provider and the customer. The scope for SLAs includes availability of service (e.g., 99.9% uptime), governance, responsiveness, efficiency, etc. It's imperative that any SLA be clearly understood and legally reviewed before such an agreement is signed.

Security and Regulatory Compliance

This is the most critical factor to account for before an organization engages a cloud service provider. How does the provider secure the company's "crown jewels"? Does the service provider comply with appropriate regulations?

IT managers should choose a cloud service provider with a robust security structure that includes defense-in-depth, better access controls, authentication, auditing and monitoring, encryption, disaster recovery, etc.

Cost Considerations

Cost saving should not be limited to only dollar amounts spent on services; it should extend to technical support, training, infrastructure upgrades, etc., offered by the vendor.

IT managers should meticulously take time to evaluate each vendor's value proposition and avoid "vendor lock-in," in which it is difficult to switch vendors without paying penalties and operational costs. The goal here is for organizations to avoid sunk costs, maximize capacity and limit wastage of unused resources.

Cloud Provider's Track Record

Enterprises should take time to research and understand vendor profiles, core capabilities, strengths and weaknesses before deciding. Customers are likely to be more comfortable hosting their workloads with a provider that has a proven record of protecting its customers' data than with a vendor with a history of data breaches, legal issues and financial instability.

Cloud Security Strategy

To achieve a successful cloud security strategy that is in line with the tactical, strategic and operational goals and objectives of an organization, IT managers need to hire a cloud service provider that meets the organization's requirements. Investing in a holistic cloud security strategy *(see the longer version for specific details)* could be a panacea to most cloud migration woes. IT managers should restructure data and analytics to make better decisions that will drive overall enterprise-resilient sustainability and achieve competitive advantage. ●

Vincent Mutongi, CISSP, AWS Certified Security Specialty, is a senior enterprise cloud security engineer for Leidos Inc., a technology, engineering, and science solutions and services leader working to solve the world's toughest challenges in the defense, intelligence, civil and health markets. He has more than 20 years of cybersecurity experience supporting federal agencies in the Washington, D.C., area.

An expanded version of this article appears in the September Cloud Security Insights.

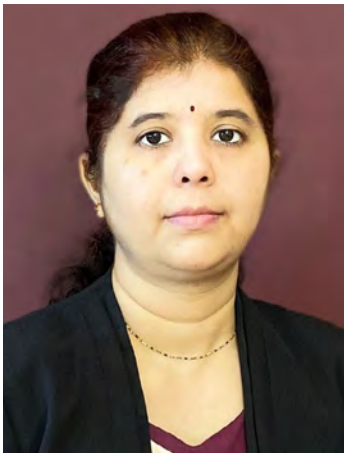
Photograph by Getty Images

Q&A

HOW I GOT HERE

Teach Your Children Well, Says One Lauded CISSP Parent and Volunteer

INTERVIEWED BY DEBORAH JOHNSON



HYMA PANDYARAM, CISSP

Pandyaram is an identity management specialist at Nulli - Identity Management in Alberta, Canada. She serves on the board of directors for the (ISC)² Alberta Chapter and leads its Safe and Secure Online program. In recognition of her work in cyber safety, Pandyaram was awarded an (ISC)² Global Achievement/James R. Wade Service Award.

Based on your volunteer work with elementary schools, what major misconceptions about being online persist among children and their parents?

A lot of children think online friends are trustworthy and are indeed who they say they are. They do not consider themselves potential targets and do not expect to encounter bad actors on children's websites and [in] game rooms. Children also think it's okay to share passwords with friends.

Meanwhile, parents are often not aware of their children's online activity. They may think that their kids are not old enough to get into trouble online, nor capable of browsing age-inappropriate content or exchanging information with strangers.

What techniques do you use to demonstrate the dangers and how children can protect themselves? What has been their reactions—any "aha" moments among the children?

The Center for Cyber Safety and Education has created excellent content in the Garfield education kits and videos. One particular slide in the privacy presentation shows a shady guy sitting in front of a computer and chatting with an elementary school kid. When I ask what is wrong with that picture, the children begin to think. I ask if the guy looks friendly, if the guy is a child. Does the kid in the picture know that he was chatting with an adult? Would that kid approach such a shady guy in real life? That one slide in my opinion is the most powerful because it delivers the entire presentation's message in one image.

Was there a specific event or person that led to your work teaching cyber safety to children?

When my son was three, he was a big fan of *Paw Patrol* and I wanted to buy him a Pup Pad as a gift. One evening I ordered it online from Amazon and left my iPad unlocked (as many parents do when they are busy raising little ones). Later, I started hearing email alerts on my phone. I was shocked to see that my innocent little boy had accessed my Amazon account and ordered three Pup Pads and a subscription to Amazon Prime! That made me think seriously about how accessible technology and the internet is, and how this can happen to any child.

I began teaching my son appropriate internet usage and discovered the Center for Cyber Safety and Education. I have so far reached out to 600-plus elementary school children via these awareness sessions, and I am very proud of that.

RECOMMENDED READING

Suggested by **Larry Marks**, CISSP, CISA, CISM, CFE, PMP, CRVPM, CRISC, CGEIT, ITIL, CDPSE

Medical Device Cybersecurity for Engineers and Manufacturers

BY AXEL WIRTH, CHRISTOPHER GATES AND JASON SMITH (ARTECH HOUSE, 2020)

The author of Recommended Reading did not receive financial compensation from the book publisher, nor a free copy of this book. All opinions are the author's alone.

THERE ARE MORE than 6,000 hospitals in the United States, according to the American Hospital Association. Most, if not all, rely heavily on networked medical devices.

In 2019, the Health Sector Coordinating Council issued a best-practice guide for medical technology companies that includes security-by-design principles offered by OWASP to mitigate risk early on in the device lifecycle. *Medical Device Cybersecurity for Engineers and Manufacturers* incorporates this guidance and provides the optimal controls to implement and manage the devices and protect their ecosystems.

A cyber incident to any medical device could be life-threatening. Authors Wirth, Gates and Smith provide the basic "blocking and tackling controls," which can be enhanced as the enterprise matures and adopts a further threat framework such as MITRE ATT&CK.

The authors look beyond medical devices to include the entire medical environment: "A cyber incident involving a hospital elevator impacts patient transportation, a change in temperature or humidity in the operating theater may force procedures to be delayed … the practices outlined herein are equally beneficial and can be applied to other care-critical, albeit not regulated devices."

Also addressed: risks to personal health information contained in the devices and protections needed against unauthorized extractions. This book is marvelous since it provides a roadmap for a stakeholder to structure their ecosystem to minimize the risks and threats presented by these devices.

(ISC)² Announces Newly Elected Board of Directors Members

FOUR SEASONED CYBERSECURITY professionals from Canada, the United States and Switzerland begin new terms on the (ISC)² Board of Directors in January 2022.

Rachel Guinto, CISSP, of Canada has worked for two decades in operations, governance and risk management. Prior to joining the industry, she worked in media and advertising.

Dan Houser, CISSP-ISSAP, ISSMP, CSSLP, is senior principal technologist for a global NGO/nonprofit where he develops and executes strategy for the information security program. He is a prior member of the (ISC)² Board of Directors (2009-2014).

Lori Ross O'Neil, CISSP, is the current vice chair for the board and a cybersecurity project manager at the Pacific Northwest National Laboratory.

James Packer, CISSP, CCSP, founded the (ISC)² London Chapter and currently heads information security at Education First in Zurich, having moved from KPMG in the U.K.

Pictured from left to right: Rachel Guinto, Dan Houser, Lori Ross O'Neil and James Packer.

The newly elected board members will join a 13-member, all-volunteer board that includes top cyber, information, software and infrastructure security professionals from around the world representing academia, private organizations and government agencies. Learn more here.

CHAPTER SPOTLIGHT

How to Build an (ISC)² Chapter During a Pandemic

BY JORGE OSORIO, PRESIDENT, (ISC)² MEXICO CITY CHAPTER

NINE YEARS AGO, when I became a CISSP, someone suggested that I join a local (ISC)² Chapter or start one. At only 28 years old, I found the idea of building a new chapter daunting—so seemingly impossible that I let the idea go.

Then, seven years later in 2019, with Mexico still without a single chapter, someone asked if I was interested in starting one from scratch.

"Yes, of course," I answered. But what I was really thinking was: "Am I crazy to do this? After all, I don't have any idea where to start." I talked to five other CISSPs and they each enthusiastically responded: "Let's do this!"

Launching a Chapter at the onset of COVID-19

It took two years to get the chapter officially formed. In September 2019 at the (ISC)² Secure Summit LATAM, I met two others interested in forming a chapter. We started a WhatsApp group to seed the idea for a Mexico City Chapter. Word spread quickly and a month later we held our first meeting to discuss requirements to build a new chapter. More than 100 professionals expressed interest in joining; however, not everyone was certified.

The low number of CISSPs would turn out to be one of three main challenges faced:

- Less than 360 people held an (ISC)² credential in Mexico, providing a very limited pool of people able to officially join our chapter.
- We needed to dispel myths about the CISSP examination and accreditation process so more of our peers could join our ranks.
- The pandemic pulled people away to focus on managing all of the disruptions COVID-19 caused in the early months.

So how did we respond to these challenges? We continued to meet monthly, even if we didn't have any update on our official request to form an (ISC)² Chapter yet. We used the time to hash out upcoming chapter musts: officer elections, vision and mission statements, objectives and goals, etc.

Next, we identified people with genuine interest

in building a chapter. More than 20 people expressed interest, but not everyone had the time to serve in an official capacity.

Finally, we created a vision and mission void of any ego and focused instead of creating a more secure world, even if some of us worked for competing companies.

Early accomplishments

We are now just six months old as an official (ISC)² Chapter, but we have already:

- Held a public expert panel.
- Conducted more than 20 meetings as chapter members.
- Provided a CISSP CBK update session for all the chapter members and three review sessions for anyone who wants to become a CISSP.
- Hosted a meetup with university students.
- Conducted five interviews for local newspapers, podcasts and other media.

Not too bad for being the new kid on the block in Latin America. Especially given we launched our chapter during what continues to be a difficult time for everyone, here in Mexico and elsewhere. The pandemic may continue, but so will our efforts to expand and help the organizations we all support. ●

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.

Photograph by Getty Images

(ISC)² Scholarships Highlight Diversity in 2021

EVERY YEAR (ISC)² and other sponsors like SAIC, Raytheon and KnowBe4 partner with the Center for Cyber Safety and Education to provide students with much needed support in pursuing a career in information security and cybersecurity. In 2021, a record U.S. $230,000 in financial aid and support was awarded to 70 recipients from around the world, bringing the total award by the Center to more than U.S. $1.7 million.

A deeper dive into the applicants and awardees of just the (ISC)² Scholarships paints an even better picture for the future of our industry:

- 73% of recipients were female. (Even if you remove the women's only scholarship that number is still 67%.)
- Winners came from every region (APAC, EMEA, LATAM, North America).
- 44% of scholarships were given to individuals residing outside of North America.
- 81% self-identified as a race other than White/Caucasian.
- More than 225 (ISC)² members volunteered 2,300-plus hours reviewing and judging over 864 (ISC)² scholarship applications.
- There were 1,136 total applications in 2021 when you include the other scholarships from KnowBe4, Raytheon, SAIC and the Richmond (ISC)² RVA Chapter.

Do you know someone who could use some help in 2022? Good news: The next round of scholarships opens on November 15. To learn more and apply go to https://iamcybersafe.org/s/scholarships. If you are an (ISC)² member in good standing and would like to volunteer to review applications, please contact Carole Boniface at scholarships@isc2.org.

(ISC)² Women's Cybersecurity Scholarship

Maryam Mohammadpour, Iran, Aalto University

I am so thankful to (ISC)² for choosing me and supporting me through my educational journey. It's a golden opportunity for me, and I feel like I'm finally one step closer to my goals. I want to inspire more women to join in the field of cybersecurity and show that women in technology are beyond compare.

I will use my skills to prevent any cyberwar between countries and make the world a better place to live. I want to make a virtual world a safer place and protect people against cybercrime. We can make the future bright with the help of each other. I believe no one is powerless when we come together.

(ISC)² Undergraduate Cybersecurity Scholarship

Mariel Klosterman, U.S., Dakota State University

Working full time to cover my living expenses and college tuition, I have little time for anything else. With this scholarship, I will have an opportunity to spend more time working on personal projects and volunteering in the community.

I desire to be a leader in the cybersecurity community and to help protect and defend my country from cyber threats. As a leader, I want to influence others, especially youth, to have a security mindset and empower them to do something about it. Throughout my years volunteering, I learned that experience or the authoritative position you have doesn't mean that you know what you're talking about. But if you put in the time and effort, you'll be miles ahead of the people who have become complacent.

Building on projects and working with the cybersecurity communities I'm part of, I will advance the field of cybersecurity by providing leadership, help and support to those I can reach.

(ISC)² Graduate Cybersecurity Scholarship

Collings Bunde, Kenya, Strathmore University

My dream is soon becoming a reality at Strathmore University's School of Computing and Engineering Sciences. This award gives me an opportunity to earn skills that will make me effectively contribute to the cybersecurity industry. Thank you for your generosity.

It's without a doubt that scholarship patrons like (ISC)² enable budding cybersecurity professionals unable to raise the school fees to pursue advanced cybersecurity courses, which later helps in a great way to define their careers in life. Your scholarship will help me earn a Master of Science in Information Systems Security.

Once again, thank you for the vote of confidence. I am, and I will always be, committed to my education and the cybersecurity industry to help solve global cybersecurity challenges. I will also make an effort to champion your scholarships in our local Kenyan universities as well as in our local cybersecurity communities.

MEMBER'S CORNER

It's Not the Drivers. It's the Road.

A plea for secure-by-default infrastructure software

BY RICHARD PAUL HUDSON, CISSP

This is an excerpt from the October Insights e-newsletter.

Richard Paul Hudson, CISSP, lives in Munich, Germany, and wrote this while employed at msg systems. He wrote a book to introduce laypeople to the world of information security (http://mybook.to/cybertwists).

IF A COMBINATION OF ROAD MARKINGS were consistently shown to confuse drivers, leading to avoidable accidents, the appropriate response would be urgent repainting rather than mere driver education. Yet in the world of application security, where the insecure default behavior of infrastructure software repeatedly causes developers to build vulnerabilities into their applications, the focus remains on increasing developer awareness rather than on mending broken tools.

Unlike drivers, junior programmers do not have to undergo any formal training before they start work. And while driving and programming both get easier with experience, the learning curve is far steeper when writing software.

It is so difficult to get one's first programs to work at all that the greenhorn developer has no attention left for secondary requirements like security. The crucial question is not why application developers are not better educated. It's why infrastructure software (programming languages, libraries, etc.) is still designed and documented in a way that leads new application developers to combine code and data within the same query string variable when there is virtually never a good reason to do so.

A solution for SQL injection vulnerabilities

When writing a program rather than working on an interactive console, it is always preferable to use one variable for the SQL code with bindings to a second variable or variables for the parameter data. This is true even in the relatively rare cases where the code of the SQL query is itself built up dynamically by the program.

The only conceivable situation in which a programmer would need to be able to submit code and data within a single string would be where the program is itself realizing an interactive SQL console, which is hardly an everyday requirement. *(See the October Insights newsletter for more details.)*

Going through the OWASP Top 10, equally simple potential improvements come to mind for some other issue types. For example, insecure deserialization would occur much less frequently if deserialization methods required programmers to specify by default the data type or types they were expecting to receive over the wire.

Infrastructure software (programming languages, libraries, etc.) is still designed and documented in a way that leads new application developers to combine code and data within the same query string variable when there is virtually never a good reason to do so.

A plan of action

Such basic steps are seldom taken because the developers of infrastructure software have a fundamentally different agenda from a security manager. They typically aim for elegance, versatility and usability. It is easy to see how these goals lead to infrastructure software exposing overly general methods that place an unnecessary security burden on the application developer.

Because the best infrastructure software is open source and freely available, no law could directly force it to become more secure. However, anyone developing any kind of

The most important users of infrastructure software include commercial enterprises, and if commercial enterprises were legally required to use only infrastructure software that is secure by default, its authors would soon start paying attention.

publicly available software is ultimately motivated by it being used.

The most important users of infrastructure software include commercial enterprises, and if commercial enterprises were legally required to use only infrastructure software that is secure by default, its authors would soon start paying attention. Most software is published and used globally, but legislation in any major jurisdiction—perhaps the United States, China or the European Union—would probably be sufficient to improve things everywhere.

Such legislation could reference a certification that programming languages and infrastructure frameworks would need to obtain before companies were permitted to use them. To keep down costs and, hence, industry resistance, it's imperative to set a strikingly low bar for any such certification. It would expressly not be appropriate to involve penetration testing, or in-depth source code analysis, or any sort of guarantee that software is secure. It would merely need to ensure that dangerous methods were named accordingly; that documented examples reflected good security practice; and that other such low-hanging fruit received minimum attention.

Over time, such measures, as simple as repainting road markings, would save the world billions of dollars annually and make the online world a much safer place.

(ISC)² | PROFESSIONAL DEVELOPMENT INSTITUTE

(ISC)² Members and Associates Are Talking About

PDI Online Learning

Build your cybersecurity skills anytime, anywhere. Earn CPE credits.

Cybersecurity professionals never stop learning and growing. That's why we are proud to continue offering rich educational content to satisfy your learning objectives.

From AI to cloud security, risk analysis to interpersonal skills, ransomware to firewalls and everything in between, we have a course for your current role and your career aspirations.

Our Immersive, Express and Lab courses are all available online and on-demand to fit into your busy schedule and all are eligible for CPE credits.

Don't miss out on this important (ISC)² member and associate benefit.

Get Started Now

40+ Self-Paced Courses: Express | Hands-on | Immersive

To receive communications when new courses are released, add *Continuing Education and Professional Development* to your preferred communications at isc2.org/connect.

A Glimpse of Hiring Challenges in 2022

BY DEBORAH JOHNSON

A paradox of 2022: U.S. Bureau of Labor statistics project growth in tech jobs while the shortage of qualified tech professionals continues, as reported in the most recent (ISC)² Workforce Study.

As a result, says workplace consultant and writer Heidi Lynne Kurter: "Talent is owning the market. They know how in demand they are and can make demands of how they work, where they work, the companies they want to work with. And their salaries. I feel that with any tech talent, the ball is in their court."

"The shortage of experienced talent in the cybersecurity space is daunting right now," acknowledges Dan Lohrmann, chief strategist and chief security officer at Security Mentor, Inc. based in Monterey, California. "It's gotten substantially worse during COVID-19, and part of that is people want to change. People have more opportunities, more choices and can be more selective."

As a result, among the hiring trends predicted for 2022, these three are getting a lot of play.

Photograph by Louise Roup

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

INCREASED SALARY DEMANDS

Risk management firm Willis Towers Watson, in a recent survey of 1,220 large and midsize companies, found that tech companies are projecting 3.1% raises to those working in technology, higher to top performers.

It's key to know the current pay bands, Kurter warns. "Have you measured your current salary against the current market? Are you flexible if you find talent outside of that pay range? How much are you flexible? What can you sacrifice? For a lot of positions now, people are getting hired at 30% more than they've been working at." And don't forget to review the benefits package, she adds.

REMOTE WORKFORCES CONTINUE

The pandemic expanded the definition of "workplace." A Citrix survey of 2,500 knowledge workers and human resource managers revealed that 88% of employees and 69% of HR directors agreed that flexibility in location and working hours will continue to be highly desirable.

"Some people won't apply for a job if it's not remote," Lohrmann says. "It may be, 'I don't want to commute. I don't want to get in the car and drive a half-hour or 45 minutes one way every day anymore.'" Similarly, companies also are changing their recruiting tactics because they can now go nationwide.

Look for revisions of workplace policies. "In terms of flexibility, there are companies that are establishing core working hours for this very reason. Set times or days for meetings," Kurter says.

UPSKILLING A PRIORITY

Retraining—or upskilling—current team members to take on higher-level assignments is a developing option. A CompTIA survey reported that 79% of 400 surveyed HR and development specialists are taking that approach.

Just make sure that you're training for the future, Lohrmann warns. "[Don't] just look at what's hot today, but what's coming up two, three years out, because it may take a year or two to get [workers] where they need to be."

ARM YOUR TEAM
to Secure the Enterprise

A strong security culture is key to minimizing security incidents and knowing exactly how to react when one occurs. The first step? Implementing a formal training and certification program to keep your cybersecurity team engaged and current on the latest threats and mitigation practices

Our eBook will help you develop a training plan that...

- Maps to your organization's specific requirements
- Helps retain (and attract) top talent amid a growing skills shortage
- Demonstrates operational value and investment in cybersecurity

Prepare for Tomorrow's Threats Today!

Get the FREE eBook

A look at implementation challenges for this popular security architecture concept.

BY MICHAEL PINHORN, CISSP

Zero Trust is among this year's most prominent buzzwords vendors use to sell solutions, often without considering the implementation challenges to achieving the promised goal: Keep malicious activity from infiltrating an organization's IT infrastructure.

Zero Trust is harder than it looks. Nonetheless, it is an important concept as it promises to overcome some of the growing problems of a conventional security architecture. It is still immature and requires a considerable amount of research to understand what it's about and how it could help with current and future challenges.

In essence, Zero Trust is the realization that it's increasingly difficult to keep bad actors out.

IMAGE BY JOHN KUCZALA

I facilitated workshops with the leadership team and other stakeholders and it became clear that there is a lot to consider before a Zero Trust strategy can be established.

A DECADE-OLD CONCEPT STILL EVOLVING

Zero Trust was proposed as a security concept in 2010 by analysts at Forrester. The Idea initially focused on micro-segmentation at the network level and least privilege access. This has evolved toward a de facto "framework" with strong emphasis on identity, constant verification of users and devices, and highly granular access to systems and information. "Trust no one" is the Zero Trust credo. The secure perimeter no longer exists.

As I started to research the subject, it would have been easy to rely on vendors' marketing and sales material. However, it quickly became apparent that their focus was on partial solutions, with very little on the preparation needed to move to a Zero Trust approach, or the way different products and services might be integrated.

I participated in several vendor-agnostic roundtable discussions with security professionals and found that the thinking around Zero Trust was underdeveloped. So, I went back to basics; in particular, I decided to focus on what can be achieved both short and long term.

NIST has recently developed valuable guidelines for a Zero Trust architecture, but this only deals with the conceptual or logical layer. The U.K. National Cyber Security Centre (NCSC) recently issued a beta release of its eight principles of Zero Trust and is planning to publish guidance for some of the most critical issues involving related migrations. The NCSC guidance provides more focus on implementation, but only in very general terms.

There are similarities in the two sets of guidance but also differences, which illustrate how ideas are still evolving. They both emphasize a need to have accurate information about users, devices, services and data, as well as dynamic, risk-based policies for resource access. You can't protect what you don't understand. In a complex organization, with a multitude of systems and business processes, information gathering is a major undertaking.

WELL THEN, WHY BOTHER?

Knowing the difficulty of implementing Zero Trust, the question becomes: Why bother?

Initially, I considered where we face the greatest risks today and how Zero Trust might help. Accounts being compromised through phishing attacks has been a big problem, but multifactor authentication has helped tremendously. However, we still face other internal and external attack vectors, and advanced persistent threats continue to grow. Is a fundamental change to our security architecture a better path than improving on what is already there?

After consulting with other members of my organization's Information Security Team, I concluded that at some point we would reach the limit of what's achievable using conventional approaches. I facilitated workshops with the leadership team and other stakeholders and it became clear that there is a lot to consider before a Zero Trust strategy can be established.

NO ONE APPROACH FITS ALL

A market review indicates many suppliers deliver one or more elements of a Zero Trust solution, such as identity governance, access management, mobile device management, next-generation firewalls and security monitoring. NCSC recommends choosing managed services designed for Zero Trust, preferably based on established standards, such as OAuth, OpenID Connect and SAML. The agency also advises to avoid reinventing the wheel, due to the cost, complexity and potential for error. However, NIST's market survey concluded that currently there is no established single set of terms or concepts to describe Zero Trust architecture components and operations. What is clear is that there is a lot for the customer to do.

There can be a high-level representation of a Zero Trust architecture solution, but the precise components of their integration is likely to evolve and vary from one organization to another. *(See Figure 1, p. 23.)* It is easy to be drawn toward technical solutions, but before even considering any vendor offerings, there is work to determine where the implementation challenges are and how they will be overcome.

We need to identify potential weaknesses in the end-to-end security architecture, taking into consideration current trends and how the landscape might look in five to 10 years' time.

PREREQUISITES FOR IMPLEMENTATION

Core to Zero Trust is a logical policy decision point along with policy enforcement points. Ideally, the decision point is a single, centrally-controlled service; however, this may not be possible if multiple enforcement points are needed. To work effectively, the policy points need accurate and current information about:

- Data and IT assets (value, sensitivity)
- Users (end users, admins, services, contractors)
- Workflows (existing workflows are likely to require at least some redesign)

Some Zero Trust solutions can help build a picture, but substantial work is required to document use cases, assets and access policies as a prerequisite to a robust enterprise-wide solution.

IMPLEMENTATION CHALLENGES

A heterogeneous IT architecture with decentralized management does not lend itself to a centralized approach. This is a key constraint to factor into strategy and implementation planning.

One approach is to make some components of a Zero Trust architecture available as a centralized service, while taking individual systems toward a Zero Trust architecture at an appropriate point in their lifecycle. A framework of Zero Trust standards and guidelines will help bring convergence over time. Further investigation is certainly needed to ensure all implementation challenges are identified before going too far.

The cost of Zero Trust is likely to be substantial for many organizations looking to implement it. In addition to the cost of components and services, a substantial investment in the preparatory work must be made. Discovery solutions can help, but they will not replace the need for understanding and defining processes, identifying appropriate boundaries for granular access, and the associated access control policies.

The use of personally-owned devices is another big issue for Zero Trust, especially in the era of COVID-19 and so many still working from home. Bring Your Own Device (BYOD) policies are long-established, predating the concept of Zero Trust and in some instances clashing directly with it. If users are routinely allowed to access systems using their own devices, the key principle of verifying user and device status becomes a lot harder to apply.

WHERE TO START?

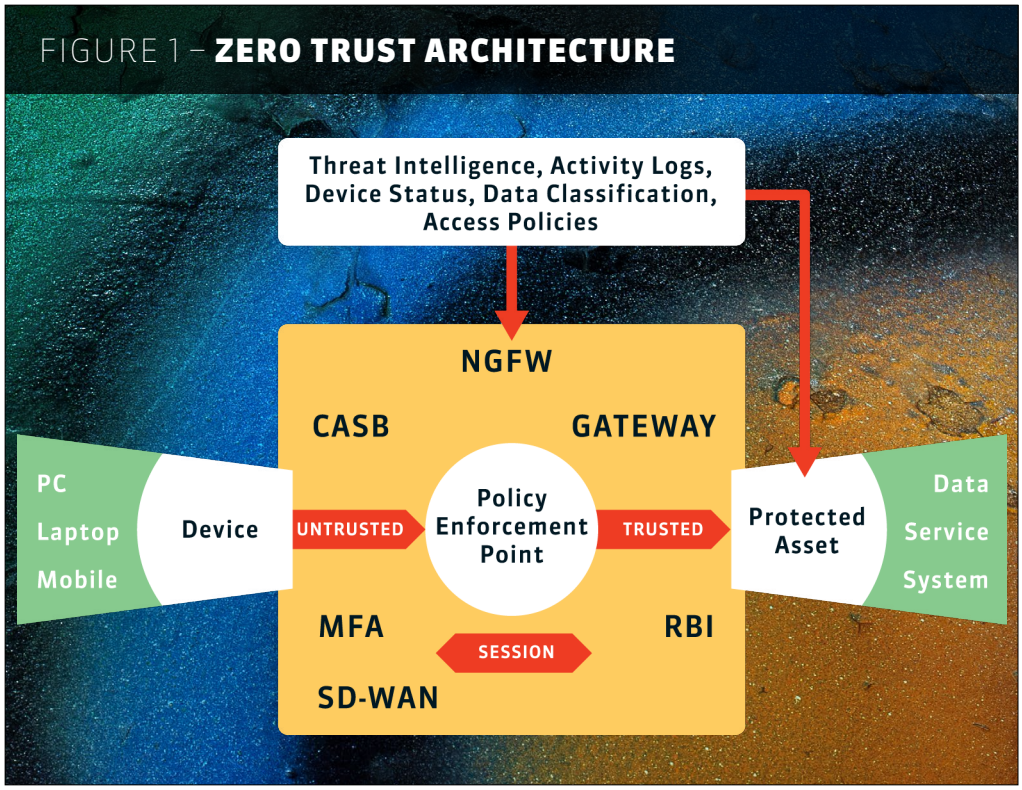
According to NIST, most enterprises embarking on a Zero Trust strategy will continue operating in a combined Zero Trust and perimeter-based mode for years while investing in IT modernization initiatives and improving business processes. Let me repeat that: Expect bimodal operations for *years*.

We have yet to decide which areas to take forward first. There is a degree of consensus that this should start with an assessment of risk; in other words, identifying the biggest current and future threats to critical assets. Beyond that, we need to understand which Zero Trust architectural components best address risk and which bring other benefits.

Remote working and cloud services are often cited as risk areas that can be mitigated using Zero Trust solutions. But are these where the highest risks lie? Not necessarily, particularly with multi-factor authentication in place. That said, a Zero Trust architecture may provide a more cost-effective approach to securing remote access and cloud services than current controls.

My view: We need to identify potential weaknesses in the end-to-end security architecture, taking into consideration current trends and how the landscape might look in five to 10 years' time. This should encompass people, processes and technology.

FIGURE 1 – **ZERO TRUST ARCHITECTURE**



Infographic by Robert Pizzo

QUICK WINS

Attaining Zero Trust is a long journey and needs a strategic approach, but I see early benefits by focusing on specific areas rather than waiting for every facet to fall into place. Create a sound implementation plan that draws on internal (or third-party, as needed) expertise in multiple areas. By understanding risks, challenges and constraints within the organization, that plan will be based on a good understanding of what currently is probable and what will be possible. Zero Trust capabilities continue to evolve and will vary in effectiveness and integration with legacy systems. Furthermore, as there currently is no established standard or model for Zero Trust, it will take time to assess offerings fully. But such a step is essential to avoid making decisions that may be difficult to unpick later on.

THE ZERO TRUST JOURNEY CONTINUES

We are on a journey that will take many years to complete. Zero Trust is about a fundamental change to the extant security architecture and extensive preparation will be needed to implement an effective solution. If implemented badly, it will likely weaken rather than enhance an organization's security posture.

The number of Zero Trust products and services available is vast, with some big claims around their benefits. Perhaps "Trust no one" should be applied to such claims, as well as to the network. Ultimately, we have to ask ourselves what risks we need to mitigate and where Zero Trust can deliver the most value after taking into account effectiveness, ease of integration and implementation efforts.

Michael Pinhorn, CISSP, is the head of Information Security Governance, Risk and Compliance for the University of Oxford.

You Can Train Like This...

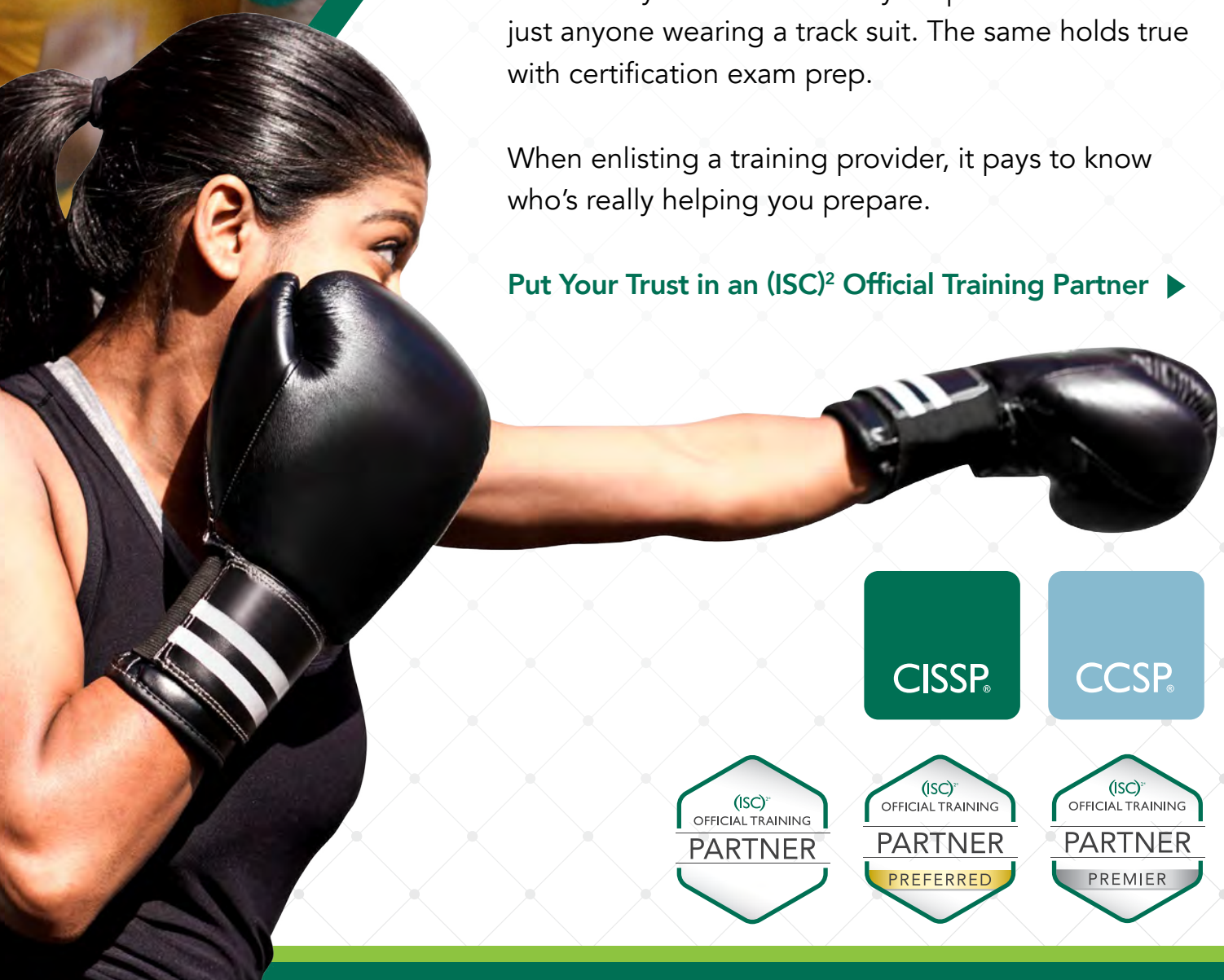
or with (ISC)² Official Training Partners

You Can Train Like This!

(ISC)² certifications are highly regarded certification in the cybersecurity industry, so it's not surprising that countless training companies offer exam prep for them. But you wouldn't trust your personal fitness to just anyone wearing a track suit. The same holds true with certification exam prep.

When enlisting a training provider, it pays to know who's really helping you prepare.

Put Your Trust in an (ISC)² Official Training Partner ▶



CISSP®

CCSP®

(ISC)² OFFICIAL TRAINING PARTNER

(ISC)² OFFICIAL TRAINING PARTNER PREFERRED

(ISC)² OFFICIAL TRAINING PARTNER PREMIER

Infection Control

Pandemic privacy remains a major healthcare security issue, but so do vulnerable implantable medical devices, telehealth platforms and remote-access software.

BY SHAWNA McALEARNEY

SINCE WORLDWIDE COVID-19 OUTBREAKS BEGAN IN LATE 2019, healthcare privacy and security have taken near-center stage at various times during the pandemic. But that preoccupation with protecting patient health information tied to infection and vaccination rates has allowed another major security risk to fly lower on the radar: the harmful hijacking of implantable medical devices (IMDs) for conditions as common as hearing loss and diabetes.

"COVID-19 has vastly increased attack surfaces, impacting organizations and healthcare," says Aisha Berry, principal consultant, CyberSec Health Consulting. "The focus was primarily on sustaining lives and preventing the spread. Simultaneously, focus on medical technology decreased, not understanding how technology is a part of patient safety."

ILLUSTRATION BY PETER AND MARIA HOEY

"Patient teaching is necessary for watching for infection at the surgical site, functionalities and implantable device settings. And it's crucial to establishing and maintaining proper cybersecurity practices to prevent malware and ransomware attacks."

—Aisha Berry, principal consultant, CyberSec Health Consulting

Since their inception, IMDs have steadily evolved. Now many use Bluetooth to install updates and connect to mobile applications, online platforms and the cloud to improve patient care. More than a decade ago, a Black Hat conference speaker showed how to tap into and modify wireless control signals sent to his own insulin pump to change his dosage. Later research showed that wireless heart devices could also be hacked.

"These smart devices are increasingly connected by two-way communication protocols, and have embedded memory, mixed-modality transducers and the ability to adapt to their environment with artificial intelligence (AI) algorithms," says Alan Michaels, director of the Electronic Systems Lab at the Hume Center for National Security and Technology at Virginia Tech. "They represent significant concerns to the security of protected data, while also delivering medically necessary benefits to their users."

'PATIENT TEACHING IS NECESSARY'

Patients can and should be trained in basic cybersecurity for their devices in much the same way as they are expected to watch and report signs of infection.

"Patient teaching is necessary for watching for infection at the surgical site, functionalities and implantable device settings. And it's crucial to establishing and maintaining proper cybersecurity practices to prevent malware and ransomware attacks," says Berry. "With the emergence of [modern] pacemakers and insulin pumps, penetration testing should always be mandatory before implanting medical devices.

"In addition, IT security professionals should be treated as part of the healthcare team and assigned to patient data. Furthermore, if the implantable device does not meet the criteria per penetration test results, postpone the surgery if necessary."

Berry suggests the most substantial ROI will be found in patient education, as well as mandating continuous cybersecurity education and cyber hygiene evaluations for healthcare teams involved in the patient's care and viewing healthcare and cybersecurity as two parts of the same whole. "Healthcare teams (need to) focus on device functionality, automating cyber hygiene to endpoints to harden security and activate anti-malware and firewalls, and track device security status and misconfigurations to prioritize responses."

Experts fear that IMDs, from pacemakers to hearing aids and asthma monitors, could be weaponized to leak classified data, location information and more.

This is particularly relevant in the case of sensitive compartmented information facilities, or SCIFs, where sensitive and classified information from internal sensors, microphones and transducers is worked on and discussed.

"First is the potential and concern of a cleared individual being blackmailed by virtue of third-party control of their embedded medical device," says Michaels. "Consider the scenario of a pacemaker that could somehow be remotely controlled to emit a charge, hypothetically on a periodic schedule unless a wireless 'skip charge' command was given. It's feasible to believe that someone may freak out and be compelled to make poor choices concerning classified information. This is an overt attack-the-person scenario."

Secure facilities often have policies that require visitors and employees to leave phones, fitness trackers and other personal electronic devices at the building entrance. But IMDs are medically necessary and rarely detachable.

Smartphones are the lowest risk because they are left outside the facility … smart glasses and smart watches are a bit riskier, but hearing aids, asthma monitors, pacemakers and insulin pumps top the list of risky devices, says Michaels.

"The external devices, which tend to be battery-powered or rechargeable and have more wireless capabilities, represent the highest risk," he adds. "At present, I think those risks are reasonably limited, yet it's a niche technology race that could quickly outpace the average facility security officer's knowledge and experience base using purely commercial technology."

One of the threats he envisions "is a scenario where a more capable device, such as an

"Policy should be proactive in addressing tech from five years from now, rather than consistently being five years behind."

—Alan Michaels, director of the Electronic Systems Lab at the Hume Center for National Security and Technology at Virginia Tech

externally worn insulin pump that contains open source software, is configured to record speech inside a secure facility and subsequently download the raw content via the internet. The user will not have had any intent or insight to the potential exfiltration of classified information. This is a surreptitious attack-the-device scenario."

It is a legitimate concern. The U.S. Director of National Intelligence's Technical Specifications for Construction and Management of SCIFs defines known threats, including IMDs, and is meant to be a "living" document that evolves over time with changes in technology. Not long ago, the Food and Drug Administration appointed Kevin Fu to serve as its acting director of medical device cybersecurity, leading the agency's efforts to ensure the safety and security of medical devices.

According to the specifications noted above, "As a minimum, the medical device must be reviewed to determine any technical security issues introduced by the device." Such a policy, however, can conflict with human resource policies and applicable laws like the Americans with Disabilities Act. Based on U.S. workforce demographics and estimated IMD hosts, Michaels estimates there are approximately 100,000 potentially affected users in the security space that could be targeted.

However, the number of those affected may be far higher when you realize that not only IT and security professionals work around sensitive information. In *Implantable Neural Prostheses 2: Techniques and Engineering Approaches*, Guangqiang Jiang and David Zhou maintain that 8% to 10% of the population in America and 5% to 6% of people in industrialized countries have an implantable medical device.

MITIGATION WITH LIMITED CONTROL

How can you mitigate such a threat when you legally have no control over the device?

Some experts have proposed external mitigations, including:

- IMD permission lists considered secure enough
- Random inspections of device settings
- Ferromagnetic detection to identify implants
- Device data wiping upon exit
- Physical signal attenuation
- A form of "airplane mode" software
- Signal jamming

Many of these have drawbacks, including battery drain on the devices, being overly complicated or cumbersome, or requiring protected information about the devices.

"We want to protect the information and support individuals, but there is a point in which you probably deny entry," says Michaels, "and it may be coming sooner than people think. Policy should be proactive in addressing tech from five years from now, rather than consistently being five years behind."

Healthcare organizations offer a far easier target in their increasingly widespread use of the cloud and the internet of things (IoT) for collecting diagnostic information and maintaining patient records, or even dispensing medication. The industry is far more conservative with technology advances, simply because the stakes are much higher if a health system gets it wrong. As a result, incompatible legacy systems and latent vulnerabilities are common.

"A paradigm shift is needed in healthcare, emphasizing that effective cybersecurity measures play a part in patient safety," says Berry. "State and federal agencies should prepare and mandate healthcare facilities and providers implement cybersecurity practices. Including continuous education and positive leadership is being proactive and placing patient safety in its best interest."

"They don't see the value in implementing a security program. For smaller organizations it comes down to pricing and the misconceptions that it is expensive to be secure and that an attack would never happen to them."

—Debi Carr, CEO, DK Carr and Associates

A hesitancy within healthcare to embrace new technologies also stems from a near-constant need to cut costs, particularly when a rise in COVID-19 cases reduces elective procedures that generate revenues. Physicians and staff must redirect resources to COVID patients, rather than treat those with ongoing, non-life-threatening medical needs.

"Many private practices have an ad hoc security budget and often they don't see the value of working with an IT partner," says Debi Carr, CEO of healthcare security specialist DK Carr and Associates. "They don't see the value in implementing a security program. For smaller organizations it comes down to pricing and the misconceptions that it is expensive to be secure and that an attack would never happen to them."

Telehealth use—along with associated IoT devices—sharply increased once COVID hit, with platforms adopted quickly instead of being exhaustively vetted for cybersecurity and privacy risks, says Carr, an HCISPP.

"At the start of the pandemic, many practices used whatever means they could," she explains. "There are many good platforms; the problem occurs when the users prefer to take the 'convenient' way instead of the secure way. Now, for many, telehealth has become an integral part of their practice, so they are starting to look at more secure platforms and measures."

EXPLOITING HEALTHCARE PROVIDERS' REMOTE ACCESS

Carr says that many of the earlier attacks she saw were the result of doctors using free remote software to access their practices.

"At the start of the pandemic, many went home to work, but still wanted to connect to their practices and offices. Threat actors were elated," she says. "One client was using RDP, and the threat actor was able to get in and was in the network for 48 days. On the 49th day, they used their escalated knowledge, exfiltrated patient data, deleted the on-premesis and cloud backup accounts, encrypted the data and asked for 5 Bitcoin to show that they were serious. The threat actor posted the patient data on a web page [and shut the] doctor down completely for three and a half weeks."

In another case, an attacker sneaked into a system to launch malicious code. "It came down to the doctor being greatly inconvenienced for about seven weeks and paying restoration expenses of $54,000. This included hiring an IT/MSP—the doctor had been doing his own IT—and buying a new server, wiping and reconfiguring workstations, etc.," she recounts.

"Doctors doing [their] own IT sadly happens a lot because they don't want to pay someone to do what they think they can do," the consultant explains. "They just don't see the value and they continue to have the mindset that it will never happen to them. They honestly believe they are doing the right thing, but, sadly, most small healthcare practices do not have any administrative controls, a disaster plan, etc."

Carr has seen the threat landscape for healthcare change for the worse. "In the beginning of 2020, in most of the attacks we saw, the threat actor would deploy code that encrypted, posted a note and was done—no exfiltration, just inconvenience. By October we were seeing data exfiltrated, posted to websites, patients contacted, etc. The attacks have become more aggressive and more sophisticated."

Now the attackers remain in the system for long periods of time gathering information, including admin credentials, and then launch their attack.

"In the threat landscape that we see today, all healthcare entities, large and small, must prepare for a cyberattack," says Carr. "It is not a matter of *if* but a matter of *when*, and the when can be very expensive."

Shawna McAlearney is a freelance writer based in Las Vegas and regular contributor to *InfoSecurity Professional* magazine.

COPING WITH LOSS

The stages of incident response and grief are similar, according to an (ISC)² member who transitioned from social work to cybersecurity. **BY MARC MUHER, CISSP**

HAVING A FRAMEWORK—clear, repeatable and defined steps to operate within—is one of the most important parts of working in cybersecurity. It separates a professional from an amateur.

In incident response, the framework we often work from is called PICERL, which is shorthand for preparation, identification, containment, eradication, recovery and lessons learned. It allows incident responders to follow definitive steps to meet a variety of threats based on years of best practices and practical knowledge.

Cybersecurity isn't the only profession with frameworks. I was fortunate enough in a prior career to study and practice social work, which deals with the response of the mind to both inside and outside forces that affect it. In social work, we deal with frameworks as well, and one of the best known is the Kübler-Ross model, or five stages of grief.

ILLUSTRATION BY ARD SU

While Kübler-Ross contains five stages and PICERL contains six, we as cybersecurity experts know that preparation is a rare luxury.

TABLE 1 – **THE FIVE EMOTIONAL STAGES OF GRIEF**

In the 1960s, Swiss-American psychiatrist Elisabeth Kübler-Ross identified how those facing a terminal illness engaged similar emotions, though not always in the same progression, in processing their impending deaths. Today we apply the same five stages to those who must survive the loss of a loved one, as well as other traumatic events, such as a job loss or divorce.

Denial. In this stage, the individual believes there's been a mistake and cannot accept the reality of results.
Anger. When reality does set in, the individual is outraged to be among those forced to suffer such a fate.
Bargaining. The person looks to alter an anticipated outcome through belief in lifestyle changes, if only to buy time to find a cure or hit a major milestone, such as a child's graduation.
Depression. Despair at a different future than planned leads an individual to withdraw from others while they silently mourn.
Acceptance. In the final stage, the individual is ready to face a new future, and survivors prepare to move on.

Source: Psycom

FIVE STAGES OF GRIEF

Elisabeth Kübler-Ross was a Swiss-American psychiatrist who identified five reactions the mind typically employs to cope with a traumatic event, such as a cancer diagnosis or loss of a loved one. The Kübler-Ross model defines five such stages: denial, anger, bargaining, depression and acceptance. *(See Table 1, above.)* The similarities between the stages of both the Kübler-Ross and PICERL models can give us, as cybersecurity practitioners, insight into how to deal with the inevitable grief of the human condition.

While Kübler-Ross contains five stages and PICERL contains six, we as cybersecurity experts know that preparation is a rare luxury. Even when we have time to prepare, an actual incident often renders that preparation useless. Thus, we will also ignore that part of the framework.

MAPPING GRIEF TO A CYBER EVENT

Identification is the first step that we take when dealing with an incident. Knowing what the problem is, whether it be ransomware or a natural disaster causing loss of data, is very important but perhaps not as important as verifying that an incident has taken place.

Cybersecurity professionals often deal with a staggering number of alerts and use our knowledge and experience to sift through, verify and identify the issue. Likewise, the denial stage allows the mind to perform a similar function as we verify a correct diagnosis or bad news. It allows the person to begin to cope with an issue by making sure that the issue is occurring and prevents the trauma of grief where it may not be needed.

Containment is the next step in the incident responder's toolbox. After finding the issue, we seek to isolate it to prevent further damage. Disabling network connections, terminating suspicious access and switching to backup systems are all methods of containing an issue once it has been verified.

This is no different than the grief reaction of anger. Anger lets us sift through the complex emotions and become upset with the appropriate issue. Using anger allows the mind to identify what is causing us grief. Just as different techniques are used when dealing with

a security incident until the correct one is found, anger lets us find the correct target. It's often a difficult stage of grief, as the affected person can lash out unexpectedly—just as cybersecurity professionals are met with the challenges of containment: mass password resets, network cutoffs, or anything else to stop the spread.

Just as incident response rarely goes exactly as planned, so too are we imperfect practitioners of grief.

Eradication is the next step in dealing with a cybersecurity incident. Once the problem is known and contained, eliminating its source is required in order to begin the recovery. This requires a level of introspection and a plan to rebuild systems and install new defenses to stop future intrusions.

Bargaining holds a similar place in the grief cycle, helping us come to terms with a pending or recent loss. Bargaining allows us to shape our understanding of the problem and minimize the parts of our lives that it has affected. Promises to ourselves, whether to eat better, seek out medical care earlier, or spend more time with our remaining loved ones are ways that our mind seeks to route around the grief.

Recovery is often the most difficult stage of dealing with a cybersecurity incident. We tried to fix the problem; now we need to return everything to its previous state. This often involves new practices and workflows as complex systems are replaced and can sometimes be best described as "trying to put the toothpaste back into the tube."

Depression is the mind attempting to do just that, as we try to come up with a new way to function even though a great loss has occurred. Depression is a natural reaction following a traumatic event; it allows the time that we need for introspection and soul searching, which helps us deal with a different future than the one we imagined.

Lessons learned. Eventually, systems are restored, and new protections are put in place following a disruptive cybersecurity event. This is the time to step back and reflect on what worked, what didn't, and what can be improved going forward.

Acceptance is the mind's way of doing that as well, as we adapt to a new normal without a loved one or continued treatments. Be aware that some of us never fully move on from the acceptance stage of grief. They may continue along in life, but they never fully recover from the loss. So too do some of us fail to fully embrace the lessons learned and instead slide back into bad habits that contributed to a breach.

STEPPING BACK TO MOVE FORWARD

Just as incident response rarely goes exactly as planned, so too are we imperfect practitioners of grief. We experience it and it changes us, just as networks are changed in response to an incident.

The knowledge of these stages is difficult to see while we are experiencing them, which is why organizations often use outside consultants for incident response, and people may seek out the help of friends, counselors and other mental health professionals.

Some organizations never eliminate threats from their systems, or as has been seen with some ransomware events, a business may simply close rather than try to rebuild and recover. Sometimes people never fully recover from a traumatic life event, holding on to denial, anger, bargaining and depression, and we can fixate on these coping strategies by incorporating them into our personalities.

What's important to remember is that there is no set timeframe to move through the anticipated stages. Incident responses will vary, and everyone works through their grief at their own pace. ●

Marc Muher, CISSP, CEH, MSc, MSW, is a former clinical social worker who works in information security for a large municipality.

NEWSLETTERS WEBINARS PDI BLOG COMMUNITY MAGAZINE EVENTS CHAPTERS RESEARCH

WELCOME TO BUZZWORTHY, A ROUNDUP OF WHAT'S BEING SAID AND HEARD AROUND (ISC)² CHANNELS

"The best way to train for a DDoS scenario is to turn on prevention."

—Ameet Naik, product marketing, Cloudflare, (ISC)² Security Briefings webinar, "DDoS Trends and the Ransomware Threat"

"If we don't know what's there, how can we protect it? And that might seem like the most simplistic comment … but that's exactly what we are asking our security teams to do. … We found that 99% of cloud security failures are happening because of a customer's fault. We are trusting in that cloud security model."

—Ell Marquez, Linux and security advocate, Intezer Labs Ltd., (ISC)² Security Briefings webinar, "Someone Else's Computer: On-Prem vs. Cloud Security"

"A major driver of cloud adoption is cost savings. Everyone on the security team must clearly understand the cost implications of cloud migration—both benefits and potential pitfalls."

—Vincent Mutongi, CISSP, Cloud Security Insights' "What Your CISO and/or SOC Shouldn't Miss in Evaluating a Cloud Service Provider"

"Data is becoming the new commodity. It is the high-priority target for criminals. We all know that the new war today is fought in the cyber domain. Ones and zeros are far more disruptive than actual kinetic bullets and missiles, and criminals know this."

—Justin Fier, director of cyber intelligence and analytics, Darktrace, (ISC)² Security Briefings webinar, "Darktrace #2: Cyber AI and Protecting the Innovation that Drives Transportation"

"Professionals say that having a mentor to shadow and rely on for guidance in their first three years in the field was invaluable for their success. Encourage your senior team members to take on this role of leadership."

—2021 (ISC)² Cybersecurity Career Pursuers Study, Build Resilient Cybersecurity Teams

CENTER FOR
CYBER SAFETY
AND EDUCATION™

HEROES GIVE THE GIFT OF CYBER SAFETY

You can help protect children and families with a one-time donation, monthly or annual contribution or even by rounding up your change.

Through generous contributions, the Center is able to provide internet safety education, scholarships and cyber research to the global community. Your gift will help make the cyber world a safer place for everyone!

Be the hero your community needs—donate to cyber safety education!

Learn more: **https://IAmCyberSafe.org/Give**