

A POTENTIAL UPSIDE TO RANSOMWARE THREATS

# InfoSecurity PROFESSIONAL

MARCH/APRIL 2022

Practical Advice. Actionable Insights.

Pam Rowland,  
Mike Manrod and  
Christian Taillon on  
building a training  
range without  
breaking the bank.

## HELPING OTHERS TO HELP THEMSELVES

CREATE CYBER RANGES

FIND HIDDEN ASSETS

FLEX SOME MUSCLE

(ISC)<sup>2</sup><sup>®</sup>



# Get Involved and Make a Difference.

Serving as an (ISC)<sup>2</sup> volunteer is a rewarding experience that provides the opportunity to:

- Share ideas and expertise
- Collaborate with colleagues outside your usual work environment
- Interact with industry experts
- Make an impact in the local and cybersecurity communities

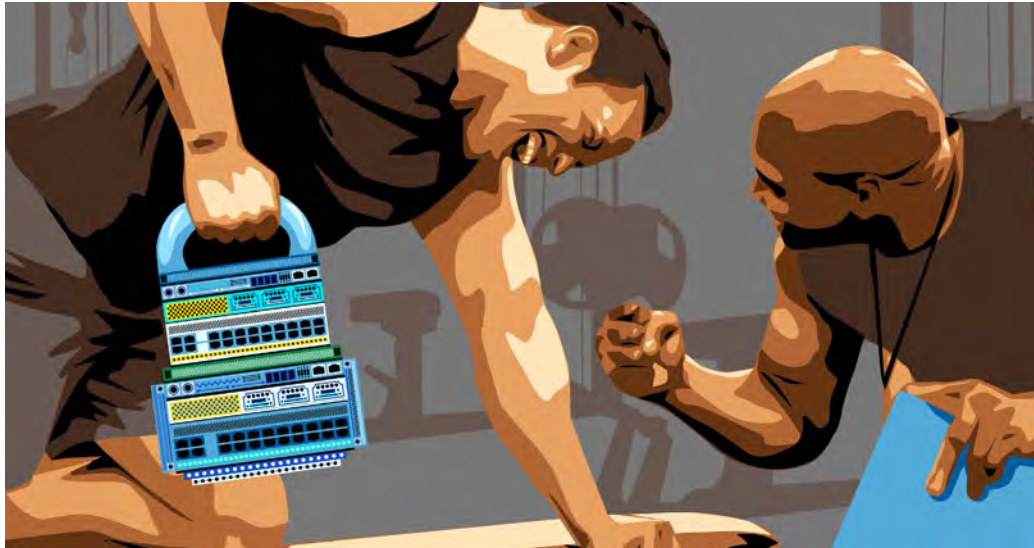
The larger the pool of volunteers, the greater the variety of perspectives and ideas that benefit the organization. Our volunteer base is diverse, which brings a broad perspective, a wealth of ideas and a depth of understanding of member interests to the table.

(ISC)<sup>2</sup> offers a variety of ways for members to get involved, from short-term volunteer projects to committee, council and board services. With every new volunteer, (ISC)<sup>2</sup> grows more energized, diverse, inclusive and ready to reach our common goals.

---

**Give back and connect with your peers.  
Be a part of the (ISC)<sup>2</sup> Volunteer Program!**

[Learn More](#)



Time to pump up your cybersecurity skills.

PAGE 31

## FEATURES

### 20 A Range of Experiments ... on a Budget

BY MIKE MANROD, CISSP; PAM ROWLAND, PH.D.;  
AND CHRISTIAN TAILLON, CISSP

How to build a cyber training range without breaking the bank.

### 26 Are You in the Dark About Where Your Assets Are?

BY CHARLES CHIBUEZE, CISSP

A member explains how he found a way to locate hard-to-find assets.

### 31 Working Out

BY ROBERT WEBSTER, CISSP

Taking the time to build a structured program will make it easier to flex some serious security muscle when needed.

## DEPARTMENTS

### 5 Editor's Note

There's more than one way to do it yourself.

BY ANNE SAITA

### 8 Executive Letter

Expanding pathways to cybersecurity careers.

BY DR. CASEY MARKS

### 10 Field Notes

Latest research shows impact of ransomware on cyber funds; new program to boost soft skills; introducing new (ISC)<sup>2</sup> leaders; most popular webcasts.

### 15 Member's Corner

Don't discount the value of DIY cybersecurity.

BY JASON McDOWELL, CISSP

### 18 Help Wanted

A better way to attract diverse job candidates.

BY DEBORAH JOHNSON

### 36 Office Hours

A DIY approach to career advancement.

BY SPENCER WILCOX, CISSP

### 7 ADVERTISER INDEX

Cover photograph by Mark Lipczynski

Illustration (above) by Daniel Hertzberg

Illustration (right) by Jan Feindt



# CISCO SECURE

Protecting what's now  
and what's next.



# EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

## There's More than One Way to Do It Yourself

**YEARS AGO**, I created a fun run to cap a year's worth of group marathon training with the San Diego Track Club. At the time, I lived about a mile from a neighborhood famous for its winter holiday displays. There's even a [Wikipedia entry](#) about it.

Without any formal training in race directing, I cribbed ideas where I could and picked the brains of race directors I admired. I considered what resources I needed, and how to get them on the cheap since there was no entry fee to cover costs. I researched required permits, I mapped out a five-mile course that minimized risks with motorists and, to add my own twist, made it a predicted run—that is, everyone had to predict their finish time within seconds and without wearing a watch or listening devices that might help them cheat. That first year, it worked brilliantly—the top two “winners” finished first and last.

Across the subsequent years I added to my initial efforts, bringing in costumed volunteers and giving each participant a branded ceramic mug made by an organization that gives jobs to the intellectually disabled. The start and finish lines moved twice before settling for good in an area with plenty of parking while maintaining a still-challenging course.

I left the track club several years later, but until COVID hit, I annually returned by invitation to see what had come of my little fun run. It had grown in both size and ambition without losing its initial just-wing-it-and-have-fun flavor. My little DIY project had exceeded my expectations.

I never thought of that fun run as a do-it-yourself project until we began putting together this issue, which is focused on ways to save money (maybe even time) by putting together your own cybersecurity programs and hiring practices. We do this with our careers as well, self-educating to improve ourselves, or finding new ways to improve productivity or add value to our organizations that isn't outlined or outsourced.

It's about that time of year where self-proclaimed goals for 2022 begin to taper. If you've gotten off track with important goals, now is as good a time as any to figure out why a practice isn't working and make a change to get back on track. Don't give up! Do turn to experts for advice—including educational opportunities through (ISC)<sup>2</sup>. Don't depend entirely on others but do strive to be the best you can be. A little self-help and sweat equity can lead to a lasting legacy that withstands the test of time. ●



**Anne Saita** lives and works in San Diego. She can be reached at [asaita@isc2.org](mailto:asaita@isc2.org).

Photograph by Louise Roup

## CONTRIBUTORS

Two of the three bylines—Grand Canyon Education CISO **Mike Manrod**, CISSP, and threat response engineer **Christian Taillon**, CISSP—may ring familiar since both contributed to the magazine in 2021. The third author of our cover story on cyber ranges is **Dr. Pam Rowland**, the associate dean of computer sciences and technology in the College of Science, Engineering and Technology at Grand Canyon University. Pam's passion project is CybHER, which she co-founded to empower, motivate, educate and change the perception of girls and women in cybersecurity.



Another member-author is Nigeria-based senior security consultant **Charles Chibueze**,

CISSP, who shows how to establish your own asset management program. When he isn't helping financial companies, he can be found reading—for fun and for educational courses.



**Rob Webster**, CISSP, shares how he learned to flex some serious cyber muscle. This

former collegiate musician once played the sousaphone for the University of Southern California Trojan Marching Band.



**Mark Lipczynski**, cover photographer, has been honing his craft since childhood in northeastern

Ohio, photographing trains with his dad and brother. He now lives and works in Phoenix with his family. Clients include Major League Baseball, *Essence Magazine*, *Marie Claire* and more.

This issue's “Working Out” article is elevated by **Daniel Hertzberg's** lively artwork. In addition to teaching and playing hockey, Daniel illustrates for *Time*, *The New Yorker*, *The New York Times*, *Rolling Stone*, Major League Baseball, ESPN and more.



# Build Your **Best Team** with our new **Entry-Level Certification**

Cybersecurity team leaders can help answer the critical need for more cyber professionals with the **new Entry-Level Cybersecurity Certification from (ISC)²**, the leading provider of cybersecurity certifications.

Designed as a starting point for students, professionals and career-changers, the Entry-Level Cybersecurity Certification **demonstrates knowledge in the key foundational concepts in information security and requires no work experience** – just a passion for cybersecurity and the desire to dive into an exciting field that protects the world from cyber threats.

**Who on your team is ready to start their path to cybersecurity leadership?**

Entry-Level  
Cybersecurity  
Certification

An (ISC)² Certification

Show Them the Way

**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)<sup>2</sup> 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/March-April-2022>

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

### ADVERTISER INDEX

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

(ISC) <sup>2</sup> Volunteer Program .....	2	Illumio .....	19
Cisco .....	4	Identity Defined Security Alliance .....	24
(ISC) <sup>2</sup> Entry-Level Cybersecurity Certification .....	6	Securonix.....	25
(ISC) <sup>2</sup> Commit to CCSP .....	9	(ISC) <sup>2</sup> The Power Duo of Cybersecurity Certifications .....	30
SEM .....	11	SecurityScorecard.....	35
(ISC) <sup>2</sup> Secure Summits.....	14	Reciprocity.....	37
SimSpace.....	16	(ISC) <sup>2</sup> Attend Infosecurity Europe 2022.....	38
Auditboard.....	17		

InfoSecurity Professional is produced by Twirling Tiger® Media. Contact by email: [asaita@isc2.org](mailto: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)<sup>2</sup> 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)<sup>2</sup>. (ISC)<sup>2</sup>, the (ISC)<sup>2</sup> 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](http://www.isc2.org). To obtain permission to reprint materials, please email [infosecproeditor@isc2.org](mailto:infosecproeditor@isc2.org). To request advertising information, please email [lpettograsso@isc2.org](mailto:lpettograsso@isc2.org). ©2022 (ISC)<sup>2</sup> Incorporated. All rights reserved.

### (ISC)<sup>2</sup> MANAGEMENT TEAM

#### EXECUTIVE PUBLISHERS

Chris Green  
+44-203-960-7812  
[cgreen@isc2.org](mailto:cgreen@isc2.org)

Tim Garon  
571-303-1320  
[tgaron@isc2.org](mailto:tgaron@isc2.org)

#### DIRECTOR, CORPORATE COMMUNICATIONS

Jarred LeFebvre  
727-316-8129  
[jlefebvre@isc2.org](mailto:jlefebvre@isc2.org)

#### SENIOR PUBLIC RELATIONS MANAGER

Brian Alberti  
617-510-1540  
[balberti@isc2.org](mailto:balberti@isc2.org)

#### MANAGER, MEMBER COMMUNICATIONS

Kaity Pursino  
727-683-0146  
[kpursino@isc2.org](mailto:kpursino@isc2.org)

#### SR. CORPORATE COMMUNICATIONS SPECIALIST

Andrea Moore  
727-270-9613  
[amoores@isc2.org](mailto:amoores@isc2.org)

### EDITORIAL ADVISORY BOARD

Brian Alberti, (ISC)<sup>2</sup>  
Anita Bateman, U.S.  
Felipe Castro, Latin America  
Brandon Dunlap, U.S.  
Rob Lee, EMEA  
Jarred LeFebvre, (ISC)<sup>2</sup>

### SALES

#### VENDOR SPONSORSHIP

Lisa Pettograsso  
[lpettograsso@isc2.org](mailto:lpettograsso@isc2.org)

### TWIRLING TIGER MEDIA MAGAZINE TEAM

#### EDITOR-IN-CHIEF

Anne Saita  
[asaita@isc2.org](mailto:asaita@isc2.org)

#### ART & PRODUCTION DIRECTOR

Maureen Joyce  
[mjoyce@isc2.org](mailto:mjoyce@isc2.org)

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



# Expanding Pathways to Cybersecurity Careers

BY DR. CASEY MARKS

The current [cybersecurity workforce gap](#) stands at 2.72 million professionals globally, and the truth is that there just aren't enough individuals who are educated to take on all the roles we as an industry need to meet that shortage. One of the key suggestions is that organizations start getting more creative in their recruiting efforts and look for talent in adjacent professions that can be converted to cybersecurity, such as those working in legal, communications or engineering positions. The second prong of that approach is to try to attract younger entrants to the field, even if they don't have information technology or even STEM backgrounds.

The challenge for hiring managers then becomes: How do we assess a given candidate's aptitude for and base knowledge of cybersecurity concepts if they have no direct experience? This conundrum has traditionally been a bit of a leap of faith for organizations, with the understanding that some staff will be able to make the transition through on-the-job training and some won't.

What's needed is a measuring stick to confirm a baseline understanding of the domains in which a cybersecurity professional will be working and provide employers with a level of assurance that a candidate has the foundational knowledge, skills and abilities needed for an entry-level or junior cybersecurity position. This is also a critical indicator of a candidate's future success, so organizations can be confident that the educational investments made in training that staff will pay off in the long term.

It is for this reason that (ISC)<sup>2</sup> is introducing our first new certification since 2015—when the CCSP certification launched. The [Entry-Level Cybersecurity Certification](#), now

in pilot phase, will support cybersecurity career ambitions and help shape a long-term professional development framework that leads individuals to experience-driven certifications as they progress in the workforce. This creates another channel through which we can attract and develop diverse talent to round out the cybersecurity teams of the future. With more than 150,000 CISSPs in the world, clearly support is needed for additional pathways to entering the field.

As a foundational certification, it will play a role in helping employers, educators and governments close the cybersecurity workforce shortage by narrowing the gap between entering the workforce and being able to verify and advance skills through independent and globally recognized industry qualifications. Additionally, the new entry-level qualification will provide more clarity for candidates who aspire to eventually obtain the CISSP credential.

Built on industry insights, the exam tests candidates on five domains—security principles; business continuity, disaster recovery and incident response concepts; access controls concepts; network security; and security operations. We've compiled an [exam outline](#) with more details on the content that each domain covers. A [training course](#) is also available to help exam candidates prepare and familiarize themselves with the domain areas.

This is a major shift for (ISC)<sup>2</sup> and for the industry, and we're excited about the prospect of igniting the passions of so many individuals who may have thought cybersecurity certification was beyond their grasp. By expanding the pathway to entry, we believe organizations will have new opportunities to build security teams for the long haul in order to inspire a safe and secure cyber world for all. •



**Casey Marks** is the chief qualification officer at (ISC)<sup>2</sup> and can be reached at [cmarks@isc2.org](mailto:cmarks@isc2.org).



NO MORE!  
EXCUSES!



CCSP®

Certified Cloud  
Security Professional

An (ISC)<sup>2</sup> Certification

Is achieving the CCSP one of your goals this year?  
Maybe you've started your pursuit but need a little push.  
With any goal, the best way to stay on track for success is  
to develop a plan and commit to it.

That's why we created the (ISC)<sup>2</sup> Exam Action Plan to  
help you move forward with confidence. Invest in you by  
pursuing the most in-demand vendor-neutral cloud security  
certification, named the No. 1 certification survey respondents  
plan to earn in 2022 by *Certification Magazine*.  
You've got this.

## Invest in You with CCSP Certification

Get Your Action Plan



# FIELD NOTES

A ROUNDUP OF WHAT'S HAPPENING IN (ISC)<sup>2</sup> COMMUNITIES

## (ISC)<sup>2</sup> Study: C-Suite Ready to Invest More People, Products to Combat Ransomware

IF YOU FIND YOUR ORGANIZATION is on a cybersecurity hiring or spending spree, you might credit ransomware. The steady surge of high-profile attacks last year made C-level executives more willing to invest in technology and staff to keep ransomware gangs at bay.

That was among the findings in a recently released (ISC)<sup>2</sup> study, *Ransomware in the C-Suite: What Cybersecurity Leaders Need to Know About What Executives Need to Hear*. Researchers surveyed 750 executives across the U.S. and the U.K. and found high confidence in organizations' ability to defend against ransomware attacks. There also

was a strong willingness to invest more resources to keep it that way. Listen to (ISC)<sup>2</sup> CISO Jon France summarize the data [in this webinar](#).

"The study gives cybersecurity professionals a window into what their C-suite cares about when it comes to the potential impact of ransomware. Knowing this, and by tailoring their ransomware education and risk reporting accordingly, security teams can get the support they need to mitigate this high-profile risk to their organization," said (ISC)<sup>2</sup> CEO Clar Rosso.

To learn more details, download a copy of [the report](#).

### STRONG CONFIDENCE

85%

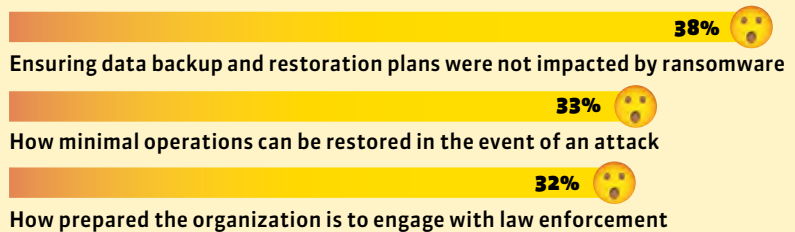
of respondents expressed confidence in their organization's ransomware preparedness



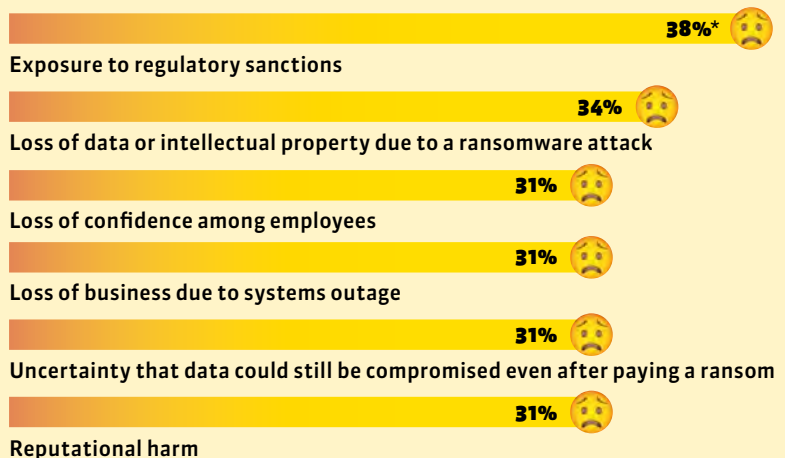
### FIVE TIPS FOR CYBERSECURITY TEAM LEADERS WHEN COMMUNICATING WITH EXECUTIVES ABOUT RANSOMWARE THREATS

- ➔ Increase communication and reporting to leadership.
- ➔ Temper overconfidence as needed.
- ➔ Tailor your message.
- ➔ Make the case for new staff and other investments.
- ➔ Make clear that ransomware defense is everyone's responsibility.

### TOP RANSOMWARE CONCERNS



### GREATEST RANSOMWARE FEARS



\*The concern is higher in the U.K. (41%) than in the U.S. (36%). Heightened awareness and enforcement of the GDPR in the U.K. would explain the high level of concern in the region.

WHO TOOK THE SURVEY: 750 executives for organizations with more than 500 employees—500 based in the U.S., 250 based in the U.K.



## New Volunteer Program Provides More Opportunities to Grow and Give Back

*Members can advance the profession and help solve industry challenges to narrow workforce gaps*

(ISC)<sup>2</sup> MEMBERS AND NON-MEMBERS looking for a way to contribute to their profession now have another venue: a new volunteer program where they can share insights that help influence smarter policy and standards around the world. This program launched in late January seeks meaningful contributions that address industry challenges, such as the cybersecurity workforce gap and educating communities on privacy and security threats, and more.

“With this new program, we hope to inspire more individuals to channel their passion and expertise, give back to their communities, gain useful experience and inspire a safe and secure cyber world,” said Tara Wisniewski, (ISC)<sup>2</sup>

EVP of advocacy, global markets and member engagement.

In addition to helping others, an (ISC)<sup>2</sup> volunteer also develops new skills in areas like change management and conflict resolution; gains a sense of self-accomplishment and self-confidence; and expands their network of cybersecurity professionals. Members and associates can earn continuing professional education (CPE) credits by contributing their time and participating in various professional volunteer activities.

Members and non-members interested in becoming an (ISC)<sup>2</sup> volunteer can opt-in to the volunteer pool by filling out the online form at <https://www.isc2.org/Volunteer>. •

## Introducing the 0205 series of SSD crushers — only from SEM



Global Leader in High Security Information  
End-of-Life Solutions for Over 50 Years

The SEM Model 0205 Series includes two state-of-the-art mobile crushing devices designed specifically for solid state media. Both devices feature solid steel rotary crushers that destroy each and every chip regardless of size, as well as a touch screen interface, attractive and durable metal cabinet, and dual voltage for ultimate flexibility. Designed and made in the USA at SEM's manufacturing facility in Massachusetts. TAA compliant.

### MEDIA ACCEPTED FOR DESTRUCTION:

#### 0205NANO:

- ▲ Compact Flash Type I
- ▲ SD Cards
- ▲ SOIC-8
- ▲ PLCC-32
- ▲ SOIC-16
- ▲ TSOP48
- ▲ Other Microchips

#### 0205MICRO:

- ▲ SSDs
- ▲ Cell Phones
- ▲ Small Tablets
- ▲ Thumb Drives
- ▲ RAM
- ▲ IronKeys
- ▲ PC Boards



In-House Design and Engineering | Custom Solutions for Complex Environments

[www.semshred.com](http://www.semshred.com)





## (ISC)<sup>2</sup> Leadership Expanding to Better Serve Members, Industry

(ISC)<sup>2</sup> RECENTLY ANNOUNCED new executives to the organization to better serve members and the industry at large.

**Jon France**, CISSP, is the organization's first chief information security officer (CISO). In this role, France will be responsible for leading cybersecurity operations, including driving enterprise IT security governance efforts, and will serve as an inspirational advocate for security best practices around the world.

He brings more than 25 years of experience building and leading diverse technology and security teams, setting and executing strategy and delivering programs that empower stakeholders and operations while effectively managing risk across media and telecommunications sectors.

Prior to joining (ISC)<sup>2</sup>, France served as head of industry security for GSMA, a global organization unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change.

**James Prather** is now vice president of global marketing, where he'll be responsible for strategic global marketing initiatives that facilitate member growth and expand global awareness of the (ISC)<sup>2</sup> mission. With more than 30 years of proven marketing operations expertise, Prather will lead all aspects of (ISC)<sup>2</sup> product marketing and global brand activities, working closely with sales, customer experience, strategy and product teams to reach targeted growth goals and increase brand awareness.

Prather previously served as the director of marketing at the Association of International Certified Professional Accountants (AICPA) and CPA.com, a subsidiary of the AICPA.

**John Giddings** is the new VP of global customer experience, where he will help facilitate (ISC)<sup>2</sup> growth by transforming the association's customer service strategy to continually improve customer value and customer experience.

"Under John's leadership, we will double down on our commitment to customers, members and candidates and build a robust customer experience program that evolves with changing customer needs," said Greg Clawson, executive vice president global sales, marketing and customer experience, (ISC)<sup>2</sup>.

Giddings previously served as vice president of global engagement centers and member experience for AICPA.

**Richard Shandelman** is the new vice president of technology, where he will be responsible for implementation, integration and maintenance of core business systems to support the strategy and growth of (ISC)<sup>2</sup>. With 20 years of business leadership, Shandelman will now support operational processes to ensure compatibility, security and integration of various components in (ISC)<sup>2</sup>'s multi-platform environment.

He most recently was head of e-commerce technology and operations for Charlotte's Web Holdings, Inc. •



Jon France



James Prather



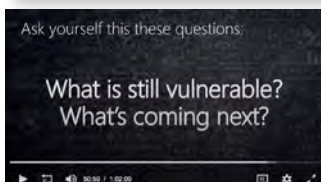
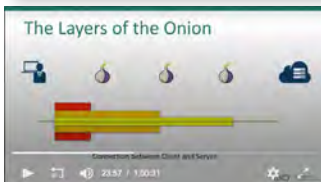
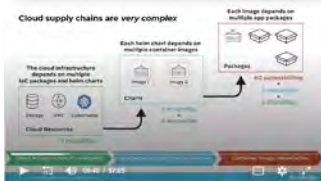
John Giddings



Richard Shandelman

## Best Webinars of 2021

Wondering what were the most popular (ISC)<sup>2</sup> webinars last year? The following—still available on demand—were the highest-ranked webinars in each region through mid-December 2021.



### EMEA Webinars

[Practical Steps to Privileged Access Management: Beyond Password Managers](#)

[Is DoH a Problem or a Solution?](#)

[Leveraging the Assume Breach Mentality](#)

[Go Dox Yourself! Practical Security Awareness Training](#)

[Busting Advanced BotNets](#)

[Cybersecurity Risk for SMB – Defending your Business from Big Threats](#)

[Lighting a Path to Zero Trust: 6 Steps to Implementing a Zero Trust Model](#)

[Detecting Tor in Your Network](#)

[Cyberthreat Game Changer: A New Look at Insider Threats](#)

[Compliance Begins with People: A Case Study from a Leading Financial Institution](#)

### Americas Webinars

[The Many Ways to Defeat Multi-Factor Authentication](#)

[Your Ransomware Hostage Rescue Guide](#)

[Working with Law Enforcement and the FBI](#)

[Beyond the Buzzwords – The Trends Behind SASE and Zero Trust](#)

[Countering Threat Evasion: You Cannot Stop What You Cannot See!](#)

[The Cloud Gambit: Advanced Moves for a Cloud Security Career](#)

[Ransomware Deep Dive: To Pay or Not to Pay?](#)

[Defending Against the Modern Threat Landscape with Zero Trust](#)

[Cloud Threat Report: Supply Chain Attacks – The Early Bird Injects the Worm](#)

[Celebrating International Women's Day: Carving a Cybersecurity Career Path](#)

### APAC Webinars

[Cloud Web Firewall and ISMS-P](#)

[Digital Supply Chain: The Exposed Flank](#)

[Security Debt, Running with Scissors](#)

[Securing the Cloud Native Software Supply Chain](#)

[Robbery by Ransomware: Stick'em Up and Hand Over the Bitcoin!](#)

[Lighting a Path to Zero Trust: 6 Steps to Implementing a Zero Trust Model](#)

[Decoding End Point Attack and Protection –](#)

[Threats, Challenges and Best Practices](#)

[Exploring Passwordless Authentication](#)

[Defining an XDR Strategy: What Does it Mean for Your Organization](#)

[The Three Stages of Ransomware: Barracuda Threat Spotlight](#)

Introducing (ISC)<sup>2</sup><sup>®</sup>

# SECURE SUMMITS

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

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

## Each SECURE Summit features:

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

## IN-PERSON SUMMITS:

- [SECURE Washington, D.C.](#)  
Wednesday, March 30  
Renaissance Washington,  
DC Downtown Hotel
- [SECURE London](#)  
Thursday, April 7  
BMA House
- [SECURE Singapore](#)  
Thursday, July 14  
Shangri-La Singapore

## LIVE VIRTUAL SUMMITS:

- [SECURE North America](#)  
Wednesday, June 15
- [SECURE Asia-Pacific](#)  
Thursday, November 10
- [SECURE UK & Europe](#)  
Thursday, December 8

LEARN MORE  
AND REGISTER AT  
[isc2.org/events](https://isc2.org/events)



INTERESTED IN SPONSORING? [EMAIL US](#) FOR MORE INFORMATION.

## Giving DIY Cybersecurity a Second Glance

BY JASON McDOWELL, CISSP

### THE DO-IT-YOURSELF (DIY) CONCEPT

can sometimes get a bad rap, especially when applied to areas requiring knowledge and expertise. However, when resources are tight, a DIY approach may be the only viable option.

The challenge posed by limited resources does not negate the fact that cybersecurity is increasingly important for all businesses. Many companies remain impacted by the pandemic or market shifts and compensate for their reduced resources by adopting a DIY approach to cybersecurity. This isn't an inherently bad option; however, there is a right way and a wrong way to go about it.

Here are a few DIY missteps I have seen in my career and how to correct them.

### Secure remote access

One school of thought purports that legacy solutions are innately more secure than current solutions despite their reduced service set and limited functionality. For example, an office may adopt an isolationist mindset in which all data remains housed within company walls, which can prove challenging for employees who travel frequently or telework from hotels and customer sites. Lacking a current VPN solution and no feasible means to securely reach back to the home office, traveling employees naturally resort to local solutions such as caching sensitive data on their mobile systems, relying on open internet connections without appropriate safeguards, and using email as a means of uploading and downloading files.

In contrast, embracing current technologies with appropriate and robust safeguards is a much better path forward, even if there is a higher initial expense. In our example, establishing an effective in-house VPN solution that incorporates strong boundary

controls is attainable even on a limited budget. Additionally, ensuring mobile systems are using a secure remote access client that prevents full network connectivity without an established secure tunnel is an excellent method of protecting both home base and the endpoint as much as possible.

My point: Relying on legacy technologies and archaic policies may force users to DIY their own (insecure) solutions, which generates unnecessary risk to the company.

### Not minding the gap

Implementing security controls, whether that be technical, physical or administrative, must be done in a manner that ensures all controls are complementary and preferably synergistic with one another. This applies whether it's an ambitious, enterprise-level operation or small DIY one.

Unfortunately, it is commonplace to see the opposite occur. Two scenarios I've encountered relate to money-saving efforts and asynchronous system lifecycle schedules. In one, an assessment of a company's data center found a collection of high-end core network equipment operating in a leased space where the door and lock were so old that the door literally came off the hinges with a single pull.

In the other scenario, asynchronous system lifecycle schedules can occur when one or more components in a chain of systems is upgraded while the remaining components are legacy or are at the end of their lifecycle. Temporary residual legacy equipment is commonplace in a phased upgrade plan; however, problems arise when residual legacy equipment remains in place permanently, thus making any age-related vulnerabilities a persistent issue.

The way to address this challenge is to expect end-of-life considerations. Planning

Relying on legacy technologies and archaic policies may force users to DIY their own (insecure) solutions, which generates unnecessary risk to the company.

ahead introduces no additional cost beyond taking additional time to ensure purchased solutions have a reasonable remaining lifespan, and that that lifespan will see the business through to the next round of procurement.

### Forgetting to change the oil

Everything requires maintenance. That includes DIY cybersecurity.

Maintenance activities apply to all controls, whether repairing a broken door lock, upgrading firmware or updating policies. That said, it is common, especially in a DIY-minded small business environment, to implement a control and forget about it until it becomes a problem.

Unfortunately, adopting this mentality

guarantees security issues in the long run, and will likely increase costs compared to implementing a proper maintenance plan. To avoid this scenario, never procure a cybersecurity solution without considering its maintenance requirements at the time of purchase. Doing this helps ensure not only proper and effective operation of the solution, but also works to maintain the value of the solution over its lifecycle.

Building an effective DIY cybersecurity program is absolutely achievable. With proper consideration given to avoiding common pitfalls, a small business or even large enterprises can leverage a DIY cybersecurity program to reduce overall costs without sacrificing efficacy. •



**Jason McDowell**  
CISSP, is a California-based cybersecurity professional and perpetual optimist.

# Creating Cyber Confidence.

SIMSPACE CYBER RANGE  
ATTACK SIMULATIONS  
ACTIONABLE INSIGHTS

[Simspace.com](https://www.simspace.com) [info@simspace.com](mailto:info@simspace.com) [simspace.com](https://www.simspace.com)

2022 ©Simspace Corporation. All rights reserved.

**SIMSPACE**





# Are You Ready for CMMC?

If you are a prime contractor or subcontractor that plans to do business with the DoD in the future, CMMC applies to you. For organizations new to this cybersecurity framework, *Are You Ready for CMMC? Getting on the Right Track with the New DOD Cybersecurity Framework*, coauthored by AuditBoard and RSM US LLP provides an introduction to CMMC, including:



- Whether CMMC applies to your organization, implementation requirements and costs, as well as compliance deadlines.
- The three different CMMC maturity levels, and which level your organization should be targeting.
- How CMMC maps to NIST 800-171 and NIST 800-172, if your organization has already achieved alignment with the NIST standard.
- A CMMC Preparation Checklist to help you get started.

[Click this link to get your free guide to CMMC.](#)

# Dispelling Stereotypes to Bring in New Talent

BY DEBORAH JOHNSON

It's time to shake up the perception of cybersecurity professionals, says Tony Vizza, CISSP, (ISC)<sup>2</sup>'s director of advocacy. "Imagery that's conjured up is invariably a hoodie-wearing guy hunched over a laptop, a nerdy looking guy with no fashion sense, some weird-looking guy wearing a balaclava doing God-knows-what to a computer," he proclaimed in a panel discussion at the 2021 (ISC)<sup>2</sup> Security Congress.

Those already in cyber know these stereotypes are false, but what about those outside the industry—the potential candidates we need to create more diverse, inclusive teams?

In its 2021 report, *Diversity in Tech*, MThree, a training and talent development company, revealed that a majority of business leaders are aware of a lack of diversity in their tech teams. More than half say they struggle to recruit diverse entry-level tech talent.

So, what do talent acquisition experts recommend?

**Look elsewhere.** "Of course you're going to find good talent at an MIT Technology recruitment event," Aurora Bushner, executive VP at Incentive Technology Group, stated in an article on [glassdoor.com](https://www.glassdoor.com). "But having a presence at job fairs with lesser-known colleges and universities can bring in a pool of outstanding tech talent that isn't already being tapped by your competitors. It's also often home to minority students looking for career opportunities."

**Widen your focus** beyond specific candidate experience, advises the job site [Monster.com](https://www.monster.com). "Instead, focus on skills and capabilities over prestige credentials and be open to a variety of career paths. Candidates

from less advantaged backgrounds may have traversed a non-traditional path toward the expertise you are seeking, but the experiences they've gained along the way may have given them the unique vision your current team is missing."

**Fine-tune your job postings** as online searches have become the most popular method workers use in their job hunts. Watch for pitfalls, warns Eva Sage-Gavin, senior managing director at global talent firm Accenture.

"A significant majority (88%) of employers believe that qualified, high-skills candidates are screened out because they don't match the exact criteria defined by common job descriptions," she wrote, citing a study by her firm and Harvard Business School. As an example, she argues that having a four-year college degree may not be necessary if people have the right skills.

**Beware of biases with automated resume screenings**, according to Katrina Kibben, CEO of Three Ears Media, in a presentation for the [Society for Human Resource Management](https://www.societyforhr.com).

"Creating an inclusive job posting is not just about pushing your content through gender bias AI," she said. "In fact, many of the standard techniques in a job posting, like years of experience, can infuse additional bias, more than is already introduced simply because we have humans with their own biases making hiring decisions in the first place."

Developing techniques to build a more diverse team will require widening nets and broadening qualifications beyond what hiring managers traditionally use. ●



**Deborah Johnson** lives and works in San Diego. She can be reached at [djohnson@twirlingtigermedia.com](mailto:djohnson@twirlingtigermedia.com).

Photograph by Louise Roup



**Stop Ransomware.  
Isolate Cyberattacks.  
Reduce Risk.**

Segment in minutes on your path to Zero Trust.

Real-time visibility and Zero Trust segmentation from Illumio allow you to see and secure your most important data and applications across clouds, containers, data centers and endpoints.

**90%**  
Simpler

Eliminate manual network segmentation

**5x**  
Faster

Segment at the speed of business

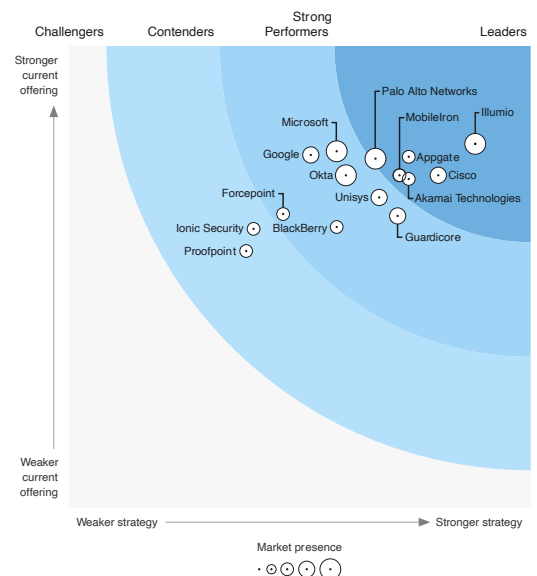
**100%**  
Confidence

Reduce risk and increase uptime


**FORRESTER**<sup>®</sup>

## Illumio named a Leader in The Forrester Wave™ for Zero Trust

Highest scores in three primary categories: current offering, strategy and market presence.



Learn more at [illumio.com](https://illumio.com)



Christian Taillon, Pam Rowland  
and Mike Manrod

# A RANGE OF EXPERIMENTS ... ON A BUDGET

## HOW TO BUILD A CYBER TRAINING ENVIRONMENT YOURSELF WITHOUT BREAKING THE BANK

BY MIKE MANROD, CISSP; PAM ROWLAND, PH.D.; AND CHRISTIAN TAILLON, CISSP

**AT A TIME WHEN DEMAND** for cybersecurity talent is surging against a backdrop of Ransomware-as-a-Service and widespread compromise, finding and cultivating expert security practitioners has never been more difficult. The latest [\(ISC\)<sup>2</sup> Cybersecurity Workforce Study](#) shows an estimated global shortage of 2.7 million cybersecurity workers, with some positions taking six months or more to fill. As compelling as the usual over-referenced labor metrics may seem, they fail to adequately capture the skills gap faced by the majority who are already working in full-time cybersecurity jobs.

PHOTOGRAPH BY MARK LIPCZYNSKI

If the infrastructure provides you with the vehicle you need to go somewhere, the content represents the maps and directions for how to get to the desired destination.

Although many academic institutions have stepped up to help bridge the gap—and masses rush forth to seek new careers in cyber—there is a growing chasm in practical skill development, even among those with adequate foundational knowledge. For experienced professionals and aspiring applicants alike, developing and maintaining practical skills at a pace on par with our adversaries has proven elusive.

A potential bridge across this abyss is in the practical lab environment, typically provided by a cyber range, home lab or guided tutorial. Conditions are present to produce quality practitioners when talented and motivated individuals are provided with foundational knowledge forged in the fires of practical range, lab and capture-the-flag experiences.

## FIRST COMES A CLEAR VISION

When seeking an optimal learning experience for practical skill development, the first step is to decide the goal. Are you the leader of an organization attempting to cultivate the skills of a team? A university professor working to elevate the capability level of students or an individual seeking to learn? Is the focus on basic skills, specific advanced skill sets or an organized progression from fundamentals through mastery? Are you focused on red team attack skills, blue team defensive capabilities or a balanced development of both (purple team)? Once you have a clear vision for what you want to accomplish, formulating a strategy to get there becomes much easier.

It is also important to identify what resources are available to you, based on your specific scenario. There may be opportunities for grants, donation of resources or procurement of low-cost hardware via online auction or discount merchant sites, particularly if your scenario does not entail production or high-availability uptime.

Those charged with building an enterprise or government range that is designed to replicate a complex enterprise or operational technology (OT) system should plan and invest accordingly. On the other hand, if you are creating a basic range for a small organization or a home lab, budget will be an overriding concern, and in such cases, much can be done at a low cost.

## BUILD OR BUY?

Once the scope is defined, it's time to decide whether to build or buy.

For individual learners, there is a wide range of tools and tutorials available for low or no cost that will help get you started. There also are quality, commercial cyber range offerings, starting at a basic and economical level up to full-production environments that reset after each scenario.

In addition to a broad range of options, you may also choose between cloud or hosted, full Software-as-a-Service (SaaS) or on-premises variants. Factors that influence decision-making include budget, scale and rollout timelines.

## RELATIONSHIP BETWEEN INFRASTRUCTURE AND CONTENT

It is important to recognize that there are fundamentally two topics when creating a range or lab environment: infrastructure and content.

Although the tendency is to think first about infrastructure, facilities and logistics, it is impossible to make informed decisions about a preferred type of environment until the content has been addressed. If the infrastructure provides you with the vehicle you need to go somewhere, the content represents the maps and directions for how to get to the desired destination. This usually takes the form of exercises, labs and challenges to help someone discover key insights and develop skills along a developmental journey.

In some cases, a core team of experts can create or curate content to help facilitate a learning journey that will result in the desired outcomes. Even so, most of the time, it is necessary to leverage free resources and/or commercial solutions to chart the course of a learning journey as a supplement if it is not the principal method for learning.

# HYPERVISORS AND VIRTUALIZATION STRATEGIES

**IF YOU WANT TO RUN A CYBER RANGE** or home lab, virtualization will be one of the first and most important technical topics to consider. A wide range of YouTube videos are available for basic virtualization, making such tasks common knowledge. Accordingly, a more difficult decision may be what virtualization platform to select for a scenario. There are two levels of hypervisor: bare metal (type 1) or operating system (OS; type 2). Your choice will depend on whether you want the virtualization platform to run natively on your hardware or if you want it to just be another set of installed software.

**In selecting a hypervisor for a range, consider factors such as licensing, cost, performance, scalability, features, and how well the solution fits with your overall vision and strategy.**

Some of the most popular bare-metal hypervisors useful for range and lab scenarios are ESXi, Kernel-based VM (KVM) running QEMU, XCP-ng, Unraid Hyper-V and Proxmox. If scale is not important, and requirements are conservative, sometimes type 2/OS hypervisors will work fine (VirtualBox, VMware Workstation, Parallels, etc.) for the work of an individual learner or analyst. In selecting a hypervisor for a range, consider factors such as licensing, cost, performance, scalability, features, and how well the solution fits with your overall vision and strategy. It is also important to consider containerized platforms such as Docker or Kubernetes. Although the selection of

a virtualization or containerization platform is highly individual based on specific requirements, it can be valuable to consider your specific range requirements and let factors such as scale, agility, cost and ease of support inform key decisions.

## NETWORK TOPOLOGY AND MONITORING CONSIDERATIONS

The first priority for network segmentation of a range or lab environment relates to containing attack scenarios to target systems and not administrative systems or out-of-scope network segments. Simply put, if the objectives are well understood, and the network environments and account permissions are scoped accordingly, the risk of material issue is reduced significantly.

Although the first level of range network requirements comes down to self-defense, and the second level may relate to simulating a realistic enterprise environment, the third is most certainly related to monitoring and response. There is a wide range of open-source technologies you can use to improve detection and response capabilities. The first is a solid security information and event management (SIEM) solution, feeding into effective security operations center (SOC) monitoring and responding to the most noteworthy of events (for this, consider ELK, Splunk or Humio, among others). Monitoring and intrusion detection system (IDS) solutions, such as Zeek and Suricata, may also be helpful to validate the effectiveness of controls, as range participants dutifully test key scenarios. At the end of the day, even if the primary focus is cultivating talent, if along that journey we can learn something more about what software, systems or processes are weak, then we are better for it.

—M. Manrod, P. Rowland, C. Taillon

In this sense, content is more than just the lab guides and steps to follow. It includes the vulnerable systems, exploit methods and tools needed to attack or defend in a specific scenario. When deciding to build, buy or leverage, understanding the full scope of activities a learner will need to complete will be critical. If creating new content seems out of reach, leveraging open-source or commercial resources to bootstrap your efforts is a good idea.

When it is necessary or advantageous to use a commercial offering for content, sometimes such offerings will also provide the infrastructure (as a service) at a discounted rate, making an all-in-one solution optimal. If your approach is more conservative and your available technical resources are minimal, a comprehensive package may be ideal. On the other hand, if you need the solution to scale widely, and have team members who are highly knowledgeable on key topics, it may make more sense to create most of your own content, manage the infrastructure and reduce dependencies as much as possible.

In each case, it will be necessary to leverage multiple open-source projects to be effective, and the license agreements of the projects used will need consideration.

## IF YOU BUILD IT ...

For individual learners or smaller organizations, consider cloud options—especially if they bundle content and infrastructure into a comprehensive package. Even if complete control of the infrastructure must be retained, it is valuable to consider what can be offered by open-source projects. A cloud platform is particularly advantageous if the duration of use will be relatively short. For example, if you need massive compute resources for one capture-the-flag exercise, you should use cloud resources. Whereas, if you want to practice a bit every day, it may make more sense to set up a home lab or range. Solutions such as Amazon Web Services (AWS), DigitalOcean or Amazon Lightsail provide low-cost access to a lot of economical compute power if utilization is less than continuous.

When building a robust cyber range or home lab, server resources and enterprise-level infrastructure products are a likely consideration. It is also important to note: For full-production range environments with many concurrent users and uptime service level agreements, treat it as you would any other production application and use modern and supported products. For everything else, there are sites like eBay, donations and repurposing hardware that has been decommissioned from the production environment. Fortunately, many hypervisor products run on older hardware without issue, assuming the server model is compatible. And what you really need are virtual cores, memory and a reasonable amount of disk space.

As data centers refresh and decommission, older model servers that are quite powerful and viable become ideal candidates for repurposing as range or home lab systems. For example, there is a tremendous array of online resources dedicated to configuring Dell R710 or R720 servers for home lab or entertainment systems. One data center's trash is another home lab learner's treasure. If you want a realistic production environment at a low cost, build the elements on a foundation of low-cost legacy servers and switches.

## SOURCES AND RESOURCES

National Initiative for Cybersecurity Education (NICE),  
National Institute of Standards and Technology (NIST),  
Cybersecurity Workforce Demand

[https://www.nist.gov/system/files/documents/2021/12/03/NICE%20FactSheet\\_Workforce%20Demand\\_Final\\_20211202.pdf](https://www.nist.gov/system/files/documents/2021/12/03/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf)

Art of Server YouTube Channel

<https://www.youtube.com/c/ArtofServer>

Lawrence Systems YouTube Channel

<https://www.youtube.com/user/TheTecknowledge>

Spaceinvader One YouTube Channel

<https://www.youtube.com/c/SpaceinvaderOne>

### Commercial Range and Training Solutions

Advanced Business Learning (ABL) Cyber Academy

<https://ablcyberacademy.com/>

Cyberbit

<https://www.cyberbit.com/>

Hack the Box

<https://www.hackthebox.com/>

Linux Academy/A Cloud Guru

<https://acloudguru.com/>

Merit

<https://www.merit.edu/security/training/>

Pentester Academy

<https://www.pentesteracademy.com/>

—M. Manrod, P. Rowland, C. Taillon

## IDEAS FOR RANGE ARCHITECTURE

When creating a range environment to help cultivate attack or defense skills, try to closely resemble a real-world environment as much as possible. This can be easily accomplished by setting up a network context for attackers—a firewall and a context for servers and workstations intended for use as attack targets.

At more advanced levels, the firewall can be set up with both permissive and locked-down policies to allow testing of exploits under both conditions. Likewise, targeted virtual machines can be set up with antivirus and intrusion detection tools to prevent modes to run different scenarios to validate prevention versus to confirm detection and response capabilities. This approach can be extended to span all security controls with a degree of creativity.

## A PHYSICAL RANGE ENVIRONMENT

Today, many things that were scheduled in person continue to be held virtually. That said, there are many situations where a physical range environment may be highly desirable, such as for a university or corporate campus. Although the ideal range environment will vary widely based on an organization's requirements, a basic template could be considered as follows:

- A large room with adequate space to set up tables for six to eight people per table
- Prominent podium and mirrored projector screens in each direction for maximum visibility
- Laptops with the appropriate attack tools (e.g., Kali Linux) set up and wired into the correct range networks

Note that the laptops do not need to be powerful—just reliable and compatible with what you want to run on them. Consider using repurposed (working) user laptops that are being phased out or seeking donated laptops. Set up and testing prior to implementation are crucial for smooth operation and optimal learning.

## CYBER TRAINING IS IN YOUR HANDS

As we face the challenge of cultivating the next generation of cyber practitioners and elevate the skill level for those already on the job, we need to closely simulate a real-world experience. Creating quality learning experiences for building practical skills and exposing learners to realistic environments for practice and training must be considered key elements to bridge the skills gap.

A cyber training center will provide the needed hands-on skills, and organizations or individuals can create an environment that does not “break the bank.” ●

**Mike Manrod**, CISSP, is CISO at Grand Canyon Education; **Pam Rowland**, Ph.D., is associate dean of computer sciences and technology at Grand Canyon University; and **Christian Taillon**, CISSP, is threat response engineer at Grand Canyon Education. Additionally, the authors give special thanks to their colleague, **Aaron Clark**, who provided expert contributions and helped inspire and shape their own home lab/range.

**IDENTITY DEFINED  
SECURITY ALLIANCE**

[www.IDSAAlliance.org](http://www.IDSAAlliance.org)

# #BEIDENTITYSMART AND GET CPE CREDIT

Boost your identity security knowledge and strategies for reducing the risk of an identity-related attack, while earning CPE credits.

[Explore our program today](#)

**(ISC)<sup>2</sup> | CPE SUBMITTER**



The logo for Securonix, featuring the word "securonix" in a white, lowercase, sans-serif font. The letter "x" is stylized with two small orange dots above it. The logo is positioned on a dark purple background that is part of a larger graphic design featuring a white arc and a cloud-like texture on the left side.

securonix

# Security Analytics at Cloud Scale

Securonix is redefining SIEM. Built on big data architecture, the complete Cybersecurity Analytics & Operations platform is a pure SaaS solution that provides analytics-based threat detection with unlimited scalability.

For more information: [www.securonix.com](http://www.securonix.com)

Follow us @securonix



© 2022 Securonix. All rights reserved



# ARE YOU IN THE DARK ABOUT WHERE YOUR ASSETS ARE?

BY CHARLES CHIBUEZE, CISSP

**A FEW YEARS AGO**, as a bank's newest information security analyst, I initiated a vulnerability scan on a select group of assets. I aimed to measure remediation action and advise on how to fix outstanding issues commensurate with the bank's risk appetite.

Once the scan was done, I exported the report and took a quick look to validate the results. I have this one rule for carrying out assessments: Never trust the first results; always assume something is missing or not done properly.

I was right! A couple of assets (servers) didn't initially show up in the document. It turns out the initial asset list was outdated, so I updated it by extracting a fresh record from the inventory tool (with negligibly near real-time accuracy) and ran a new scan. I ran my analysis, prepared a fresh report and sent it out to the relevant stakeholders.

This incident served as an important reminder of the importance of a solid asset management program. You can't protect what you don't know you have.

ILLUSTRATION BY JAN FEINDT

## WHAT IS A CYBERSECURITY ASSET MANAGEMENT PROGRAM?

A cybersecurity asset management program ensures efficient oversight of an enterprise's digital assets (e.g., infrastructure, applications, web services, cloud services), from creation to disposal, to ensure nothing is compromised by threat actors.

Poorly managed assets can be a weak link in an organization's security chain, in turn causing large amounts of money to be unnecessarily invested and wasted on boosting an organization's security posture.

An asset management program simply ensures the following:

- Creation of assets in the proper way following due process
- Identification of rogue assets that may compromise an organization or be compromised by threat actors
- Complete coverage of organizational assets to ensure they are secured properly
- Decommissioning of assets that have no business justification for existing any longer

Organizations cannot afford to not have a crucial program like this. Imagine spending a lot of money recruiting a world-class cybersecurity team, investing in next-gen security tools and implementing security programs. Later, you discover the company was breached by a threat actor who gained access to customer details stored in an unprotected public S3 bucket that was unaccounted for. This is one reason why a cybersecurity asset management program is fundamental.

Furthermore, without a proper asset management program in place, cybersecurity team members may carry out assessments on assets that no longer exist (stale assets), perform incomplete assessments (leaving out newly created assets that weren't registered) and disrupt business processes by working on assets without prior arrangement or permission.

Imagine spending a lot of money recruiting a world-class cybersecurity team, investing in next-gen security tools and implementing security programs. Later, you discover the company was breached by a threat actor who gained access to customer details stored in an unprotected public S3 bucket that was unaccounted for.

## DANGERS OF IMPROPER IMPLEMENTATION

Let's say an organization needs to get Payment Card Industry Data Security Standard (PCI DSS) certified. Surely, the only assets in scope would be those in the cardholder environment. The assessor requests vulnerability scans of the servers in the cardholder data zone, and an analyst quickly executes that.

However, the analyst uses a list of servers from five years ago. The assessor, while scrutinizing the scan results, notices that the assets in the inventory provided to him/her do not match the assets in the scan results. A number of servers are missing and therefore haven't been assessed.

On investigation, the security team notices that the list of assets used for the scan is outdated. Some assets no longer exist in the network, while others do exist, but were either created without due permission or without notifying the team responsible for documenting assets.

## WHAT ARE THE MISTAKES HERE?

First, the analyst was not working with an updated inventory. Second, the team in charge of managing the payment of critical assets, which were most likely decommissioned, set up new servers without due process. If this were done properly, the security team would be in the know and could update accordingly. A properly implemented asset management program helps to close this gap.

Now, let's talk about what's needed to create your own working, effective asset management program.

**Organizations need to perform a business impact analysis on their assets, where they measure the impact of a cyberattack on each asset or group of similar assets. The higher the impact, the more important that asset is and, therefore, the higher management priority.**

## IDENTIFY CURRENT ASSETS

This may or may not qualify as the first step in creating an asset management program, but it is extremely important to know what your current assets are. Again, assets here refer to information assets such as servers, applications (web, mobile, APIs), containers, storage devices, network devices, etc.

Know what assets you have and what assets you shouldn't have. Have a system in place to detect when rogue assets have been connected to the network. Have a system in place to identify assets that have outlived their usefulness.

Outdated assets pose the risk of being compromised due to lack of proper care and maintenance. Think of a test server that is no longer needed for its original purpose and now lies unused and unsupported. Due to a lack of routine patching, a malicious user with access to the network can easily compromise it and pivot to other areas of the network to accomplish their mission.

## IDENTIFY OWNERS AND DETERMINE RESPONSIBILITIES

When I started out building my first vulnerability management program, I discovered that different parties needed to fix different issues identified. The IT (infrastructure) group, of course, didn't have the expertise to fix application-related vulnerabilities. They also couldn't fix system-related vulnerabilities without due permission from the asset owners.

Every asset, whatever form it takes, has an owner. And every asset owner has a responsibility to ensure that security issues identified in any asset in their jurisdiction are reported and fixed in a timely manner.

Different business units have various IT assets that drive their processes, whether it is business or in-house processes. The point to note here is that assets must be grouped, and owners identified and assigned. This way, when security assets have been carried out, different reports will be sent to different business groups with respect to the assets they own.

## RANK YOUR ASSETS BY CRITICALITY

In 2017, a ransomware attack spread globally like wildfire and wreaked havoc on information systems. This malware exploited a particular vulnerability inherent in the Windows operating system with the common vulnerability and exposure known as CVE-2017-0144.

This particular vulnerability was easily exploited and lingered for a long time. (As a penetration tester, I had a high rate of success in my engagements where this vulnerability was present.) This is where it gets dicey. For example, if you discovered this vulnerability on a number of revenue-producing servers and other assets, like the staff leave portal, which would you fix first? Of course, the revenue-producing servers have to be fixed first because revenue is a higher priority. Without it, there is no business.

Organizations need to perform a business impact analysis on their assets, where they measure the impact of a cyberattack on each asset or group of similar assets. The higher the impact, the more important that asset is and, therefore, the higher management priority.

## HAVE A PROCESS AROUND UPDATING ASSET LISTS

Assets are dynamic; they get created and disposed of almost every day. The DevOps team is constantly spinning out new instances to either test or launch a new application. This should be a focal point for security analysts in charge of asset management because any test asset left without any form of maintenance support becomes a weak link.

**If any change is to be made on that asset, or any new feature is implemented, it should require leadership's approval. Also, ensure that newly created/changed assets pass through vulnerability assessment and remediation cycles to guarantee they don't introduce additional risk to the enterprise IT environment.**

This brings me back to my story at the beginning: What if I didn't update the asset list before scanning for a second time? A lot would have been missed. I would have presented a false vulnerability status report, and my work would be doubted had there been a breach due to an unpatched system.

An asset management tool can scan the network and have an accurate list of the current inventory at a snapshot period. If you're dealing with cloud assets, asset lists are usually updated automatically. That said, you may need to grant an analyst read-only access to generate the current list of assets for assessment purposes. Also, constant reminders need to be communicated to ensure that analysts do not use stale lists for their assessments.

## **INCORPORATE CHANGE MANAGEMENT**

If there is any reason why ownership of digital assets is unaccounted for, it is usually because they were created without due permission.

If any digital asset is to be created, it must have an approval from leadership attached to it. Leaders must know an asset's purpose and how long it stays in use before decommissioning.

If any change is to be made on that asset, or any new feature is implemented, it should require leadership's approval. Also, ensure that newly created/changed assets pass through vulnerability assessment and remediation cycles to guarantee they don't introduce additional risk to the enterprise IT environment.

By going through a formal process, there is less chance of introducing unintentionally rogue assets to an environment.

## **ENSURE EFFECTIVE DISPOSAL**

Assets that have served their purpose need to be decommissioned so:

- They don't create a weakness in the organization's security posture
- They don't add to management overhead (e.g., patching and maintaining an asset that isn't useful)
- They facilitate efficient use of IT resources

Assets that are no longer needed or have reached the end of their useful life should be decommissioned, and assets that are out of support should either be upgraded or decommissioned.

By decommissioning unneeded assets, you ensure that only useful assets are allowed to function and thus bring down the cost, effort and risk involved in asset management. And by following all of the above recommendations, there's a smaller chance that your organization will fall victim to an asset—active or otherwise—serving as the vector to launch an attack. •

**Charles Chibueze**, CISSP, CISM, CEH, is a Nigerian-based senior security consultant providing cybersecurity services to global organizations.



THE  
POWER  
DUO

CISSP®

CCSP®

of Cybersecurity Certifications

---

**CISSP:**

The Most Required Security Credential by Hiring Managers  
on LinkedIn

**CCSP:**

The Top Security Certification Experts Plan to Earn in 2022,  
Certification Magazine

**To learn more download our Ultimate Guide.**

[Get Your CISSP Guide](#)

[Get Your CCSP Guide](#)

(ISC)<sup>2</sup>



# WORKING OUT

Taking the time to build a structured program will make it easier to flex some serious security muscle when needed.

**BY ROBERT WEBSTER, CISSP**

**UNLESS YOU'RE AN ATHLETE OR GYM REGULAR**, the idea of starting a serious exercise routine can be daunting. You replace easy or relaxing activities with those requiring some level of initial physical discomfort and even financial outlay until you start to see results.

It is similarly daunting to exercise one's business in cybersecurity. In the short term, these exercises divert your attention and resources away from money-making operations. You may even uncover findings that will require painful changes. Nonetheless, like going to the gym and being proactive with your physical health, cybersecurity exercises are important to the overall health of your organization.

ILLUSTRATION BY DANIEL HERTZBERG

It is often more effective to develop a short, concise, scenario based simply on a confidentiality, integrity or accessibility compromise to one or more systems.

## ESTABLISHING A SAFE PLACE TO WORK OUT

Exercising information systems requires a few more considerations than the traditional all-hazard-type exercises. All-hazard exercises focus primarily on physical response and recovery after an incident has occurred, often using long-established response plans. Cybersecurity exercises, however, must address incidents that often have unknown scope and scale and that do not completely fit off-the-shelf plans.

When more detailed attributes about a cyber incident become evident through identification and analysis, periodic modification-to-response efforts may be necessary. Also, although a firefighter can exercise with a real fire or simulate destroyed facilities, it is difficult, even impossible, to exercise a cyber incident on real-world network systems. This is because the risk of actively degrading a network for an exercise is simply too high.

When planning your exercise, consider the type of cyber incident you need to meet your objectives. Cyber-related incidents manifest in one or more of the following types:

- **Cyber-induced cyber consequences:** Any significant event occurring on or conducted through a computer or computer network either intentionally or accidentally that compromises the integrity, confidentiality or availability of computers, networks, information communications systems, data or virtual infrastructures. Furthermore, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls or implementation that could be exploited by a threat actor.
- **Cyber-induced physical consequences:** An incident event specific to a subset of target data systems such as industrial control systems, internet of things (IoT) devices or other systems that interact with physical machinery and equipment—essentially, anything that destroys, removes, replaces or alters the operations of devices or connections. Typically, this is a data integrity issue.
- **Physical-induced cyber consequences:** Intentionally or accidentally destroying, interrupting or degrading a critical network's physical infrastructure in a way that prevents data accessibility and/or delivery of essential data.

Your scenarios need not be too detailed to be effective. Long, in-depth technical scenarios are often sidetracked, as participants spend more time dissecting the technical aspects than addressing potential gaps in their plans, policies and procedures. It is often more effective to develop a short, concise, scenario based simply on a confidentiality, integrity or accessibility compromise to one or more systems.

When developing your scenario, you will need to include the following:

- A victim or set of victims (owner/operator/user)
- Someone who detected the malicious activity and a means of notification
- Indicators of unusual activity (compromised confidentiality, integrity or accessibility)
- A targeted data system or systems
- The type, level and scope of the incident

By manipulating these details, you can set up scenarios that force decisions about priorities. Having your main system compromised would trigger a certain response. However, how many lower-tiered systems would have to be compromised to trigger a similar response? How would you triage competing priorities?

Your exercise can explore the gaps in your plans by using different systems and then adjusting the types of impacts, level of impacts, decision thresholds, etc. For instance, consider the level of impact when an action requires amplification to get the desired effect to meet the objective. Adjusting the level of impact to two or more systems can help identify those areas of resource constraints by adjusting the scale and scope of the scenario.



# TRAINING

## TIPS AND TOOLS

Anyone planning a cybersecurity exercise should consider including the perspective of outside stakeholders such as customers, vendors, peer information sharing, law enforcement, insurance and so on.

### **Customers**

Customers, once alerted to compromises of their data, will respond accordingly. Your organization can expect an increase in inbound calls, email messages and social media comments demanding or inquiring about a cyber incident. How your organization anticipates or responds to such activity will determine how successfully you recover from an incident. Additionally, consider the role of and increased pressure on public relations, legal concerns and effects on profits and turnover.

### **Peer Organizations – Information Sharing**

Protecting and recovering from a cyber incident are heavily dependent on good information sharing. To be proactive, one should establish relations with information-sharing organizations and peer organizations, incorporate those relationships into security plans and exercise the interaction procedures. Your exercise may use such organizations to provide indications and warnings of some kind of threat, or you may need to exercise how, what and when you share information with these organizations. Among the organizations to consider are Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs).

### **Law Enforcement – Evidence Collection**

Forensic evidence is essential for high-tech investigations. Information technology (IT) professionals at organizations that are victims of cybercrime

might be tempted, for instance, to simply reimage a computer that has been infected with malicious software, wiping it clean and reinstalling the necessary programs so that it can be used safely. This comes at a high cost, however, because any evidence that might have been on the machine could be destroyed in the process.

IT professionals working with cybercrime investigators need to also understand the process of securing evidence for investigations. Instead of attempting to wipe clean an affected network to remove a threat, your organization may need to exercise how to properly preserve forensic digital evidence.

### **Cyber Insurance**

No cybersecurity program, process or system is, or will be, perfect. To mitigate this, many organizations choose some type of cyber insurance to help offset the cost incurred by an incident. It is important that organizations have a firm sense of what this kind of insurance can, and cannot, do. An organization may want to exercise its plans to determine the thresholds for when such notifications need to happen. Also, consider exploring how cyber policies may provide coverage for third-party data.

There are some specific administrative considerations that could be further explored for these aspects of cyber insurance. You may have an insurance policy that requires written consent before hiring any outside professionals, such as a lawyer, forensic consultant and public relations firm, in the event of a cyber incident. There may be requirements that if not met (failure to provide timely notice) may jeopardize coverage for an otherwise insured claim. Your organization may want to exercise these plans to determine the thresholds for when such notifications need to happen.

—R. Webster

Like any exercise, the key is consistency and determination, with the occasional pep talk to stay motivated.

## A CAUTION ABOUT COMMON PLANNING MISSTEPS

When planning a cybersecurity-themed exercise or one that includes cyber elements, it is important to avoid common missteps.

- Don't be in too much of a rush to build scenarios based on the newest threat. Threat actors adjust their tactics, techniques and procedures very rapidly. Your technical team will have to keep up with these threats as best they can. The team will benefit greatly from hands-on keyboard training environments. However, too much focus on the threat of the day can create a false sense of security. You may become good at responding to a threat action that has moved on to other methods but are then caught off guard by something new. Your exercises will benefit when they instead focus on generic threat actions and learnings that can be applied broadly.
- When planning, ensure the proper artifacts and stimuli are available to players. This requires attention to detail and coordination with various types of subject matter experts from across several functional and technical domains within your organization. Become familiar with as much of your organization as possible, bringing in subject matter experts as needed. Don't limit these experts to the technical aspects. Consider inviting experts from operations, application users, legal, public affairs, etc.
- Do not rely on a set of the same scenarios or replay the same stage. Cycle through the five stages of identify, protect, detect, respond and recover. There are valuable lessons that can be gained by dedicating an exercise to each one of these in addition to combining them in some fashion.
- A virtual cyber environment, or cyber range, may be available and useful but requires extra resources and often cannot adequately duplicate the complexity and scale of a real-world network. Instead, consider cyber training boot camps for your network engineers and technicians as a means for them to gain skills.
- When conducting an exercise with physical consequences, avoid designing a scenario event with physical consequences so devastating that the cyber incident itself is no longer the priority. This kind of event quickly becomes all about saving lives and property and not about recovering cyber systems.
- As you exercise recovery from cyber-threat events, there will not likely be a definitive end state. The best expectation is to identify a recovery process that would remain ongoing for an undetermined length of time. Cyber-threat events usually take a long time to be detected and can take much longer to fully recover. Even then, a true full recovery may not be obtainable. You need to determine in advance, maybe as an objective, what the desired end state will be. Is the end state to recover all systems, to enhance operator reaction time, to develop cyberattack countermeasures and/or preventive software, to enhance multiple organizational cooperation, etc.? The bottom line is that end states to cyber threats are difficult to truly exercise, and objectives may be satisfied by simply identifying the means for a long-range recovery process.

If you decide to pursue a cybersecurity exercise and need assistance with the basic process, you can refer to publicly available courses and templates like the ones from the Homeland Security Exercise and Evaluation Program (HSEEP) for specifics about the structural steps to plan and conduct an exercise. HSEEP includes a set of guidelines for exercise program management, design and development, conduct and evaluation.

Remember that beyond planning and preparation is the actual execution. Make sure you and your team allow the time to do the exercises and tweak your programs from there. Like any exercise, the key is consistency and determination, with the occasional pep talk to stay motivated. Stick with it, adjust where needed, and soon you'll be flexing more cybersecurity muscle too. •

**Robert Webster**, CISSP, works for a Midwestern financial service.

# Effective Third-Party Risk Management Starts with *Knowing* your Third and Fourth Parties

The third and fourth parties you know about



The vendors with access to your organization that you don't know about

Go below the tip of the iceberg with **Automatic Vendor Detection** from SecurityScorecard.

- ✓ Visualize 3rd and 4th party risk
- ✓ Instantly discover unknown vendors
- ✓ Drive targeted discussions with your supply chain

**Gain a complete view of digital supply chain risk.**

**Request a demo today** to learn how **Automatic Vendor Detection** can help you.

*The Power of Knowing.*



# DIY Approach to Career Advancement

BY SPENCER WILCOX, CISSP

I recently joined a Ph.D. program at the New Mexico Institute of Mining and Technology (New Mexico Tech) focused on transdisciplinary cybersecurity. I am also the chief security officer (CSO) and executive director of technology at a mid-sized utility in New Mexico.

So, what is a CSO supposed to do to recruit talent and bring in the “best of the best”? For me, it’s about taking a “DIY approach”—that is, me building my own hiring plan from scratch, rather than relying on insufficient solutions.

A professor at New Mexico Tech once approached me in my role as CSO and asked: “What would your ideal cybersecurity candidate be trained in?” The program that I described included some of my own experiences and identified technical and non-technical training that would create what I perceive to be an ideal practitioner. Thus, my perfect cybersecurity candidate would be educated in the following disciplines:

- Logic, to make good solid decisions and achieve accurate conclusions
- Political science and sociology, to help understand the motivations of an advanced persistent threat (APT) and the ideologies of the inappropriately named 4chan /b/tards
- Psychology, to understand the way a threat actor and an end user think
- Law, to understand the criminal and civil law and the regulations that dictate many of our activities
- Networks, to understand the communications environment in which these ideas and their subsequent attacks propagate
- Operating systems, to understand what threat actors are attacking
- Databases and data analysis, to turn volumes of traffic into usable information

- Engineering, to understand failure modes and effects analysis
- Accounting and finance, to articulate the business risk management issues
- Statistics to help articulate and quantify risks
- Programming, to gain familiarity with applications and integration
- Familiarity with certain tools and technologies, to identify, detect, defend against, respond to and mitigate any event that impacts the technology assets of a corporation
- A DIY mentality when it comes to building tools and capabilities to harden defense against a bad actor, regardless of the budget

This program would help to contextualize the challenges in cybersecurity and deliver life lessons that would help to solve them.

Two years later, I am both a student in the New Mexico Tech program and an instructor. Through a DIY-like partnership, we built a cybersecurity academic program to prepare tomorrow’s practitioners to add incredible value to any security program. New Mexico Tech is developing a set of courses in each of these disciplines with a focus on their applicability in information security.

The transdisciplinary cybersecurity program is designed to produce well-rounded professionals who’ve studied more than technical manuals and can apply their academic backgrounds to help organizations in many other ways. They are great communicators, strategists and, of course, cybersecurity experts. I encourage you to set up your own DIY approach to personnel development. All it takes is a plan, some materials and instruction, sweat equity and an eye toward a brighter future. ●



**Spencer Wilcox**, CISSP, is a CSO and Ph.D. candidate living and working in New Mexico.

# Unlock your risk management potential



Unifying compliance and risk

LEARN MORE AT  
**[RECIPROCITY.COM](https://www.reciprocity.com)**



In-person Event

# Attend Infosecurity Europe 2022

(ISC)<sup>2</sup> is once again a Media Partner for Infosecurity Europe, the meeting place for the industry's finest minds. The event will deliver expertise and knowledge from the world's most celebrated cybersecurity experts, connecting practitioners with suppliers to find true solutions, and bringing together industry peers to network, share ideas and ultimately grow stronger and more resilient together.

With threats increasing – 39% of UK businesses reported a breach in the last year – equipping yourself with the right knowledge and tools has never been more important.

When you attend Infosecurity Europe, you have the opportunity to:

- Meet with the (ISC)<sup>2</sup> team and select UK Official Training Partners at stand Q89
- Tune in to (ISC)<sup>2</sup> Advocacy Director Dr. Sanjana Mehta's thought provoking presentation
- Earn up to 24 CPE credits – the points will automatically appear in your member account

## Infosecurity Europe

21-23 June, 2022

ExCeL, London

[Register Your Interest](#)

Visit the (ISC)<sup>2</sup> Stand: **Q89**