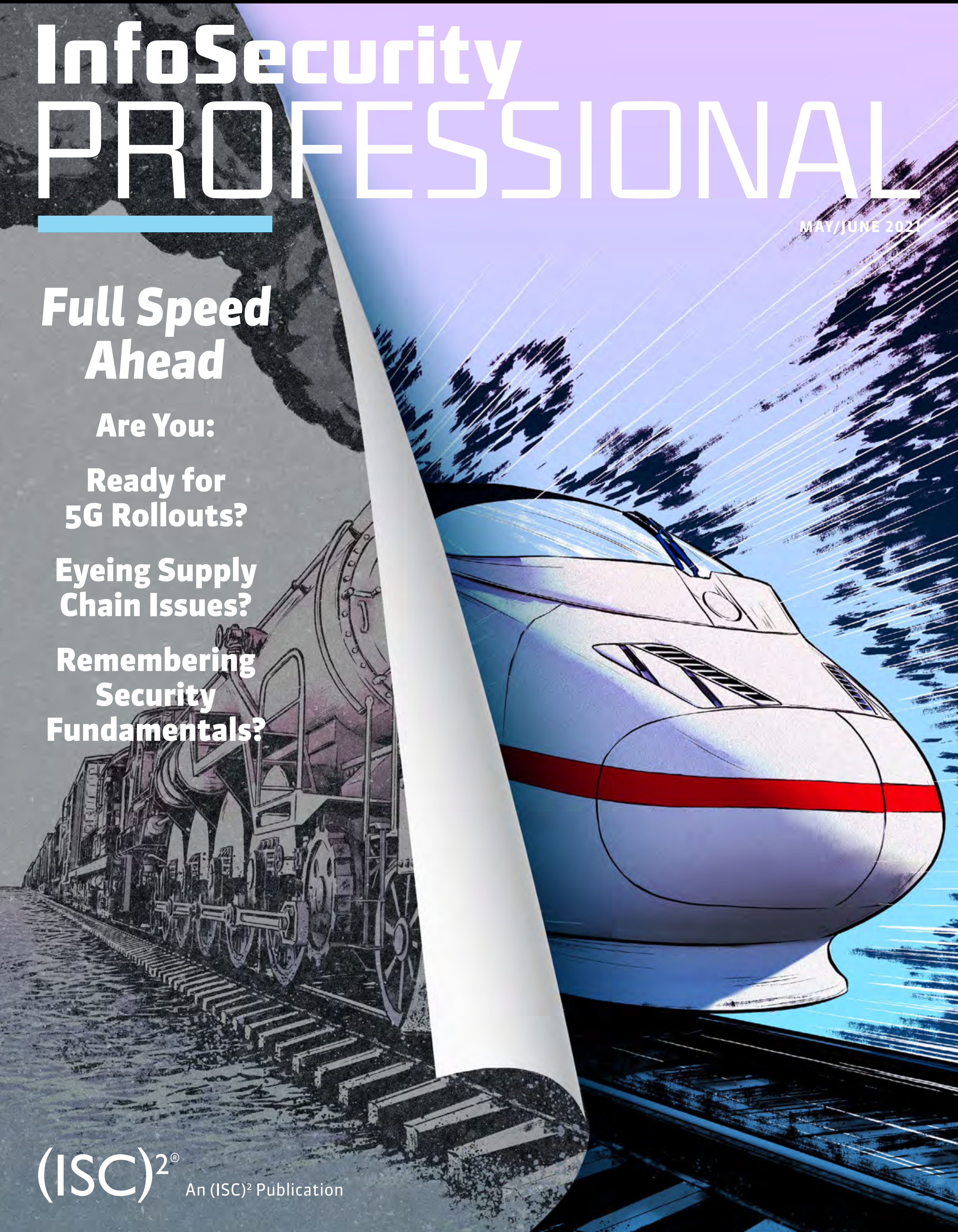
TIPS TO AVOID HIRING THE WRONG PEOPLE

InfoSecurity PROFESSIONAL

MAY/JUNE 2021



Full Speed Ahead

Are You:

Ready for 5G Rollouts?

Eyeing Supply Chain Issues?

Remembering Security Fundamentals?

(ISC)²®
An (ISC)² Publication

(ISC)²

2021 SECURITY CONGRESS

(ISC)² Security Congress 2021

Every year, Security Congress brings together a global community of cybersecurity professionals. Our goal is to provide you with invaluable education, career advancement opportunities and everything you need to best secure your organization.

Plan to join us for our first hybrid conference!

What to expect:

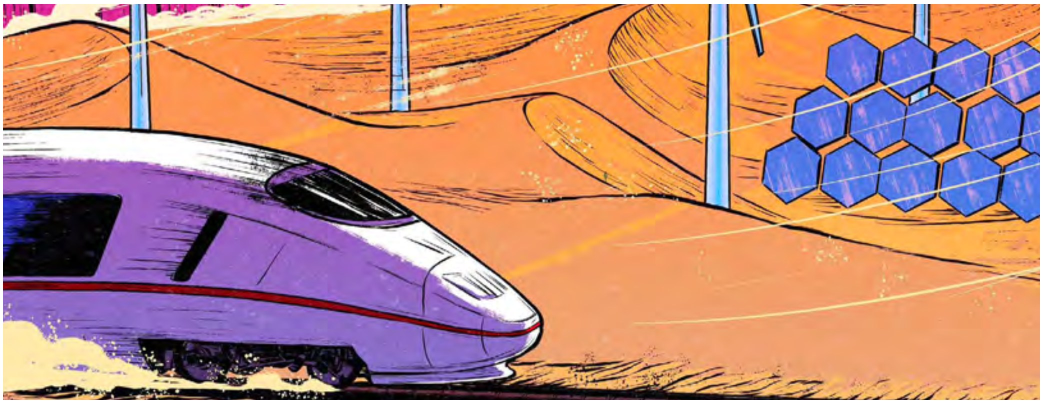
- Enriching and educational content from keynotes and speakers
- Networking and engagement activities
- Career Center
- CPE credits for (ISC)² members and non-members
- (ISC)² Global Achievement Awards Honoree Recognition
- Exhibition Hall

Be on the lookout for more info on registration!

GET MORE INFO

October 18-20, 2021 | #ISC2Congress

CONTENTS ▪ MAY/JUNE 2021 ▪ VOLUME 14 · ISSUE 3



Long before SolarWinds, attackers aimed their arsenals at vulnerabilities within supply chains.

PAGE 27

FEATURES

Cover and above illustration by Raul Allen

DEPARTMENTS

LEARN HOW TO EARN FREE CPE CREDITS

TAKE
COMMAND
WITH CCSP

EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

Making More Room for Content that Matters

ONE OF THE MORE frustrating parts of writing for *InfoSecurity Professional* is all of the good stuff that gets left out due to limited space and today's attention spans. Inevitably I'll conduct a number of interviews that span hours and then whittle down those talks to the most salient points.

Now there's a way to add back some of what's left out. Beginning next month, I'll be hosting a quarterly (ISC)² webinar focused on the issues—both of the day and within this magazine. It could center on a single subject or expand on something we wrote elsewhere, like companion e-newsletters *Insights* and *Cloud Security Insights*.

If you haven't watched an (ISC)² webinar lately, you should. Not only is there such a rich library of content, but the frequency keeps growing and format expanding to include video of speakers/presenters. Longtime moderator Brandon Dunlap brings together subject matter experts for 60-minute roundtable discussions for (ISC)² Think Tanks. Everything from deep dives to bite-sized topics fall under the different flavors of Security Briefings. The Briefings are sometimes organized by regions, though topics tend to appeal to cybersecurity professionals everywhere.

As I write this, there's a Think Tank coming up about managing risk within your supply chain. I highlight that one, which will be available for playback by the time you read this, because we also have content in this issue around supply chain security, including one story focused on what's next for those impacted by a particular software supplier you might have heard of (*cough* SolarWinds *cough*). CISSPs from Grand Canyon Education return to remind us to not pass over fundamentals when adopting the latest cool tools. And then there's my cover story on 5G security.

I'll expand on 5G vulnerabilities and threats in a June 15 webinar with some of the experts I interviewed. It's a relevant topic, whether you're a consumer concerned about being tracked, or part of a team that must figure out how to protect millions of machines connecting and communicating within a hypercharged ecosystem. I hope you'll join me live or listen later when the presentation is available on demand. Until then, thanks, as always, for helping keep us all safe. ●

Photograph by Louise Roup

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

CONTRIBUTORS

Shawna McAlearney is a freelance writer in Las Vegas who has covered the information security industry for more than 20 years. Her feature on supply chain security was inspired by a session at last year's Black Hat conference, which she attends annually.

Daniel Addington provides management, leadership and technical guidance for the security team. His professional and career interests have focused on the strategy, design and deployment of secure, critical information programs, systems and data across various organizations and industries including aerospace, defense and education. He enjoys spending time outdoors with his family, teaching, and running purple team exercises and research in his home lab.

Ed Brown leads IT Security Engineering, responsible for the firewall and email gateway ecosystem, along with coaching, mentoring and training new staff and students to cultivate new cyber warriors. When not working, Ed enjoys photography, hiking and camping and dreams of combining the three in retirement.

Mike Manrod currently serves as the Chief Information Security Officer, responsible for leading the security team and formulating the vision and strategy for protecting students, staff and information assets across the enterprise. He is also a co-author/contributor for the joint book project *Understanding New Security Threats* published by Routledge in 2019. When not exploring the implications of the rapidly evolving threat landscape, he spends time playing video games with his kids, practicing martial arts and cooking.

Your Skills Have Never Been More Important

The cyber world needs your expertise. But the security leaders of tomorrow require a broad set of skills that job experience alone does not arm you with.

The globally recognized Certified Information Systems Security Professional (CISSP) credential help you prepare for real-time incidents and stand out as the expert employers are looking for. Download the white paper to discover the 9 key characteristics of effective leaders in the field.

Are you ready to stand out as an expert?

9 TRAITS

(ISC)² 9 Traits You Need to Succeed as a Cybersecurity Leader

Cybersecurity is an important factor for business prosperity

More than 50% of the world's population is now online[1]. Approximately one million people join the internet[2] each day, while two-thirds of humanity own a mobile device[3]. What is known as the Fourth Industrial Revolution (4IR) is already bringing tremendous economic and societal benefits to the world.

Smart technologies have enormous potential to improve both human life and the health of the planet. However, many new challenges and risks have also surfaced. Cyberattacks have become a common hazard for individuals and businesses. Fifth generation (5G) networks, quantum computing and AI are creating not only opportunities but also new threats.

The need for strong cybersecurity is apparent: an organization falls victim to a ransomware attack every 14 seconds[4], while one successful attack could force businesses to a complete standstill for weeks, or even to shut entirely.

Organizations should not view cybersecurity as just another IT expense for protecting against imminent cybersecurity threats. The fact is that cybersecurity can also play a vital role in driving business growth[5].

Long-Term Risk Outlook

Top 10 risks by likelihood and impact over the next 10 years

Figure 1: Long-Term Risk Outlook: Top 10 risks by likelihood and impact over the next 10 years[6]

CISSP®

Certified Information Systems Security Professional

An (ISC)² Certification

CERTIFICATION MAGAZINE

2021 TOP CERT

CISSP

(ISC)²

THE NEXT BIG THING

GET YOUR COPY

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/May-June-2021

Learn about more opportunities to earn CPE credits.

ADVERTISER INDEX

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

(ISC)² Security Congress 2021	2
Expert Security to Command the Cloud	4
Stronger Cybersecurity Starts with CISSP	6
SEM	9
(ISC)² Certification Training for Your Team	10
(ISC)² EMEA at the Cybersecurity Festival	15
(ISC)² Professional Development Institute	17
Center for Cyber Safety and Education	19
Penn State	25
Reciprocity Labs	26
CrowdStrike	40

InfoSecurity Professional is produced by Twirling Tiger® Media, 10 Brassie Way, Mashpee, MA 02649. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)²® on the issues discussed as of the date of publication. No part of this document print or digital may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of (ISC)². (ISC)², the (ISC)² digital logo and all other product, service or certification names are registered marks or trademarks of the International Information Systems Security Certification Consortium, Incorporated, in the United States and/or other countries. The names of actual products and companies mentioned herein may be the trademarks of their respective owners. For subscription information, please visit www.isc2.org. To obtain permission to reprint materials, please email infosecproeditor@isc2.org. To request advertising information, please email lpettograsso@isc2.org. ©2021 (ISC)² Incorporated. All rights reserved.

(ISC)² MANAGEMENT TEAM

EXECUTIVE PUBLISHER
Timothy Garon
571-303-1320
tgaron@isc2.org

DIRECTOR, CORPORATE COMMUNICATIONS
Jarred LeFebvre
727-316-8129
jlefebvre@isc2.org

CORPORATE PUBLIC RELATIONS MANAGER
Brian Alberti
617-510-1540
balberti@isc2.org

MANAGER, MEMBER COMMUNICATIONS
Kaity Pursino
727-683-0146
kpursino@isc2.org

COMMUNICATIONS COORDINATOR
Dimitra Schuler
727-316-9395
dschuler@isc2.org

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

TWIRLING TIGER MEDIA MAGAZINE TEAM

EDITOR-IN-CHIEF
Anne Saita
asaita@isc2.org

ART DIRECTOR, PRODUCTION
Maureen Joyce
mjoyce@isc2.org

Twirling Tiger Media is a women-owned small business. This partnership reflects (ISC)²'s commitment to supplier diversity.

CONTENTS

The Return to Normalcy and Brighter Days Ahead

BY ZACHARY TUDOR, CISSP, CHAIRPERSON OF (ISC)² BOARD OF DIRECTORS

Yes, we've heard it over and over again. COVID-19 was a major disruptor to all our lives and our businesses in 2020 and that long-tail effect has lingered into 2021 as well. Transitioning to full-time remote work environments, dealing with school closings and children in your workspace, and a never-ending string of Zoom meetings. It's been difficult. But let me tell you something else: we're getting back to normal sooner rather than later.

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

It wasn't all doom and gloom for (ISC)² last year. Even in a year when in-person certification examinations were temporarily unavailable for several weeks, the association grew to more than 157,000 members. The number of CCSP certifications grew at a rate of nearly 30%. And as members were struggling to find continuing education opportunities elsewhere, (ISC)² staff executed a great virtual Security Congress with 5,700 global attendees, more than doubling the total number of practitioners who joined us the previous year. For 2021, we are planning a hybrid event for Security Congress that we hope will bring back the valuable in-person experience alongside rich online sessions.

Remote learning was more critical than ever last year. By the end of 2020 about 27% of all members had taken one of our Professional Development Institute (PDI) courses and to date have earned more than 292,000 CPE credits. The (ISC)² webinars program also had more than 650,000 views of its 166 online events.

Of course, one of the most significant accomplishments of 2020 was finding and hiring a new CEO for the association. As the Board thoroughly vetted candidates for the next (ISC)² executive leader, there were skills and qualities we were looking for, along with a clear vision for the direction of the association. Being an (ISC)² member was actually not one of the requirements.

For 2021, we are planning a hybrid event for Security Congress that we hope will bring back the valuable in-person experience alongside rich online sessions.

When we were lucky enough to find Clar Rosso, it quickly became evident that our long-term visions aligned. While it's true that Clar does not hold a CISSP, she's a professional at running an association for professionals like us. Her tenure on the executive team at the Association of International Certified Professional Accountants (AICPA) informs the kind of structural guidance (ISC)² needs during this transformative period in cybersecurity.

Clar immediately developed four main strategic priorities that she and her team will focus on in the upcoming months and years. These priorities include:

- **Amplifying the core** – Building on our strengths, making sure our certification programs are fit for purpose for the market, reviewing our Common Body of Knowledge to make it more universal and to create stepping stones between our certifications, and assuring that our organization is delivering the right set of valued services to members

- **Promoting global competence in cybersecurity** – Offering the right educational tools to our members while creating opportunity for others in the field to build greater competence
- **Advocating for our members and the profession** – Providing thought leadership in the market, engaging in public policy discussions, and launching a Global Diversity, Equity and Inclusion (DEI) initiative
- **Excelling at service** – Working more closely with our Chapters and using our programs and technology to better serve our members

On the DEI front, I've seen firsthand how (ISC)^2 walks the walk. Although we've tended to be a fairly diverse Board in past years, I'm pleased to see more gender, ethnic and geographical diversity on the Board this year than ever before.

I recently had a chance to record an "Inside (ISC)^2" video with Clar to discuss the latest updates from the Board of Directors and the association leadership. This series will be a way to foster accessible communications about the new programs and other changes that are going on within (ISC)^2. It will enable members to hear from various executives in different functional areas of the association to gain more insight into how the organization is working to better serve us. To watch my full conversation with Clar, please visit https://www.isc2.org/News-and-Events/Webinars/Security-Briefing?commid=475936.

Again, the future is bright, and I really do believe that we're close to being able to breathe a sigh of relief after the events of the past 14 months. And when we do, (ISC)^2 is well positioned to continue to inspire a safe and secure cyber world without missing a beat. ●

FIELD NOTES

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

NEW ONLINE STUDY AND CERTIFICATION GROUPS THE LATEST OFFERINGS FROM (ISC)^2 COMMUNITY

WHETHER YOU'RE LOOKING for a "study buddy," or to connect with fellow veterans, consultants and early career associates, there's a group for you within the (ISC)^2 Community on the organization's website.

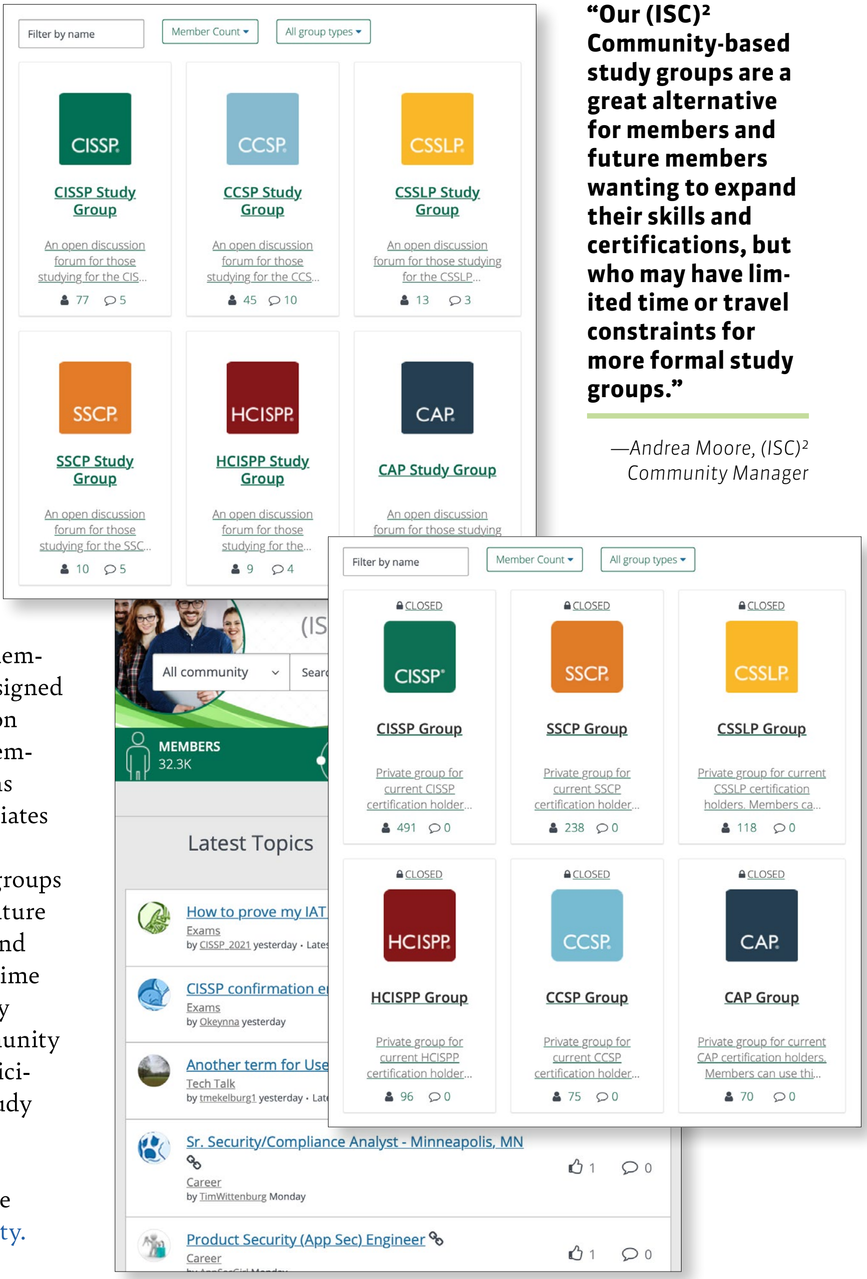
The study groups are open to anyone to join and share study tips, testing strategies or other relevant topics on CISSP, CCSP, CSSLP, SSCP, HCISSP and CAP exams. Each study group provides an open forum, allowing candidates to connect with others globally in their pursuit of a specific certification. These digital study groups allow for brainstorming, networking and positive encouragement especially when meeting in-person is not available.

The certification groups are only for members who already hold the cert and are designed as a way to network with other certification holders. A third group is organized for members who fall into career categories, such as veterans, small business owners and associates hoping to enter the field.

"Our (ISC)² Community-based study groups are a great alternative for members and future members wanting to expand their skills and certifications, but who may have limited time or travel constraints for more formal study groups," Andrea Moore, the (ISC)² Community Manager, said. "Anyone can join and participate at their convenience to contribute study tips as well as benefit from others."

You can learn more by joining almost 32,000 others who've registered to join the popular online forum at https://community.isc2.org.

> **"Our (ISC)^2 Community-based study groups are a great alternative for members and future members wanting to expand their skills and certifications, but who may have limited time or travel constraints for more formal study groups."**
>
> *—Andrea Moore, (ISC)^2 Community Manager*



Filter by name | Member Count ▾ | All group types ▾

CISSP Study Group
An open discussion forum for those studying for the CIS...
77 · 5

CCSP Study Group
An open discussion forum for those studying for the CCS...
45 · 10

CSSLP Study Group
An open discussion forum for those studying for the CSSLP...
13 · 3

SSCP Study Group
An open discussion forum for those studying for the SSC...
10 · 5

HCISPP Study Group
An open discussion forum for those studying for the...
9 · 4

CAP Study Group
An open discussion forum for those studying

Filter by name | Member Count ▾ | All group types ▾

CLOSED
CISSP Group
Private group for current CISSP certification holder...
491 · 0

CLOSED
SSCP Group
Private group for current SSCP certification holder...
238 · 0

CLOSED
CSSLP Group
Private group for current CSSLP certification holders. Members ca...
118 · 0

CLOSED
HCISPP Group
Private group for current HCISPP certification holder...
96 · 0

CLOSED
CCSP Group
Private group for current CCSP certification holder...
75 · 0

CLOSED
CAP Group
Private group for current CAP certification holders. Members can use thi...
70 · 0

All community | Sear

MEMBERS 32.3K

Latest Topics

How to prove my IAT
Exams
by CISSP_2021 yesterday · Lates

CISSP confirmation e
Exams
by Okeynna yesterday

Another term for Use
Tech Talk
by tmekelburg1 yesterday · Lat

Sr. Security/Compliance Analyst - Minneapolis, MN
Career
by TimWittenburg Monday
1 · 0

Product Security (App Sec) Engineer
Career
1 · 0

Q&A

HOW I GOT HERE

MAKING A NATION'S CYBER WORLD SAFE

Yuval Segev, director of advanced technology at the Israel National Cyber Directorate, received the 2020 (ISC)² Government Professional Award for the EMEA region

INTERVIEWED BY DEBORAH JOHNSON

YUVAL SEGEV

Segev leads Israel's development of systems to protect its economy, both government and private. He began his career in information security in the Israeli Air Force and earned an engineering degree and an MBA.

What were the biggest challenges you faced as the leader of Israel's developing economic cyber defense program?

The main challenge was to create a broad and comprehensive knowledge base that would provide information for free. The project requirements include:

- Centralizing security recommendations
- Quickly disseminating and enacting changes in best practices
- Encouraging Israel's small and medium-sized businesses, as well as those worldwide, without strong cyber defenses to use the system's capabilities

How is the project progressing?

Today, the national risk calculator ("Yuval system") provides a vast knowledge base gleaned from more than 1,000 risk questionnaires or assessments conducted by organizations in the past two years. Each economic sector that took part receives a customized recommendation for a practical work plan.

Currently, we are considering introducing the system to partners in different countries.

Tell us about your start in information security.

I joined the Israeli Air Force as a CISO. After about five years of military service, during which I was exposed to the defense of missiles, aircraft and classified networks, the decision to continue in this field, only as a civilian, came naturally for me.

My experience in large international organizations such as Deloitte and Check Point [Software Technologies] exposed me to the enormous variety in cyber defense practices in different industry sectors and diverse organizational cultures.

Among the main challenges faced in those days was protecting their data. In the early 2000s, there was a gap in the availability of orderly professional knowledge on the field of cyber defense. Organizations had to develop their systems based on their own professional experiences.

They also needed to speed up defenses. Attacks are one small step behind the new technology, while the various defense solutions are one step behind the attackers. The ability and speed of organizations to react is limited. Additionally, they needed to implement guidelines. The multiplicity of regulations and audits is a challenge for organizations to manage effectively.

What do you see as some of the biggest needs in protecting data, for individuals *and* organizations?

Improving authentication. Name and password are not enough. The use of stolen passwords remains one of the major attack vectors. Also: increasing data protection. Early adoption of the PCI standard for credit card protection was sluggish. Reality has shown that encrypting credit data and databases is not an impossible task or a privilege for advanced organizations only. Finally, keeping up to date. Organizations are often not able to keep up with defenses needed to protect data and products. ●

CONTENTS

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 WORTH, CHRISTOPHER GATES AND JASON SMITH

(Artech House, August 2020)

The authors frame their guide around best practices issued by the Health Sector Coordinating Council (HSCC) in 2019.

THE INTERNET OF THINGS (IoT) has become a pervasive element in modern living, from organizing the appliances, entertainment and security in your home to controlling your car and, more recently, connecting health and medical devices, where the risk is especially high. Imagine an attacker being able to access or modify your EKG or your wearable, internet-connected insulin delivery system or similar devices.

Medical Device Cybersecurity for Engineers and Manufacturers provides a guide to the steps necessary to ensure that security every step of the way. The challenge of this new frontier is to develop security standards for every aspect of the design, development and implementation of these devices.

Authors Worth, Gates and Smith point out that, according to the American Hospital Association, there are as many as 6 million connected medical devices just in hospitals in the United States. Each of the medical devices is a potential target for intrusion. Patient safety and quality depend on the implementation of a robust set of security controls.

The authors frame their guide around best practices issued by the Health Sector Coordinating Council in 2019. They provide the optimal security controls to implement and manage devices and protect the device ecosystem as well as the users' personal health data. The authors call them basic "blocking and tackling controls" that can be enhanced as the enterprise matures and adopts a threat framework such as MITRE's ATT&CK.

This book is marvelous since it provides a roadmap for a stakeholder to structure an ecosystem to minimize the risks and threats presented by these devices. ●

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

MORE PROOF RANSOMWARE DOES NOT DISCRIMINATE

RANSOMWARE CONTINUES TO GLOBALLY disrupt business and IT operations, regardless of location. A recent PC Matic data analysis shows that, per capita, the top five U.S. states for ransomware attacks are South Dakota, Montana, Alaska, Rhode Island and New Mexico.

"Amongst the five, you are looking at very different characteristics for each state," said Rob Cheng, founder and CEO of the U.S.-based cybersecurity firm. "This, in and of itself, reaffirms that cybercriminals do not discriminate and will target just about anyone. Big state, small state, red state or blue state, if you are an easy target, you're likely one of their next victims."

That same advice holds for those located outside North America, where ransomware continues to spread. Cheng advises long-standing content filtering solutions to mitigate the chances of someone within an organization infecting machines with increasingly sophisticated malicious code.

"Cybercriminals have coupled the two most detrimental forms of cyber threats businesses face—ransomware and security breaches—into a new bundle. Now more than ever, detection and response is not an option. Once you're infected, they not only encrypt your files but also steal your data. At that point it is too late. Utilizing a default-deny approach, like content blocking and permitting, will significantly reduce the risk of falling victim to cybercrime." ●

CHAPTER SPOTLIGHT

MEMBERS RESPOND POSITIVELY TO VIRTUAL CHAPTER MEETINGS

(ISC)² CHAPTER LEADERS were forced to move their meetings and events online after March 2020 due to the pandemic. A year later, they reported mixed views on how well virtual meetings were working, with some seeing opportunities to expand attendance and others watching participation dwindle.

Most did not hold virtual meetings prior to lockdowns required to help stop the quantum spread of COVID-19. It also was important to help members start securing their networks and data assets differently, as everyone continued to work from home. This appears to have impacted meeting attendance, which dipped in some cases but drew participants from a wider geographic range.

Preferred platforms for virtual meetings included (in order of preference) Zoom, Google Meet and Microsoft Teams. Some experimented with both freeware like FreeConferenceCall.com and popular software like Cisco Meetings and WebEx before settling on one of the other three platforms.

Here is a sampling of opportunities and challenges North American chapters faced.

We didn't see a change in attendance initially, so I don't believe they were hesitant to jump online for meetings. The biggest cause of variation of attendance is either notice of speakers or change of times, such as moving to a lunchtime event. … The biggest challenge for us was finding speakers that were willing to speak online. Some speakers/hosts wanted to use their own Convergence platform to host their meetings and some mandated it. We lost the ability to manage attendance when that happened."

—Lito Alvarez, President, Hawaii Chapter, where meeting attendance averages dipped after going online

In the beginning of the pandemic, the attendance was low because people were preoccupied with more immediate issues. As time went on, we started to do a big outreach program and we saw that we were getting better turnouts than our in-person meetings. I attribute this to people being more amenable to attend virtual meetings, since they no longer need to drive to the events. It turned out to be a big win for us. The biggest challenge: competing with other virtual events."

—Ken Fishkin, President, New Jersey Chapter, which changed its marketing strategy in October 2020 and more than doubled its local membership

It became apparent that we had to ensure that all speakers were comfortable with the technology in advance, and prep video/audio testing sessions were required to help ensure everything ran quickly on presentation day. Overall, both our members and speakers demonstrated wonderful flexibility and great attitudes, and we have been receiving positive feedback about our virtual beginning since its start."

—Victoria Granova, President, Toronto Chapter, which grew its membership base by 180% and held 200% more events than in 2019

Photograph by Getty Images

CONTENTS

Virtual meetings have opened new opportunities for us. When users don’t need to commute for a meeting, they are more likely to attend and participate. The virtual environment also lends itself to shorter, more focused gatherings, which are very attractive for people looking to learn or discuss specific topics. Having said that, the in-person meetings are the best way to hold general assembly meetings and social gatherings. What we’ve learned is that we should continue having a mix of virtual and in-person events, even after all restrictions are lifted.”

—Arturo Santos, President, Miami Chapter, which grew membership by 30% during 2020

Prior to the pandemic we did not hold virtual meetings. … The first task was to reach out to members to assure them we were still a group. This was accomplished using a group on LinkedIn ((ISC)^2 South Central Alaska Chapter). Then we posted a generic email to our membership list. The response has been very good and there may actually be more participation than some of our previous in-person meetings. We are actually getting responses from members out of the local area who could be as far as 1,000 miles from Anchorage, where we host the meetings.”

—Ronald Norris, President/Treasurer, South Central Alaska Chapter

We have been able to use virtual meetings to have a member from another chapter give a presentation. That member was the president of the Pittsburgh Chapter.”

—Todd Davenport, President, Middle Georgia Chapter, which didn’t see significant changes in membership or meeting attendance

Members were eager to attend [virtual meetings]. The traffic in our region has been growing exponentially. This made meetings accessible and easier to attend.”

—Joseph Irr, President, Quantico Chapter, which doubled its current membership and improved monthly email opt-ins (a source for attracting new members) from 60 to 270

ADVOCATE'S CORNER

THE WEIGHT OF EXPECTATIONS

Should we present more realistic views of what we do?

BY TONY VIZZA, CISSP, CCSP, DIRECTOR FOR CYBERSECURITY ADVOCACY, ASIA-PACIFIC, (ISC)²

AT THE HEIGHT of the dot-com bust of the early 2000s, I managed a retail store for a large Australian electronics chain. I had recently graduated from university with a computer science degree and, despite having work experience, IT jobs were scarce. So, rather than continuing to apply for the handful of vacancies that existed, I opted to work in retail and make the most of it.

One of the most challenging events I encountered as a store manager was a set of fraudulent incidents that occurred while I was on PTO. The store was selectively targeted by a criminal gang to purchase over U.S. $7,000 worth of electronics goods using stolen credit cards.

The first inkling that something may have been amiss was when the duty manager texted me the evening before my scheduled return to report a "record" four days of sales—four days that weren't notable in the retail calendar.

Returning to work the next day, I had barely touched my morning coffee when a large bank called about a set of previous days' transactions. All up, the criminal gang had used four credit cards, multiple individuals and many more transactions to get away with a lot of crime.

Inevitably, the chain's head office sent a fraud investigator who found my staff had followed protocol to the letter. Interestingly, the bank advised that "these things happen all the time." Simply put, it was a successfully executed targeted attack. After a nervous few days, to my relief none of my staff, my duty manager nor I were reprimanded in any way. Before leaving, the fraud investigator mentioned to me that "(the fraud) is the cost of doing business these days." The issue made us all wiser and we moved on with doing our jobs.

Let's come back to present day, where instances of cybercrime and electronic fraud continue to skyrocket. In many jurisdictions around the world, these categories of crime now rank at the very top of total crimes reported to law enforcement agencies. Yet, when a cybercrime occurs, the victim is all too often blamed for either recklessly or negligently causing the crime to occur, in significant contrast to physical crime.

Sadly, many good and hardworking cybersecurity practitioners have been reprimanded, or worse, lost their jobs and had their livelihoods threatened and reputations harmed because a cybercriminal or well-resourced cybercrime operation was able to perpetrate damage on an organization.

There is no doubt that significant challenges exist when protecting against criminals in the physical world. These challenges seem almost insurmountable when considering criminals in the virtual world, particularly given the myriad of potential attack vectors and an ever-increasing set of vulnerabilities.

This begs the question: As an industry, have we set the right levels of expectations within our own organizations in terms of protections we realistically can provide? Given that national governments and multi-billion dollar organizations continue to get breached, have we set the right levels of expectations within our management teams in relation to what we can achieve? Should we adopt and promote an "assume we have been hacked" mindset to ensure those we work for understand and accept a more realistic approach to overall cyber resilience?

Perhaps we really do need to look in the mirror and have an honest conversation with ourselves about expectations. ●

Tony Vizza is the director of Cybersecurity Advocacy, Asia-Pacific, (ISC)². He can be reached at tvizza@isc2.org.

Staffing Your Startup

BY DEBORAH JOHNSON

Staffing problems are one of the main reasons startups fail, according to CB Insights, a tech market intelligence platform. Its analysis of 101 startup postmortems revealed the third most common reason was "not the right team," after "no market need" and "ran out of cash."

Here are some tips to give your staffing a head start on the path to success.

Analyze Your Abilities

You have to be honest with yourself and know what you do uniquely well, and where you're lacking, advises Glenn Gutek, founder and CEO of Florida-based Awake Consulting & Coaching. "You, as the entrepreneur, are the fixed point, so you have to build around your strengths and also your weaknesses," he says.

That starts with an honest self-appraisal, according to Sue Andrews, business and HR consultant with KIS Finance in Talbot Green, Wales, U.K. An entrepreneur "can see where the gaps lie … and ensure that they have the right mix of skills to run the company in the day-to-day, as well as develop the business's strategy for growth."

Seek Out the Passionate

Even with tech-focused job boards such as GitHub, Stack Overflow and Dice, Gutek encourages a more personal approach, especially with top-level positions. "I would do some word-of-mouth referral recruiting. And because you're a startup, you don't want in your senior leadership people who are looking for great, safe jobs. You're going to be looking for some quasi-entrepreneurial types that will take the ride with you."

Don't shy away from colleagues and friends, he adds. "I'm a fan of going to people you know. For people who are highly dedicated [and] highly committed, their passion, drive and focus is highly infectious. The thing that I've noticed [is that] the people you know are the people you are most likely to infect."

Look for the Gaps

Your skills assessment will reveal what is missing in the venture's leadership, counsels Andrews. "If [the entrepreneur has] a financial background, they may well prefer to control this aspect of the business, while focusing their recruitment on product development and sales. Alternatively, if they have a creative background, they may prefer to retain control over these aspects and hire someone to manage the company's finances."

Hiring good people takes focus, patience and self-awareness. Some tips culled from job boards, social media and recruiting professionals include:

- Have a clear vision and mission for your company
- Hire your senior members first
- Have a detailed career page on your website
- Look for candidates whose skills complement yours
- Keep a list of possibilities. While a great candidate might not be available right now, things do change.
- Develop a salary/compensation plan you can afford
- Consider hiring part-time contractors if money is tight

The success of your startup depends not only on your skills and abilities, but on those of the people you hire. Invest well in human resources and it will pay dividends for years to come. ●

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

10
YEARS
2011- 2021

CENTER FOR
CYBER SAFETY
AND EDUCATION

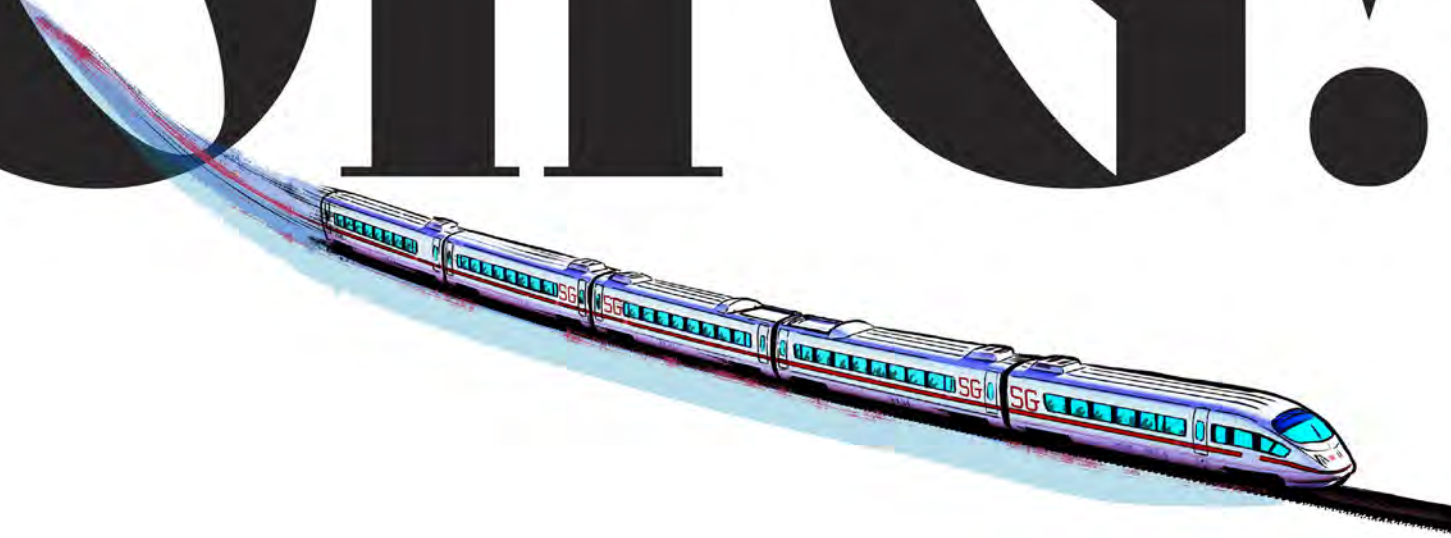
CELEBRATE WITH US AND WIN A JIM DAVIS SIGNED COMIC BOOK

TAKE ME TO THE SURVEY
CELEBRATE

DOWNLOADING
NO. 4
2020
CENTER FOR CYBER SAFETY AND EDUCATION
IAmCyberSafe.org
GARFIELD'S
CYBER SAFETY
ADVENTURES
FEATURING:
DR. CYBRINA
BAD DOG & GRANDMA CAT
ZOMBIE CATS
GO AHEAD! DOWNLOAD THAT ZOMBIE CATS MOVIE FROM AN ILLEGAL SITE!
NO, NERMAL, STOP!
NERMAL, WHAT DID YOU DO?
WARNING!
WARNING!
LESSON 4
Downloading Disaster!

IAmCyberSafe.org/Anniversary

Oh G!



Maintaining 5G security as rollouts speed along

BY ANNE SAITA

AMONG THE MANY conspiracy theories circulating at the onset of the COVID-19 pandemic was one begun by a Belgian physician who told his local newspaper that 5G *could be* biologically linked to the novel coronavirus. Soon celebrities with large online followings warned that COVID-19 might spread through 5G technology, which also was said to suppress immune systems to render people more vulnerable to the virus. Arsonists across the United Kingdom and Europe took note and torched 20 cell towers—including one that served a field hospital treating COVID-19 patients.

5G's purported COVID-related "health risks" have since been widely debunked by the medical establishment. There are, however, other threats associated with 5G that are firmly rooted in reality.

The technology's fast speeds and low latency are expected to usher in a new era of artificial intelligence-driven innovation, with the intellectual property and proprietary processes behind breakthroughs in need of strong protections. These next-generation wireless networks also will hypercharge the Internet of Things (IoT), connecting masses of more visible devices and expanding attack vectors. Additionally, the same high-throughput broadband that delivers greater flexibility and scalability for legitimate users will do the same for those with malicious motives.

ILLUSTRATION BY RAUL ALLEN

"The net benefit is going to be fantastic," says Rear Adm. (ret) David Simpson, USN, who is now a professor at Virginia Tech's Pamplin College of Business's Leadership and Cybersecurity program. "The challenges aren't meant to be showstoppers; they are meant to describe things we need to figure out."

Among those "things" are:

- A greatly expanded attack surface, given 5G elements—networks, devices, IoT sensors, actuators and terrestrial antennas, etc.—will be everywhere 5G service is available. This also will expand the IPv6 address space and make such devices more visible.
- New machine-oriented communications that will require real-time detection systems and immediate mitigations.
- Greater use of multi-access edge computing (MEC) that brings communications, computation and storage to the edge of the network, rather than these capabilities remaining within the core.
- Super accurate location access services that provide exceptional functionality but also raise privacy and security concerns as more devices and users are tracked within a 5G ecosystem.
- A need for greater coordination between service providers and customers, so everyone understands their security responsibilities within this new environment.

"The challenges aren't meant to be showstoppers; they are meant to describe things we need to figure out."

—Rear Adm. (ret) David Simpson, USN, professor, Virginia Tech's Pamplin College of Business's Leadership and Cybersecurity program

FROM ONE GENERATION TO THE NEXT

Each generation of wireless networks brings a new set of functionalities that also alters application availability and backward compatibility. This allows communications to continue with legacy infrastructure. 4G introduced capacity-building LTE (long-term evolution), a standard for wireless communications between mobile devices and data terminals that will continue into 5G.

It's the increased machine-to-machine usage that is the biggest differentiator between 5G and its predecessor. Yes, you'll be able to better stream video and group text with less drag, but the biggest benefit will be in helping convert cities, factories, medical centers, etc. into "smart" buildings designed for a much broader IoT ecosystem. This new-and-improved wireless backbone also means organizations can develop larger, more diverse data sets that become the fuel for artificial intelligence, machine learning and deep learning that until now soaked up an enormous amount of computing resources.

In addition, with 5G, the industry will migrate from hardware-oriented radio access to software-defined networks (SDN) to fully implement network virtualization once done with appliances. This also alters the threat landscape since attackers can not only compromise a wire-connected piece of hardware but also will focus on a control plane defined by code.

"We really need to be thinking about how we protect the integrity of numerous software code bases and their interconnections and assertions of integrity across a network that sees this convergence between communications, computing and storage," Simpson says.

Most are now familiar with the SolarWinds attack that threatens national security. Bad actors injected code into software that tens of thousands of organizations used to measure packet flows and monitor other pertinent network data. *(See "3 Ways to Test a Software Provider's Trustworthiness," p. 31.)*

Simpson points to a history of similar attacks where Russians have attempted to get inside sensitive networks by attacking the supply chain. In 1976, the KGB inserted eavesdropping equipment and burst transmitters in 16 IBM Selectric typewriters destined for use in the American Embassy in Moscow. Ten years ago, when he was still at the Pentagon, Russia was caught attempting to insert malicious code in the development supply chain of Netcracker Operations Support Software (OSS) used by the largest commercial and government global networks. This would have allowed cyber attackers to infiltrate organizations by adding new code into the network security development process.

In these incidents and others like them, covert operations are presumed to originate with nation-states. “Supply chain attacks have always been a goal of our adversaries, and always will be,” he indicates.

Simpson further warns: “Our high-end adversaries will seek in the very beginning to get into the elements that make up the control plane and the application content connections in the networking of 5G and the 5G user.” *(See “5 Ways 5G Networks Are More Vulnerable to Attacks,” below.)*

THE RISE (AND CHALLENGE) OF MEC

5G significantly alters the IT architecture within organizations and requires a new level of automation in order to protect endpoints, radio transport and radio access networks, network cores and all of the cloud-based applications moving to the edge. All will need to be carefully monitored and incidents responded to in near-real time.

“Multi-access edge computing is a big challenge because it means you’re running multi-vendor data centers, cloud-based throughout your network in all sorts of different locations, so you have to consider the management, the monitoring, and incident response is critical,” said Kevin McNamee, who runs the Nokia Threat Intelligence Lab, during a presentation at last November’s (ISC)² Security Congress.

In essence, a lot of mobile activity done within the core of wireless networks will move to the edge, requiring cybersecurity professionals to manage the security of “mobile edge clouds,” as McNamee refers to MEC, with a more distributed environment that will make it more difficult to secure. Access control will be key.

“All those servers that come in from different vendors—they’re running different applications, they’re running in a cloud environment, they have to be managed, . . .” he said. “From a security perspective, when you fire up an application, you want to fire up the security rules policy to support that application. All has to be done.”

The threat intelligence expert told the Security Congress audience that device security is critical, to both maintain control of this new environment and to reduce the chances of the proliferation of these WiFi-connected machines being commandeered to launch massive DDoS attacks or serve as a vector for malicious code.

This is where the concept of slicing comes in.

5 WAYS 5G NETWORKS ARE MORE VULNERABLE TO ATTACKS

5G warrants a new approach to security, especially when mission- and business-critical operations are at stake. A September 2019 Brookings article co-authored by Virginia Tech professor David Simpson and Brookings Visiting Fellow Tom Wheeler outlined five ways fifth-generation wireless networks are more vulnerable than previous versions.

1. The switch from centralized, hardware-based switching to distributed, software-defined digital routing.

2. The move from hardware appliances to virtualization for many network functions.

3. Growing use of artificial intelligence within 5G networks and applications that puts machine-learning mechanisms like algorithms in a more precarious position.

4. A proliferation of short-range, small-cell antennae will become hard targets, as will the dynamic spectrum sharing capabilities they provide.

5. A much broader IoT universe full of unprotected devices. With machine-to-machine communications expanding across all industry sectors, expect more attempts to compromise cellular connectivity to interrupt transmissions and harvest data. ●

CONTENTS

A SLICE OF 5G LIFE

With 5G, a telecom carrier is able to let customers break their networks into segments and protect them from each other, allowing access to different slices only as needed. This is a major security benefit, providing network separations based on the security profiles of different applications—such as those tied to medical, banking or industrial control systems.

There is a network component called the Network Slice Selection Function that defines how a device joins the network based on its identity and carrier-stored profile. A device can be given multiple slices, such as one for internet access and another for accessing a corporate network. This standard defines how a device requests and is given a slice; how the network works within that slice; and how it protects it from other traffic on other slices.

This allows security teams to apply more security controls where needed, within both the core and MEC, without impeding business functions.

Incorporating slicing to establish security zones requires careful consideration of:

- Application categories based on quality of service, throughput rates, service-level agreements and other criteria.
- Carrier-supported, end-to-end secure services that encrypt and isolate chosen segments for clients/customers.

"Who will be responsible for the security of these applications—the application vendor or the service provider?"

—Kevin McNamee, Nokia Threat Intelligence Lab

"It's very easy to say 'Secure the mobile edge cloud,'" McNamee says in a follow-up to his talk. "But I think this is going to be a big task that's going to involve a lot of people thinking pretty hard about how this is done. You have to be able to manage the security of multiple mobile edge clouds out there in the field, monitor their security and respond to incidents. There's managing the different applications from different vendors that are going to be running in these clouds. Who will be responsible for the security of these applications—the application vendor or the service provider?

"And then there's the whole aspect of access control. Who is it that gets to access the applications within these clouds? Who manages what applications that individual devices can access, and what features they can't access. What should they have visibility to and what should be restricted? These are not simple problems. We have to do a lot of work in that area."

One reason to make this a priority is the other side of slicing: a more focused target for attacks. By concentrating mission-critical and highly sensitive data into specific segments, it makes those prized slices more attractive to cybercriminals.

PRIVACY MATTERS

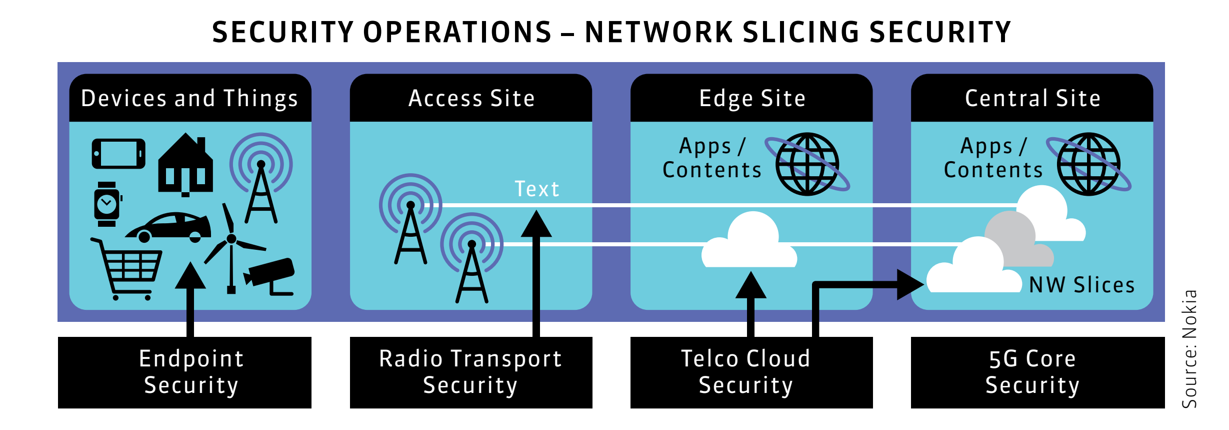
Anjali Gugle, a security architect and data governance expert who works in Cisco Systems' Customer Experience business unit, is among those concerned about privacy within 5G environments, which rely on a larger concentration of higher-frequency towers and antennae that allow hyperactive location access services. It's a great feature, she says, if you or your devices don't mind being tracked within a 5G ecosystem.

"It's going to be a ubiquitously connected kind of world; everything is going to be connected, and where I see the biggest security and privacy challenges is around sharing location and identity information—particularly personal data privacy because you'll be able to track everything, everyone, every time, everywhere," she says. "You are literally micromanaging the user. You are literally following everything like a shadow."

Those who enter "smart" buildings leveraging 5G technologies need to be aware of what happens once their device—be it a 5G-enabled smartphone, watch, tablet, laptop, etc.—accesses a network. That data needs to be protected from falling into the hands of nefarious users, especially since by then that private data is out of the consumer's control.

"The way I look at it, once you embrace and start using 5G technologies, you've given away your privacy by falling victim to hyperbolic discounting, which is a prominent decision

APPROACHING 5G SECURITY FROM MULTIPLE PERSPECTIVES



Source: Nokia

5G is designed to expand connectivity and provide a stronger platform upon which bandwidth-intensive applications, like video streaming, and technologies, such as artificial intelligence and deep learning, can be done more quickly. But this expanding ecosystem also means more protections must be in place to cover the wider array of devices, cloud services and wireless connectivity. Nokia's Kevin McNamee points to four areas that every cybersecurity professional must address.

Endpoints: Traditional 3G/4G network endpoints are primarily mobile phones that can become infected with malware. But 5G will go well beyond smartphones, laptops and tablets to any device connected to the wireless network to communicate with each other. Most of these endpoints will be built without much security by default and not be regularly updated.

Radio Transport: Expect 5G access points to continue expanding, dotting local landscapes with multiple-input, multiple-output antennae that in and of itself expands an attack surface. Then there's the radio technology utilized by 5G networks that separates a Radio Access Network (RAN) from core functions. IPsec deployments within 5G will help with authentication, but new protocols will emerge to secure radio transmissions traveling at super-fast speeds.

Cloud Services: Multi-access Edge Computing (MEC) will require a greater degree of security orchestration and automation in order to secure cloud-based, multi-vendor data centers throughout a network, of which there will be many as 5G rollouts continue.

Core Security: Running parallel to the MEC will be a new protective control plane at the 5G core. Splicing will allow for high-risk assets to be segmented and better protected when resources are limited. But it also will expand how many slices must be managed. ●

heuristic that can affect privacy decisions," Gugle warns. "You're giving away your data and subjecting yourself to being tracked 24/7 because you want to use their services."

Data-centric regulations like the EU General Data Protection Regulation and, in the United States, California Consumer Privacy Act will help push companies to maintain strong data governance and provide transparency in their usage of data generated by geolocation tracking.

MANAGING RISKS TO MAKE 5G WORK AS INTENDED

Risk management must be reassessed with any 5G rollout. That is, security implications will need to be balanced by the benefits a 5G environment provides. There also will be security responsibilities to be meted out between providers and those they serve.

CONTENTS

“5G definitely is a positive thing, especially if there is accountability. It’s improving location precision, ubiquitous connections and mass connectivity in a multi-vendor environment,” Gugle says. “But the lack of location privacy due to the amount of tracking will remain a major concern. If somebody can magically come up with a way to protect the digital trail of a customer while providing more robust facilities, it will be a good thing.”

Virginia Tech’s Simpson agrees.

“You’ve got to bring your business objectives in a 5G world into your risk management process today. That means you start to build appropriate skill sets within your company based on how you intend to utilize 5G at your company,” he advises. “You may actually reduce people in a given area because you’ll rely on more automation made possible by 5G. That means it’s all the more important that you bring some 5G transformation expertise into solution development transition and your objective business operation.

“Then work on risk mitigation efforts that include architectural changes for how you’ll implement these capabilities,” he continues. “If we just rely on acquiring a new appliance or a 5G-certified service, you’ll miss many potential satisfying risk mitigations that could apply to your 5G-enabled business operations. Transformational leaders should give business risk reduction a front-row seat as they plan to achieve automation, AI and other worthwhile 5G functional goals.” ●

“If somebody can magically come up with a way to protect the digital trail of a customer while providing more robust facilities, it will be a good thing.”

—*Anjali Gugle, security architect and data governance expert, Cisco Systems*

ANNE SAITA is editor-in-chief of *InfoSecurity Professional*.

Earn your cybersecurity degree online
Strengthen your skills and gain expertise to help you succeed.
worldcampus.psu.edu/isc2
BEST ONLINE PROGRAMS
U.S.News & WORLD REPORT
GRAD COMPUTER INFORMATION TECHNOLOGY
2021
21-WC-0592/sms/sss
PennState World Campus
A world of possibilities. Online.

RECIPROCITY | ZenGRC

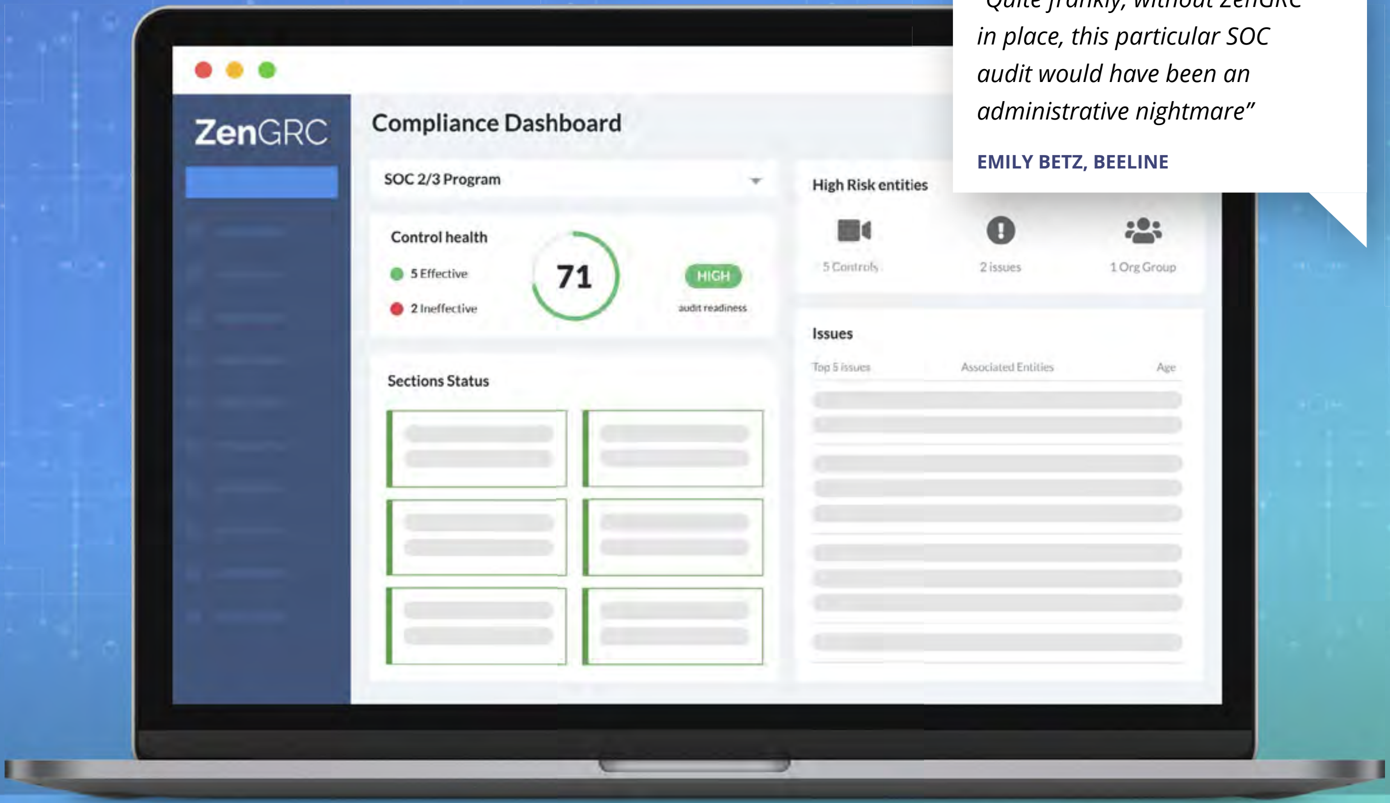
Introducing the best GRC tool on the market: ZenGRC

Reciprocity customers rely on ZenGRC to simplify their risk and compliance programs.

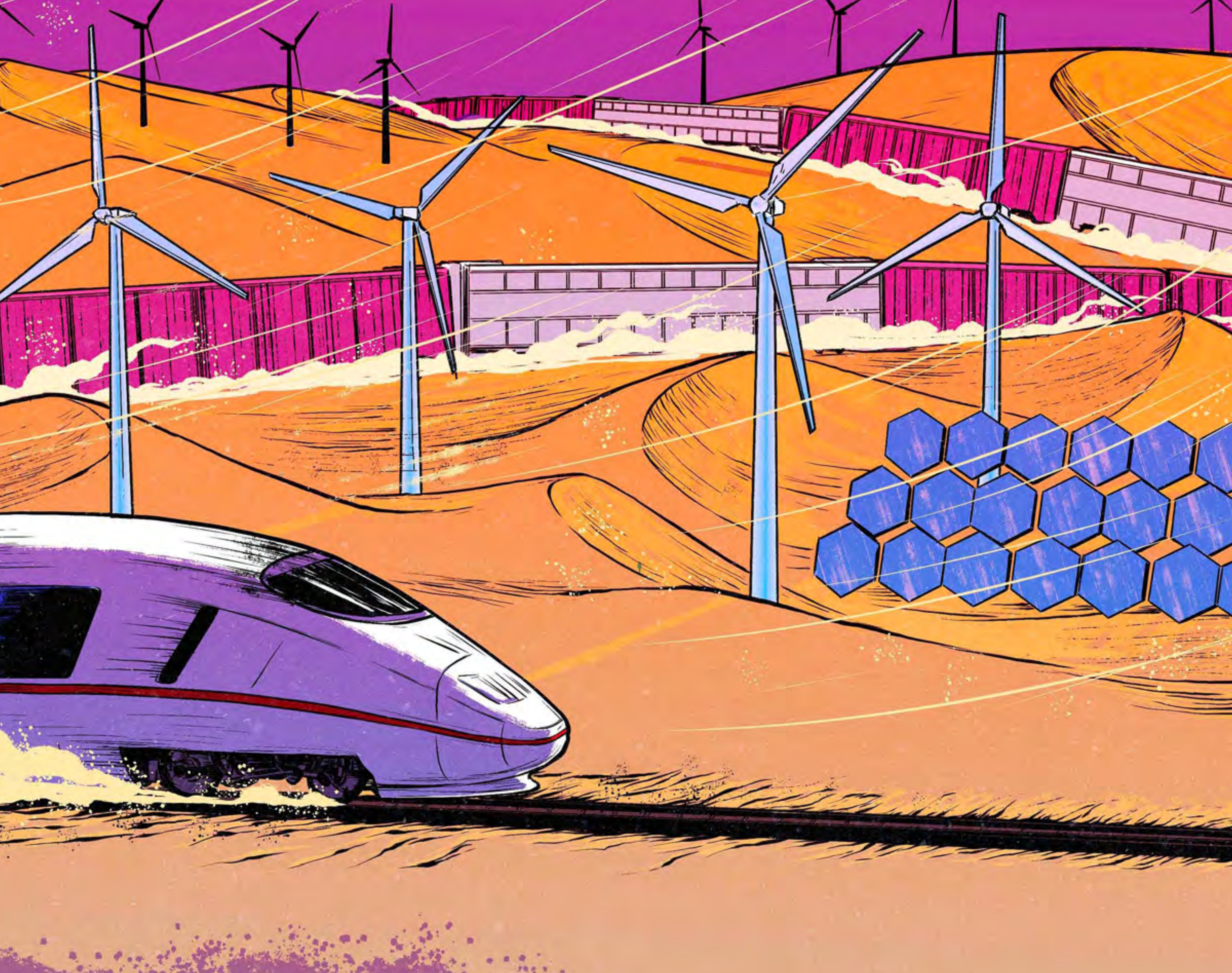
> *"Best GRC tool on the market. Additionally, the risk management capabilities of ZenGRC make it easy to integrate enterprise risk management into your overall compliance program."*
>
> **BILL DOUGHERTY, OMADA HEALTH**

> *"ZenGRC generated 35% savings and immediate ROI, eliminating the need for our 3rd-party audit firm to audit duplicative controls across multiple annual audits"*
>
> **CHRISTOPHER HENDERSON, DATTO**

> *"Quite frankly, without ZenGRC in place, this particular SOC audit would have been an administrative nightmare"*
>
> **EMILY BETZ, BEELINE**



Discover how ZenGRC can help your business at reciprocitylabs.com



Chain Reaction

HOW TO PROTECT AGAINST CYBER-RELATED SUPPLY DISRUPTIONS THAT CARRY SERIOUS CONSEQUENCES

BY SHAWNA McALEARNEY

ILLUSTRATION BY RAUL ALLEN

A LITTLE OVER A YEAR AGO, the world was shocked out of complacency when COVID-19 disrupted fairly reliable supply chains. Workers quarantined, businesses shut down, and production and manufacturing ground to a halt.

We laugh now at panic buyers who sparked nationwide toilet paper shortages, but supply chain issues are no joke. If your company can't get the components it needs, it impacts your customers, your deadlines, your reputation and your bottom line.

> "Integrity in the supply chain ensures the items can't be tampered with or replaced with counterfeits. Availability ensures items can be accessed when needed and received in a timely fashion; without availability there is no purpose to the supply chain."
>
> *—Jeff Neithercutt, founder, Blockchain of Evidence*

'LONG ATTACKS' TO SUPPLY CHAINS

From construction companies to law firms, attackers are taking the long view, quietly accessing targets by infiltrating their suppliers. This type of attack is purposely kept at a level that will evade detection for a prolonged period of time.

The three tenets of the CIA triad—confidentiality, integrity and availability—are crucial to supply chain cybersecurity, says Jeff Neithercutt, founder, Blockchain of Evidence, a provider of secure evidence integrity software.

"Without confidentiality in the supply chain, you can't be sure whether an item was tampered with in transit or is the item you ordered," he says. "Integrity in the supply chain ensures the items can't be tampered with or replaced with counterfeits. Availability ensures items can be accessed when needed and received in a timely fashion; without availability there is no purpose to the supply chain."

Nearly everyone is familiar with initial pandemic shortages in personal protective equipment (PPEs), such as N95 masks, as well as medical gloves and gowns. And hand sanitizer—let's not forget the lack of hand sanitizer that prompted many distilleries and breweries to cease making consumable alcoholic beverages and begin manufacturing that essential item. Even car manufacturers switched gears and began producing much-needed medical ventilators instead of automobiles.

In the cybersecurity world, there was another supply chain issue that led to what's believed to be one of the biggest security breaches in recorded history, with companies still discovering a third-party provider's compromised code within their own systems.

SOLARWINDS BREACH BLOWS THROUGH SUPPLY CHAIN INTERDEPENDENCIES

By now, every information security professional is aware of attackers who inserted malicious code into several software updates issued by network visibility provider SolarWinds. Though only discovered in December, more than a year ago attackers breached the SolarWinds Orion software platform and installed a trojan within the update that would later be downloaded and trusted by 18,000 clients, including the U.S. Departments of State, Homeland Security, Treasury and Commerce, as well as tech companies Microsoft, Cisco, VMWare and Intel. Security experts say the malicious code allows an attacker "broad reach" into compromised systems.

"The SolarWinds cyber breach is just the latest reminder of the digital interdependencies across the government and private sector, and the fundamental role of supply chain security to U.S. national and economic security," Andrea Little Limbago, vice president of research and analysis at supply chain risk management consultancy Interos, writes on her blog. "While there has been a significant increase in awareness and activity toward creating more trustworthy supply chains, a coordinated, whole-of-government strategy is necessary."

She cites a two-year-plus trend in which U.S. departments added hundreds of Chinese companies, and more recently, many Russian companies, to the Department of Commerce's Entity List due to national security concerns and human rights violations.

"A strong, democratic coalition can engrain transparency, security and human rights into global supply chain policies, working together to overcome the insecurity and fragility of modern supply chains and create greater agility, resilience and security," says Limbago.

"It is clear that supply chain security and resilience is an economic, national security and societal imperative," she continues. "The U.S. must modernize its approach to supply chains through comprehensive and coordinated policy and technological solutions, or risk being left behind and vulnerable to the imminent future shocks of a post-pandemic world order."

C-SUITE DICTATES SUPPLY CHAIN(GES)

The effect of the pandemic on the supply chain is a global C-suite concern—including CISOs that must protect increasingly cloud-based products and services their

> “We understand that supply chains will continue to be at high risk for hacking. It’s critical that we in the cybersecurity community use this time to learn lessons and plan for the next large-scale event that impacts the integrity of huge swaths of the internet.”
>
> *—Bruce Potter, former senior technical advisor to President Barack Obama’s Commission on Enhancing National Cyber Security*

companies provide as well as the software and equipment needed to run those solutions.

“COVID disrupted nearly every large business; 92% of companies expect the disruption of global supply chains caused by the pandemic will continue to shape their business in the long term,” reports an August 2020 survey of 450 U.S. high-level senior decision-makers in risk management, compliance, logistics, IT, procurement and operations with revenues exceeding U.S. $1 billion. The survey was conducted by market research firm Vanson Bourne at the request of Interos to gauge the level of COVID-19’s disruption to supply chains.

Almost half of survey respondents saw “fluctuations in supplier prices and order delays,” which continue to have ongoing effects almost a year after the survey was conducted. More than a third “felt disruption due to the collapse of manufacturing suppliers” and a quarter experienced supplier bankruptcy.

From a cybersecurity standpoint, this could mean fewer established and trusted business relationships, if a supplier is now out of business, and a rush to find replacement vendors whose own cybersecurity practices need to be vetted.

Industries whose supply chains were most affected were aerospace and defense companies, which reported, on average, that 65% of their supply chains were disrupted by the pandemic, according to the Interos survey. Nearly all (97%) companies surveyed agreed that “better supplier visibility is needed to tackle the problem.”

Increased sourcing agility is high on the priority list, with 45% of respondents calling geographic concentration a core risk to global supply chains. Almost a third identified reshoring to trusted countries as a necessary step toward agility, while nearly three-quarters believe onshoring—moving major production to a homeland—will not only persist long term but is already a short-term priority.

“We understand that supply chains will continue to be at high risk for hacking,” Bruce Potter, a former senior technical advisor to President Barack Obama’s Commission on Enhancing National Cyber Security,

Keeping Supply Chains On Track

The pandemic caused significant shortages that impacted nearly all industries and too many companies and products to name. If your supply chain continues to be impacted by the pandemic, PricewaterhouseCoopers recommends several steps that may help mitigate your dependence on affected distributors:

- “Securing capacity and delivery status for Tier-2 and Tier-3 suppliers, and securing allocated supplies and overtime assembly capacity where possible
- Buying ahead to procure inventory and raw materials that are in short supply
- Securing future air transportation as supply and capacity become available, shortening what might otherwise be ocean freight-based lead times
- Activating product redesign or material certification resources where reliable second sources of parts or raw material are not already available
- Updating customers about delays and adjusting customer allocations to optimize profits on near-term revenue or to meet contractual terms
- Shaping demand, by, for example, offering a discount on available inventory in cases where supply may be short for late winter-early spring fulfillment, optimizing near-term revenue.”

—S. McAlearney

> "Just as Coca-Cola cannot ship soda laced with cyanide, and Frito-Lay cannot ship potato chips packaged with rat droppings, we need Microsoft, Oracle, Adobe, Google, Amazon, Apple, Facebook, etc. to stop shipping unsafe and insecure software."
>
> *—Raj Goel, CISSP, CTO of cybersecurity provider Brainlink*

says in a news release. "It's critical that we in the cybersecurity community use this time to learn lessons and plan for the next large-scale event that impacts the integrity of huge swaths of the internet."

According to the survey, "The additional steps organizations currently are taking to build resiliency include an emphasis on suppliers' cybersecurity postures, increasing onshoring capabilities and diversifying across regions."

And, in a growing onshoring effort and movement toward "domestic resilience," companies are pushing manufacturers and suppliers for more security in their components, even as President Joe Biden presses U.S. agencies to use U.S. suppliers. For example, data center appliance provider SoftIron has engineered what it calls "edge manufacturing" that begins with an open-source software core and ends with a piece of hardware engineered and manufactured to maximize performance with every component manufactured on location, not outsourced, and the ability to audit the pre-compiled source code.

"Just as Coca-Cola cannot ship soda laced with cyanide, and Frito-Lay cannot ship potato chips packaged with rat droppings, we need Microsoft, Oracle, Adobe, Google, Amazon, Apple, Facebook, etc. to stop shipping unsafe and insecure software," says Raj Goel, CISSP, CTO of cybersecurity provider Brainlink. "The software supply chain presents a systemic risk to businesses, governments and society at large."

He believes the current situation needs a jolt similar to Upton Sinclair's *The Jungle*, which exposed the horrific conditions in America's meatpacking plants and led to workplace reforms.

SECURING THE VACCINE PIPELINE WITH BLOCKCHAIN

Vaccine rollouts worldwide have been disrupted by a complicated supply chain that's left doses unused while millions clamor to be inoculated from COVID-19. Experts say that assigning a hashed label to a bar code or QR code at creation, then scanning that code to the blockchain as it passes from production to shipping to delivery to injection, can prove every dose created was injected. This would also allow tracking of the age/sex/socioeconomic status of each vaccine recipient to ensure parity.

"Because blockchain is an immutable distributed ledger where every entry is based mathematically on the entry before it, you can track every dose of vaccine from creation to injection at the federal, state and local level, bridging private and public sector technologies with instant immutable evidence of the life of every dose. If you added temperature checks to the cycle, you could verify in seconds whether the vaccine was ever outside the acceptable temperature range," says Neithercutt.

"The use of Blockchain to track items in a supply chain adds a layer of integrity without complicating the existing inventory process," he continues. "Simplification of tracking doses gives those working in the vaccine supply chain the confidence to work quickly without concern that any dose will expire or disappear due to intentional or unintentional human error. Public confidence in the reliability and safety of the vaccine will increase, as will adoption of the vaccine as a solution."

Neithercutt said that using blockchain as an integrity check to the existing supply chain system reduces complexity and increases trust and transparency in the entire process. In addition to increasing security and trust in the supply chain, it can increase the speed of vaccine distribution without risking vulnerability to human error or theft.

"Once a vaccine record is added to the blockchain," Neithercutt adds, "it can be checked and verified forever, no matter what type of media it is stored upon, because blockchain is based on thousand-year-old math that is easy to calculate forward, and almost impossible to reverse engineer." ●

SHAWNA McALEARNEY is a Las Vegas-based freelance writer.

LEARN MORE ABOUT BLOCKCHAIN

Want to learn more about how blockchain works? Be sure to read our January/February 2019 cover story by member Tuan Phan, *What's the Rush? Beyond the Blockchain Hype*. It was named one of the best technical articles by Trade, Association and Business Publications International in 2020.

3 Ways to Test a Software Provider’s Trustworthiness

The SolarWinds hack was a wake-up call for supply chain vulnerabilities, and the industry is still mounting a systemic response. BY MATT GILLESPIE

Supply chain security depends on its weakest link, a problematic reality for software because so many links are hidden from view. Here are three ways (ISC)² members can mitigate a breakdown if the vendor itself is compromised, as when SolarWinds’ trusted components proved untrustworthy after a cyberattack in 2020.

1. Exert Governance Over Vendor Relationships

The SolarWinds hack was not unique, but its high profile and government impact can be expected to release the hounds of lobbying and legislation, which may demand stricter practices at large independent software vendors and improve supply chain safety.

Even so, as always, ultimate responsibility for everything installed on a network falls to the owners of that network, so let the buyer beware.

In verifying a software maker’s supply chain security practices, customers must work around visibility limitations placed there to protect sensitive security details and intellectual property. The chief way of doing so is to create and enforce procurement standards that place formal due diligence requirements on software suppliers.

Investigating the certifications a vendor holds for regulatory frameworks such as PCI or HIPAA can also be useful. The audits that software companies must pass for such certifications attest to sound internal governance over security systems and procedures.

2. Redouble Efforts to Be Scrupulous About IT Hygiene

Setting aside the unique threat of unsupported legacy software, even fully patched, up-to-date applications are susceptible to supply chain attacks.

Therefore, adapting a zero-trust orientation of sorts to the supply chain, all software should be regarded as a threat, so that removing software from the production environment is properly regarded as removing a potential threat. With that orientation in mind, the financial and business value of projects to decommission software become more apparent and easier to justify.

Attention to supply chain risk can also inform corporate policies and standards that require software and services to be validated by the IT security organization on an ongoing basis. Scrutinizing the pedigree of every application, microservice and plugin is likely impossible, and that goal is more obtainable for some solutions than others.

3. Validate and Adapt Cyber Measures that Protect the Supply Chain

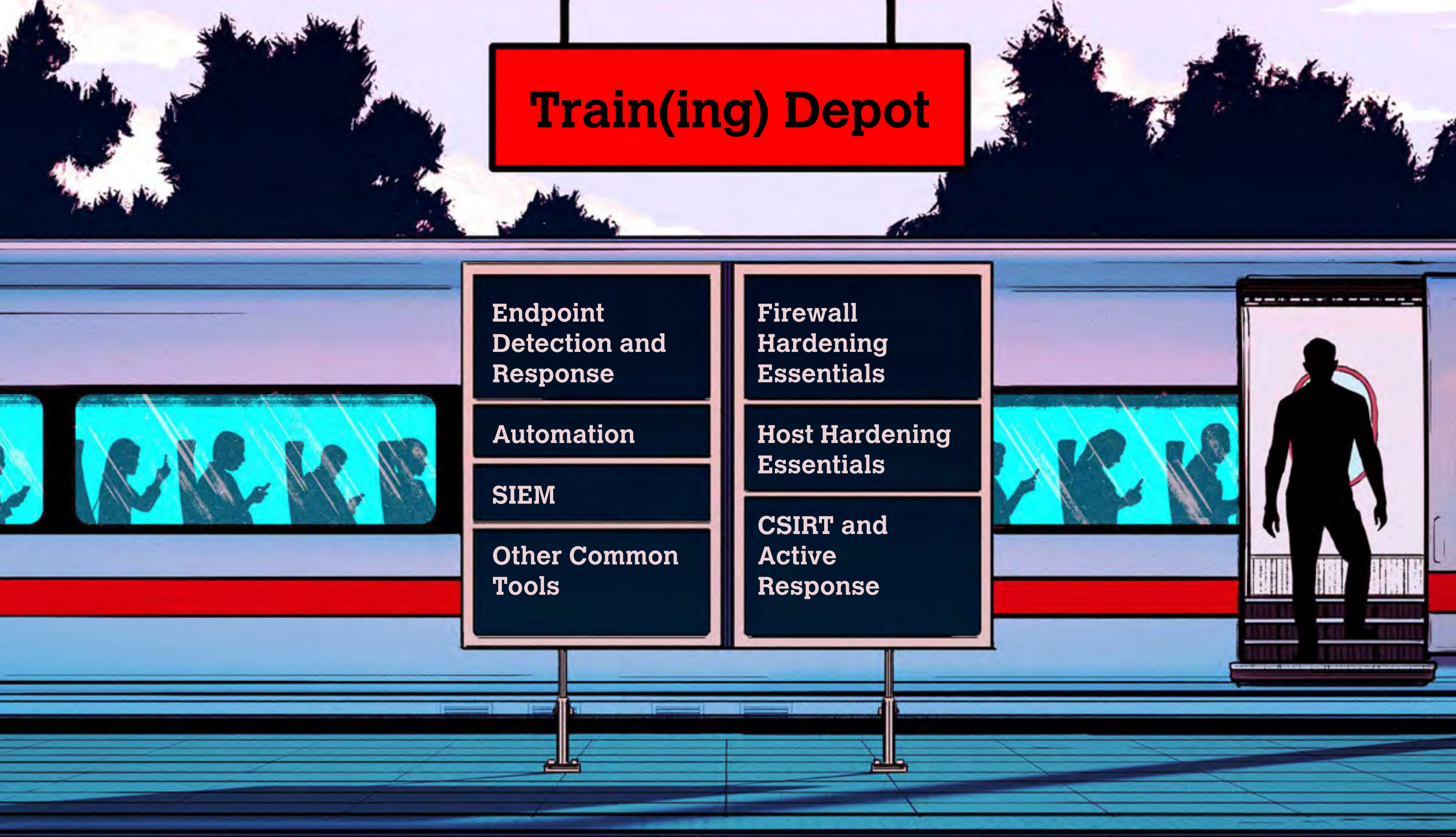
One defining characteristic of supply chain attacks is their sophistication; in most cases, the adversary is a nation-state. Guarding against and detecting them is difficult—the SolarWinds compromise was not found for months—in any of the thousands of affected organizations.

In response, existing security standards should be reassessed through the lens of threats from the supply chain, bearing in mind that, in terms of IT and security operations, measures to address software supply-chain risk overlap with those for other threats.

Supply chain compromises may be detectable by the threat-hunting practices that are becoming common in large organizations. An attack may be revealed by unusual patterns of data access, signs of lateral movement or evidence of data exfiltration. ●

MATT GILLESPIE is a technology writer based in Chicago. He can be found at www.linkedin.com/in/mgillespie1.

An expanded version of this article appears in the April *Insights* newsletter.


Train(ing) Depot
Endpoint Detection and Response
Automation
SIEM
Other Common Tools
Firewall Hardening Essentials
Host Hardening Essentials
CSIRT and Active Response

All Aboard for Fundamentals

BASICS CAN BE THE BEST ANSWER TO STOPPING THE ADVANCE OF TODAY'S THREATS

BY DANIEL ADDINGTON, CISSP; ED BROWN, CISSP; AND MIKE MANROD, CISSP

THE LEVEL OF INVESTMENT IN CYBERSECURITY—in terms of time, effort and capital expenditure—has increased by leaps and bounds for those responsible for an organization's technology infrastructure. It makes sense: Our devices and IT infrastructure are under continuous assault, and our defenses keep playing catch-up.

In this cyclical dance of attack and defense, the game evolves, and cybersecurity professionals benefit from the compound interest and the right combination of resources. We now have a dizzying array of offerings to provide all manner of protections from today's threats, such as ever-evolving ransomware.

Despite the advances we've made, something else is needed beyond purchasing the latest AI-enabled software or automation tools. We need a renewed focus on cybersecurity fundamentals.

ILLUSTRATION BY RAUL ALLEN

CONTENTS

If we build a strategy around responding to every attack—without context, as a new phenomenon—we will always be behind the power curve.

KNOWING WHEN AND HOW TO RESPOND

At this point, the number of products and services an organization can buy are practically limitless. As such, the first step is scoping what types of controls are needed and how these products need to be managed. This is done by analyzing the attack surface from the perspective of an attacker.

In martial arts we learn that while the specific attack options may be limitless, certain patterns emerge that we may use to orient our defensive strategy. If we build a strategy around responding to every attack—without context, as a new phenomenon—we will always be behind the power curve.

However, if we account for the fundamental nature of common attack methods, such as a punch or a kick, we can develop "defense and response" frameworks that are not entirely dependent on the exact nature of each specific encounter.

In cyber, at the most basic level, there are two types of attack—those requiring human interaction and those that do not. If a user is required, it usually involves a malicious attachment or link seeking credentials to spy on or control the host system.

For cases not requiring a user, the attack typically exploits an application, system or service to gain that initial foothold—often, a remote code execution vulnerability or compromised credential. Regardless of how entry is obtained, an attacker will take a range of steps to accomplish their ultimate objective. From this logic, we can identify a short list of tactics to prevent using security controls and scenarios to trigger response activities.

If we apply data on how organizations are typically compromised and then—if available—data on how a specific organization is attacked, the *next best steps* for defense and response become obvious. While the specific actions will vary wildly based upon the

SELECTING ENDPOINT DETECTION AND RESPONSE PRODUCTS

Choosing the right endpoint detection and response (EDR) product may mean the difference between a rough week that turned out well, and a career-defining failure to protect your organization.

There are a few critical attributes needed for any successful EDR product that represent non-negotiable items you cannot live without.

It should detect and alert on the most obvious signs of compromise we all need to be concerned about, ranging from activities consistent with host compromise to events consistent with expanding their foothold or lateral propagation. These include common tools such as Armitage/Cobalt Strike, methods such as the many flavors of Mimikatz or techniques such as remote PowerShell or WMI calls used to compromise other hosts.

At a more fundamental level, these tools need to provide a remote command line (CLI) to the host and remote containment, without the risk of giving the attacker more powerful credentials. Simply put, if the EDR tool does not provide the ability to get a remote CLI to the host, on or off network, this capability should be a dealbreaker.

This remote command line should allow you to perform initial triage, perform a memory dump or search for and pull down any artifacts on a remote system, as long as it has some level of internet connectivity. Without this capability, you may find yourself flying blind, and that is never a situation you want to experience.

On another note: If you want elevated visibility and do not have the budget for an EDR, seriously consider Sysmon or even just logging /var/log/messages and /var/log/secure to a SIEM tool. While this will not provide a response capability, it will give most of the visibility at no direct cost. Adding a simple/primitive response action could be as easy as a PowerShell script with local admin credentials to hit WMI and shut down network interfaces for the device.

—D. Addington, E. Brown and M. Manrod

particular threats and an organization's IT maturity level, existing resources ranging from the CIS 20 to MITRE ATT&CK will illuminate the path to establishing what controls should be deployed or refreshed. These tools will also inform where response efforts should be focused and how tuning, refinement and hardening efforts should be directed.

STARTING WITH UNIVERSAL SECURITY CONTROLS

There is a typical list of common controls practically every organization should have to stop the range of threats now out there.

Since email, messaging and malicious web content are common entry points for malware, it makes sense to first protect these potential threat vectors.

Controls such as reliable and modern email gateways, firewalls, web application firewalls, next-generation antivirus and endpoint detection and response are obvious table stakes. Advanced controls, ranging from Layer 7/application and user awareness for firewalls and malware sandboxing and link proxy/emulation for all email are critical and necessary. And with next-generation antivirus and endpoint detection and response, you must log and analyze everything on a host, perhaps with a boost from machine learning algorithms.

Of course, each topic covered in this article warrants a library's worth of books—and, they have already been written. That said, there are a few key points worth calling out explicitly in this article.

FIRST STEPS IN EMAIL PROTECTION

The same principles discussed for network security also apply to the subtopic of email security. Nuances are of paramount importance, and since email is the most common delivery mechanism for malicious content, email security and forensics very relevant.

It goes without saying, the first step is to manage DNS/MX/DMARC/DKIM records to reduce and refine the attack surface. However, at a deeper level, organizations need to guard against malicious inbound and outbound email, irrespective of the perceived trust levels that apply.

New malware and phishing constitute a continuous threat and configuration problem requiring protections ranging from URL rewrite to malware sandboxing and even automated isolation of bad email messages after delivery, to deal with active threats that are discovered later due to evasion techniques.

—D. Addington,
E. Brown and M. Manrod

Endpoint detection and response. First and foremost, all controls procured to stop an attack must validate their effectiveness against the specific threat you are concerned about. Solutions are expensive, and well-scoped engagements of expert testers are comparatively reasonable in cost. Invest the effort to validate the efficacy of every critical solution that you select and use this data to push back on all solutions providers to enhance selection and to improve the value they provide to your organization. *(See "Selecting Endpoint Detection and Response Products," p. 33.)*

Automation. Assume any layer of defense may be bypassed. There is another realm of controls dedicated to discovering when the fundamental controls fail. They enable response and containment efforts to stop an intrusion from becoming a catastrophic compromise. For some organizations, there are gaps in foundational controls—these should probably be resolved before moving much further. For organizations that have moved past the outer layer of automated defense, the next layer is intelligence and response.

SIEM. While we already touched on the fundamental topic of endpoint detection and response, or EDR, there are many other intelligence and response products that are essential if you are dealing with advanced attacks. The most obvious intelligence product is the brain of your security apparatus—the Security Incident and Event Management (SIEM) tool.

These products should include alerts on the specific scenarios you defined as your likely attack scenarios, across your control ecosystem, and should also feed into a robust response and containment process that can identify and contain attacks at the earliest phase possible.

The SIEM tool should tell you when something is going

It is possible for an attacker to perform an exploit over 443 and obtain a reverse web shell, without the firewall ever seeing anything unusual, if the attack is well executed and traffic is not decrypted.

wrong at the fundamental level and allow you to search for anything you want to know as you seek to identify and address specific threats at a more mature level. Implemented properly, it is the centerpiece of any mature security apparatus.

Other common tools. While there is a wide range of possible product combinations beyond the SIEM tool to deal with various scenarios along the Cyber Kill Chain, defining which scenarios you care most about will help focus your investment.

The first and most obvious areas are dealing with malicious traffic consistent with C2 or lateral traversal and malicious use of powerful accounts or known exploits, within the environment. This is the realm of user/entity behavior analysis (UEBA), network detection/response (NDR) and deception tools.

Essentially, you want to know when a user account behaves in a suspicious manner or when network traffic is consistent with known attack patterns, either because the pattern is recognized or because the attacker took the bait of a deception/honeypot system.

A plethora of other essential technologies are needed to secure your enterprise, ranging from secrets management and other identity and access management (IAM) tools to data loss prevention (DLP), cloud access security brokers (CASB), vulnerability management (VM) and many more.

For the sake of brevity, we have limited this discussion to technologies in the direct path of early stages for the most common attacks; however, you could apply the thought process at deeper levels of detail in organizations of greater maturity.

DEPLOYING CONTROLS IS NOT ENOUGH

If you are like many larger enterprise environments, the prior section may have seemed like your ghost of projects past. Deploying these technologies is only the price of admission—having them well tuned and integrated with an effective response process is what actually provides a fighting chance at stopping adversaries from compromising your environment.

For this, a closer look at the specific attack methods that are successful at bypassing the usual security controls will be helpful.

FIREWALL HARDENING ESSENTIALS

It is essential that we layer defenses, so attackers have additional obstacles as they move closer to their intended objective. For hardening fundamentals, we should focus on the failure modes and what typically goes wrong across the layers.

A common issue relates to how organizations deal with encrypted traffic. The obvious first step is to apply inspection of SSL to outbound web traffic—a relatively easy task, although issues such as certificate pinning require some administration and effort.

One of the more difficult challenges is handling of inbound encrypted traffic. While the technical solutions are simple, there are high expectations for external web applications, and such inspection may add considerable latency. This creates a dangerous blind spot, since the cert usually is on the load balancer or app server, meaning the firewall is potentially blind to attacks over a connection directly to an application. It is possible for an attacker to perform an exploit over 443 and obtain a reverse web shell, without the firewall ever seeing anything unusual, if the attack is well executed and traffic is not decrypted.

While there are multiple solutions available, one easy option is to combine a cloud web application firewall (WAF) with a content delivery network (CDN) to provide a security layer, while also improving availability and performance through caching and greater resiliency. This can align the business need for availability and security requirement for visibility and prevention into one product for an easier internal sell.

HIGH-RISK PORTS, PROTOCOLS AND SERVICES

Italian civil engineer and economist Vilfredo Pareto observed in 1906 that 20% of the population owned 80% of the wealth in Italy at the time. His observation, now called the Pareto principle, applies to what we need to protect in a very real way, even though the exact ratios are a little more dramatic in our line of work.

Vulnerabilities and exploits tend to concentrate around a specific range of ports, protocols and services. If we are rigorous in controlling, inspecting and blocking these types of traffic, we have a form of leverage that improves our return on effort for network or host hardening efforts.

Here are the ports and services that probably should demand the most immediate attention *(see chart on right)*.

While this list is not exhaustive, it provides a starting point for what to protect, at both a network and a host level.

—D. Addington, E. Brown and M. Manrod

PORT	SERVICE
3389	RDP
445	Directory Services / SMB "SAMBA" replacing NETBIOS – PSExec
137/138/139	NetBIOS
21	FTP
22	SSH
389	LDAP (not encrypted – should be LDAPS on 636)
80	HTTP (not encrypted – should be HTTPs on 443)
53	DNS (used for C2)
135	RPC (593 is RPC over HTTPs)
69	TFTP
1433/1434	MSSQL
161	SNMP
Ephemeral Ports	If open, these can open up a window of opportunity for many attacks

There are other ways to solve this problem; just make sure that your solution provides visibility into inbound encrypted web traffic and effective prevention of inbound attacks.

Importantly, attackers are always working hard to bypass inspection via techniques such as obfuscation, sandbox evasion or finding flaws in applications that won't trigger a rule or protection. Only through aligning network security, application security and active response does an organization have a fighting chance at repelling evasive attacks.

From an application perspective, scanning, testing and effectively remediating issues cannot be neglected just because a well-tuned WAF is in place. The same is true at the infrastructure level for patching and host hardening.

That said, at the network layer there are some applications and ports/protocols that are higher risk than others. It is essential to identify and block or isolate these high-risk communications from the internet and between trust zones.

Thought also must be given to the specific segmentation strategy, to ensure the network/security topology is conducive to protecting sensitive data and preventing lateral movement. This could be accomplished using a combination of approaches ranging from traditional firewalls/zones to micro segmentation, host firewalls and virtual firewalls (e.g., NSX).

The easy part is getting the right solutions deployed. The real protection only comes in after tuning and refining the rules—both at Layer 3 and Layer 7—and validating their effectiveness. *(See "High-Risk Ports, Protocols and Services," above.)*

HOST HARDENING ESSENTIALS

Host hardening and protection should be a cornerstone of protecting any organization. Some problems are handled via agents or upstream security controls—it is after all, the goal—to stop threats before they reach a host.

However, advanced threat actors may evade other controls, making host hardening

CONTENTS

a decisive factor in thwarting attacks. Once agents, logging and visibility/response are covered, host issues often come down to ports that are open, as well as applications, scripts and services that are allowed to run.

Finally, there is a broad range of topics to consider related to more advanced controls ranging from ASLR (address space layout randomization) to UAC (user access control) and the previously mentioned IAM that includes password/secret management. The range of possible attack vectors and defensive configurations can get vast quickly.

That said, the goal does not need to be perfection. Instead, the objective should be an elevated level of prevention, detection and response that is sufficient to delay, deter and frustrate attackers—while the response has a chance to contain and remediate.

Another common issue at the host level is with inspection of remote/unconnected devices, as we expect unconventional scenarios in the post-COVID world.

For the remote workforce, it is imperative to have an agent-based solution that extends traditional network defenses, to a host level—even when not on network/off VPN. Of course, always-on VPN can accomplish some of the same objectives, although it seems a little arcane in the modern cloud/SaaS world.

Finally, most endpoint security solutions ship with a default policy—build upon this policy to harden your endpoints against any threats that use activity not normally expected within your environment. If you block it, they (hopefully) won't come.

For the remote workforce, it is imperative to have an agent-based solution that extends traditional network defenses, to a host level—even when not on network/off VPN.

CSIRT AND ACTIVE RESPONSE

When infantry set up concertina wire and mines, the idea is not that an attacker will never make it through these obstacles. Instead, the intention is that these obstacles will frustrate the enemy, slow the approach and make the attack more obvious.

So too an effective set of security controls will enable and inform your response efforts to hopefully repel an attack. And like close air support works to protect infantry, community intelligence sharing such as Information Sharing and Analysis Centers (ISACs) or other regional/vertical-specific partnership organizations can provide critical intel when you need it most.

At the end of the day, the SOC and IR functions are the most essential elements of a mature strategy and should closely integrate with VM to correlate attacks with vulnerabilities and also with security engineering to enhance controls dynamically and adaptively in response to threats.

OUR JOB IS DIFFICULT, BUT DOABLE

The deck seems to be always stacked against us. That said, as defenders we have the benefit of shared knowledge and intelligence that may converge in the form of best practices, to keep us better protected against the latest threats.

Individually, none of us are ever guaranteed success. Working together, we can continuously elevate our collective defenses and make attackers work harder to realize their objectives.

Over time, this may be what it takes to win our war against the intrusion and compromise of the systems and information we all protect. ●

DANIEL ADDINGTON, CISSP, provides management, leadership and technical guidance for the security team at Grand Canyon Education. **ED BROWN**, CISSP, leads IT Security Engineering for Grand Canyon Education. **MIKE MANROD**, CISSP, currently serves as the CISO for Grand Canyon Education, responsible for leading the security team and formulating the vision and strategy for protecting students, staff and information assets across the enterprise. Additionally, the authors give their colleague, **CHRISTIAN TAILLON**, special thanks for his expert contributions to this article.

ADDITIONAL RESOURCES

https://owasp.org/www-project-top-ten/

https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization

https://www.sciencedirect.com/topics/computer-science/evasion-technique

https://nmap.org/book/man-bypass-firewalls-ids.html

https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon#overview-of-sysmon-capabilities

https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

https://www.nationalisacs.org/

https://github.com/christian-taillon/sunburst-hunting

Take the 10 for 10 Challenge

THE CENTER IS CELEBRATING ITS FIRST DECADE WITH MORE WAYS TO MEET ITS MISSION

BY PAT CRAVEN

THIS YEAR your Center for Cyber Safety and Education is celebrating its 10th anniversary. In 2011, the (ISC)² Board of Directors formed a charitable trust called the (ISC)² Foundation to help members give back to their communities and share their passion for cybersecurity and cyber safety. Since then, hundreds of thousands of children, parents and senior citizens have benefited from the Center's mission, built and driven by *you*.

Working with great partners like (ISC)², Raytheon, KnowBe4, SAIC and (ISC)² Chapters, we've awarded more than U.S. $1.5 million in scholarships and financial aid to 600-plus students.

What started off as providing access to jointly created educational slide decks with a U.K.-based organization called ChildNet has evolved into the award-winning Garfield's Cyber Safety Adventures and the Safe and Secure Online programs in more than 20 languages. We now provide nearly 150,000 lessons a year to families around the world.

And, working with great partners like (ISC)², Raytheon, KnowBe4, SAIC and (ISC)² Chapters, we've awarded more than U.S. $1.5 million in scholarships and financial aid to 600-plus students. This year, we will award another U.S. $230,000 to nearly 70 students!

In short, it's a safer cyber world today because of our members.

We have big plans for the next decade to deepen our impact worldwide, and I'm sure you'll want to be part of that important work. I invite you to join us for the 10 for 10 Challenge.

I hope these simple ways inspire you to join in our celebration of the lives we have impacted the last decade and help us kickstart the next one. Learn more at www.IAmCyberSafe.org/s/anniversary and please drop us a note at center@isc2.org about the 10 things you're doing to make it a safer cyber world. ●

Here's How You Can Join the 10 for 10 Challenge

1. Share our website with 10 people.
2. Share your love of the Center on social media 10 times and tag the Center.
3. Volunteer one hour a month for 10 months, either training others how to be safe and secure online, or as a scholarship reviewer.
4. Donate $10 a month for 10 months.
5. Recruit one new volunteer each month for 10 months.
6. Post one new cyber safety tip a month on your social media profiles for 10 months and tag the Center.
7. Invite 10 people to donate $10.
8. Contact 10 local elementary schools, libraries or youth groups and introduce them to the multi-award-winning Garfield's Cyber Safety Adventures.
9. Completely unplug for 24 hours once a month for 10 months.
10. Talk with bosses at work about the Center's programs and mission and discuss how the company could get involved.

Pat Craven is the director of the Center for Cyber Safety and Education and can be reached at pcraven@isc2.org.

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

"XDR is not a solution, it's a menu. And we, as the IT managers, the CISSPs, the network managers, the consultants, we have to work with our clients and stakeholders and figure out what's the soup, what's the salad, what's the appetizer, what's the entrée, what's the dessert, and what's the drink, and then weave this path through."

—Raj Goel, CISSP, CTO, Brainlink International Inc., webinar panelist during an (ISC)² Think Tank webinar, "Doing XDR Right: What It Is and What It Can Do for Your Organization"

"With 56% of our survey participants falling victim to at least one ransomware incident in the last year, we can say with some certainty that a ransomware incident is, of course, *when* and not *if*. ...And so, the importance of visibility and response, and the speed of that response to a suspicious incident, continues to grow, as does the criticality of how your organization can actually operationalize intelligence and security response tools."

—Ian McShane, CISSP, VP of Product Marketing, CrowdStrike, and speaker during an (ISC)² Secure Webinars EMEA series, "2020 CrowdStrike Global Security Attitude Survey"

"We can't really ignore the fact that the major players in the IoT/ICS hardware/software space are really lacking in considering security as part of their software development practice."

—Russ Harland, CISSP, CCSP, SSCP, Global IT Security Architect, during (ISC)² Think Tank webinar "Darktrace #3: The Industrial Immune System: Securing IT/OT Converged Ecosystems"

"When it comes to writing [software security] policies, perhaps the most important soft skill is the humility to accept constructive criticism and an open mind to accept change."

—(ISC)² content contributor Bob Covello

Source: (ISC)² blog post "The Importance of a Good Software Security Policy"

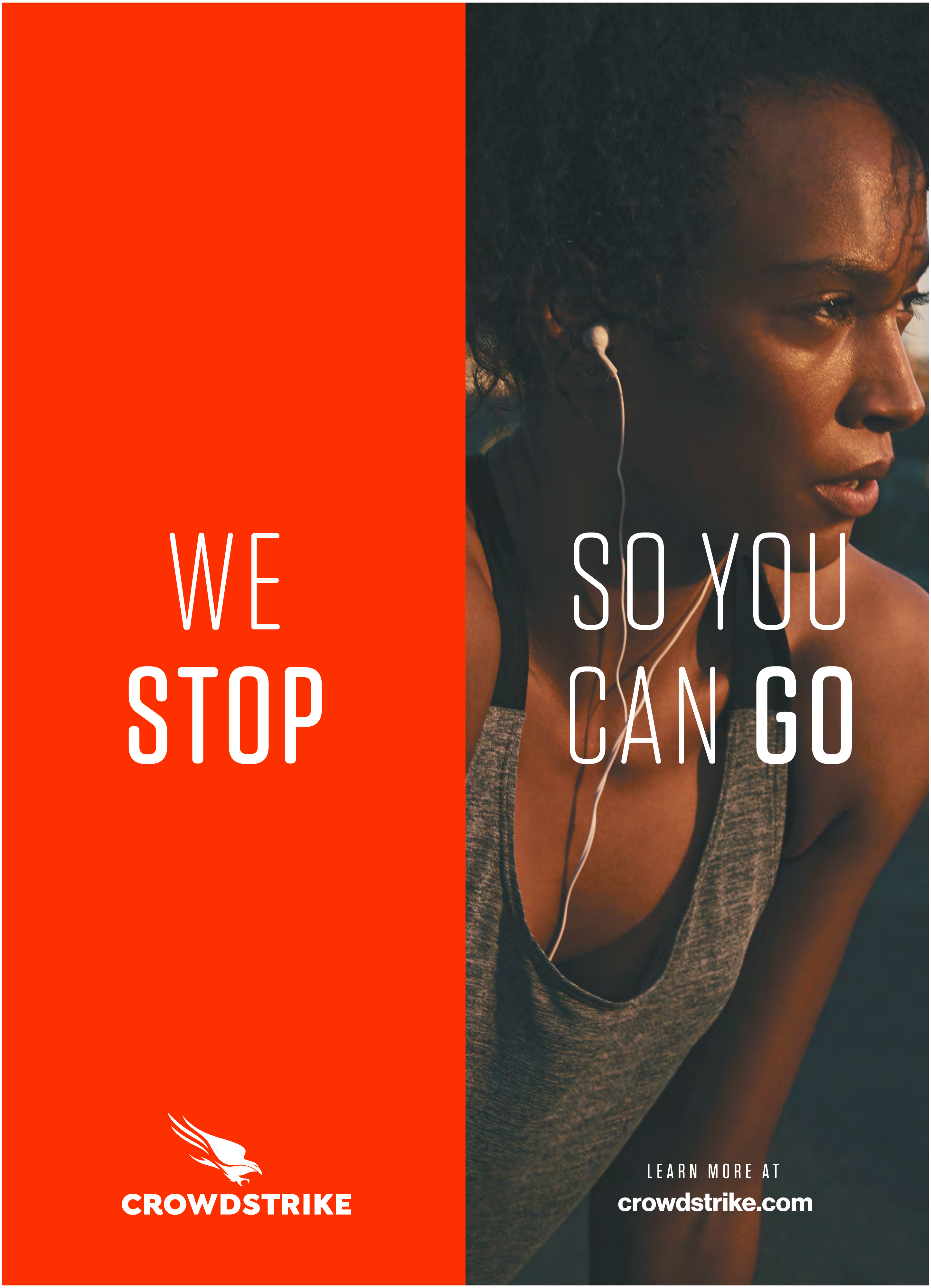
"It has generally been assumed enterprises are better equipped to fight cybercrime than smaller organizations, but findings indicate that SMBs may be working off the same playbook."

—(ISC)² content contributor Pedro Pereira

Source: (ISC)² blog post "How Small Businesses and Big Enterprises Structure Their Cybersecurity"

"I was very excited when I first heard about XDR [extended detection and response] a few years ago, because I thought, 'OK, great. Now within the organization you've got a way of pulling all this data together and making sense of it and telling you what that one thing is.' The reality, of course, is that we haven't really even defined what XDR is and no one solution is going to take care of everybody's needs, so it's not that simple."

—Lloyd Diernisse, CISSP, CCSP, CAP, LSSBB, PMP, CSM, CMMI-A, ITIL-F v3, SME, and thought leader with Copper River Enterprise Services, webinar panelist during an (ISC)² Think Tank webinar, "Doing XDR Right: What It Is and What It Can Do For Your Organization"


WE
STOP
SO YOU
CAN GO
CROWDSTRIKE
LEARN MORE AT
crowdstrike.com