A PREVIEW OF (ISC)² SECURITY CONGRESS IN OCTOBER

InfoSecurity PROFESSIONAL

SEPTEMBER/OCTOBER 2021

Social Network Attacks

Bridging Cyber Policy and Operations

Choosing a Threat Model

(ISC)²®
An (ISC)² Publication

3 WAYS TO TRAIN

CCSP

Certified Cloud Security Professional

An (ISC)² Certification

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

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

Choose your training path

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

Self-Paced
Online learning at your own pace

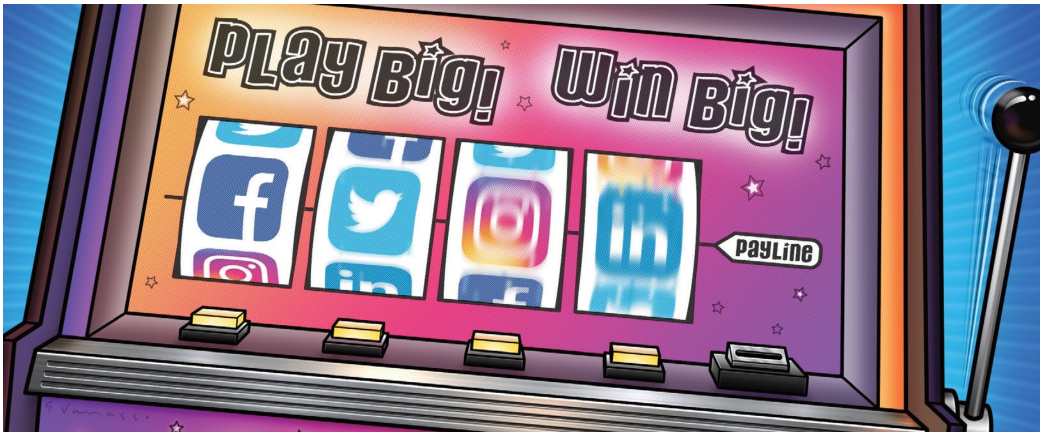
Online Instructor-Led
Virtual learning with a live instructor

Classroom-Based
Focused in-person learning

Need Help Deciding?

(ISC)² VISION: INSPIRING A SAFE AND SECURE CYBER WORLD

CONTENTS ▪ SEPTEMBER/OCTOBER 2021 ▪ VOLUME 14 - ISSUE 5



Are you giving away too much on social media?

PAGE 30

Cover image by John Kuczala

Illustration (above) by Enrico Varrasso

Photo illustration (right) by Robert Neubecker

EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

Back It Up! Back It Up! Back It Up!

IN EARLY MAY my grandson collided with a truck tailgate during a neighborhood block party and suffered a head injury. His parents rushed the vomiting, logy toddler to the nearest hospital. As soon as they walked into the Emergency Department, they noticed the warning signs hanging from computer monitors: "Do Not Use. Do Not Turn Off."

It turns out Scripps Health was under a ransomware attack. Providers had little choice but to treat those they could and transport everyone else, like my grandson, to other hospitals with working equipment and access to electronic medical records. The CEO later published a letter in the local newspaper explaining why the health system stayed mum for weeks and how hard IT crews and consultants worked behind the scenes. He also noted Scripps Health was far from the only ransomware victim this year.

Indeed, cyber gangs and nation-states continue cashing in on the increasingly lucrative ransomware trade. It's not your imagination: Lockouts are happening with alarming frequency. Ransoms are reaching record levels almost weekly. As CISSP Julien Legrand notes in his cover story, three of every four organizations are expected to face such an attack by 2025. Time to reconsider your backup strategy.

Another story in this issue is a reminder of risks we take when doing what public relations, marketers and career coaches recommend: elevating our online profiles and interacting with alumni, colleagues and prospective employers using social networks. As acknowledged in Cate Kozak's piece, even the most diligent among us can get taken in by crooks posing as peers.

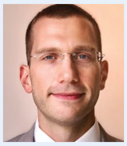
But we shouldn't stop sharing career advice and milestones because bad people are out there. That transfer of knowledge is vital to our ability to do our job and still have a life outside of it. Those starting out need the wisdom of seasoned (ISC)² members who've been granted full tenure at the School of Hard Knocks. Those deep into their cyber careers need reminders the field is changing.

One great venue to talk shop and trade war stories is next month's (ISC)² Security Congress. It's a great event to take in insightful keynotes and peer presentations. There also will be opportunities to virtually network. Just personalize that LinkedIn request you send after the show, so the recipient is more apt to trust it came from you and not some cybercriminal who knows you well. ●

Photograph by Louise Roup

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

CONTRIBUTORS



Julien Legrand has written about technology and cybersecurity for notable newspapers before, but this is his first piece for our magazine and it's a great topic: payments around ransomware. He is based in Hong Kong and has strong knowledge and experience working with data protection, risk management and cryptography.

Two other (ISC)² members contributed articles based on their own experiences. **Kumar Setty** is the principal at Zakti Security Labs, a boutique security and privacy consulting firm based in the Chicago area. He hosts a monthly podcast called Privy (https://podcasts.apple.com/us/podcast/privy/id1505644215) where he discusses security and privacy issues with experts.

Mounir Khatib is a cybersecurity engineer providing strategic and tactical consulting services to commercial and government enterprises for almost 20 years.

Our fourth feature on social network attacks comes courtesy of *InfoSecurity Professional* contributor **Catherine Kozak**, who last wrote about careers from an ecological standpoint in the award-winning November/December 2020 edition.

Props please! From a live hawk flying in his house one day to harpoons in his closet and much more, **John Kuczala** has contributed manipulated photography to *InfoSecurity Professional* over the years. His collaboration with our art director has garnered many design awards. For this issue's cover, John meticulously cut and shot our "ransom note" art. Check out last issue's art where the wires on a quantum computer were bent to create human profiles.

InfoSecurity PROFESSIONAL
An (ISC)^2 Publication

(ISC)^2® INSPIRING A SAFE AND SECURE CYBER WORLD

https://www.isc2.org https://community.isc2.org
https://www.linkedin.com/company/isc2/
https://twitter.com/ISC2 https://www.facebook.com/isc2fb

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/Sept-Oct-2021

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

ADVERTISER INDEX

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

InfoSecurity Professional is produced by Twirling Tiger® Media. 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

Lessons on Life and Work at This Year's Security Congress

BY MEGAN GAVIN, DIRECTOR OF EVENTS, (ISC)²

I think we can all agree that last year is better left in the past. One of the bigger letdowns from 2020, at least when it comes to business, was that we couldn't meet face to face to interact as a community. Sure, we all made do with the circumstances. Many of you attended our annual (ISC)² Security Congress last November, which for the first time in our history went fully virtual. It was a huge success, and we more than doubled our previous attendance record with more than 5,700 registrations.

As much as we hoped to provide a hybrid experience this year, the continued evolution of COVID-19 forced us to make a tough decision and again host an all-virtual conference.

As always, we've been working on ways to improve the event and the member experience based on previous attendee feedback. In addition to new topic areas and four highly engaging keynote speakers (Chris Krebs, Daymond John, Lisa Forte and Adam Steltzner), this year's Security Congress will be hosted virtually via a new interactive platform from Digitell, Inc., which will enable us to recognize continuing professional education (CPE) credits in real time. You'll be able to download your certificate of attendance/CPE credit certificate immediately following the completion of the event. No more waiting. We'll also showcase our brand new virtual 3-D exhibit hall.

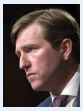
As a global membership organization, we want to deliver in-person event opportunities to where you are. For that reason, we anticipate reintroducing the (ISC)² Secure Summits next year, focusing on our global members. We will also be conducting Executive Roundtable meetings globally, which will provide opportunities for cybersecurity leaders to get together and share best practices while hearing from experts on security organization structure and strategy.

As more opportunities become available to interact in person, we hope you will take advantage of the chance to learn from each other in an open and welcoming environment and bring lessons learned back to your organizations. These events also give you the chance to address questions to (ISC)² leadership in sessions like our Town Hall, and let us know how we're serving your interests as a practitioner.

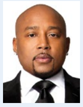
So, keep an eye out for information on our plans for 2022. We look forward to seeing you soon! ●

Megan Gavin is the Director of Events at (ISC)². She can be reached at mgavin@isc2.org.

Riveting Keynote Speakers



Chris Krebs is the former CISA director who will focus on the global cybersecurity landscape.



Daymond John, FUBU CEO and *Shark Tank* investor, discusses positive changes in life and work.

Lisa Forte of Red Goat Cyber Security explains the latest tactics in social engineering to steal for profit.

Adam Steltzner will share his own innovation challenges and leadership as leader and chief engineer of the NASA Mars 2020 mission and Rover Perseverance.

Discover the latest CLOUD SECURITY TRENDS & CHALLENGES

As organizations continue to migrate workloads to the cloud, utilizing new technologies to benefit from increased efficiency, better scalability, and faster deployments, they remain concerned about the security of data, systems, and services in the cloud.

The 2021 Cloud Security Report, sponsored by (ISC)², explores:

- Current cloud security trends and challenges
- How organizations are responding to security threats in the cloud
- Tools and best practices organizations are considering

Get ahead of emerging trends, arm yourself with the 2021 Cloud Security Report.

Get the Report

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

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

CCSP. Certified Cloud Security Professional

An (ISC)² Certification

FIELD NOTES

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

Something for Everyone at This Year's (ISC)^2 Security Congress

JOIN THOUSANDS of cybersecurity professionals at this year's virtual (ISC)² Security Congress 2021, taking place October 18 to 20.

Attendees will hear expert insights into the latest cybersecurity and career challenges. There are numerous opportunities to share best practices for combating threats, building teams, and implementing the latest processes and procedures to better defend your organization's critical assets.

Security Congress attendees can:

- **Learn** and earn CPE credits.
- **Add a two-day weekend training course** to earn an additional 16 CPE credits.
- **Strengthen understanding** of timely topics presented by insightful speakers, many of whom are (ISC)²-certified members.
- **Be inspired** by keynote speakers that challenge preconceptions about work, life and career.
- **Interact** with other virtual attendees through live session polling, virtual networking and chats.
- **Visit** an interactive, virtual 3-D exhibit hall with live chat and video features.

- **Sign up for one-on-one appointments** with our Career Center experts.

There's still time to register at congress.isc2.org. ●

Keynotes to Discuss Success in Both Life and Work

Chris Krebs, founding partner of Krebs Stamos Group

His presentation will focus on the global cybersecurity landscape, where businesses, infrastructure and our personal data are inextricably linked and constantly targeted by boundless threats.

9:30 to 10:30 a.m. EDT, Monday, October 18

Adam Steltzner, leader and chief engineer of the NASA Mars 2020 mission and Rover Perseverance

He will share his own innovation challenges, leadership struggles and flawless execution of a mission in which the Rover Perseverance touched down on Mars.

8 to 9 a.m. EDT, Tuesday, October 19

Daymond John, CEO and founder of FUBU

He is best known for backing innovative ideas on the hit TV show *Shark Tank*. John will break down the core tenets of his success to inspire Congress attendees to make positive changes in their own lives.

9 to 10 a.m. EDT, Tuesday, October 19

Lisa Forte, founder of Red Goat Cyber Security

She is a co-founder of Respect in Security, an initiative set up to take a stand against all forms of harassment in information security, who will talk about the latest in social engineering and other threats.

9 to 10:15 a.m. EDT, Wednesday, October 20

Photograph by Getty Images

CONTENTS

CMMC: A Model Born of Supply Chain Security

BY ADAM KOHNKE, CISSP

The following is excerpted from a much more comprehensive article featured in the August Insights e-newsletter now available online.

APPROXIMATELY 300,000 suppliers and organizations contribute to U.S. Department of Defense (DoD) combat efforts, its supply chain ecosystem and services needed to maintain DoD systems, networks, IT system installations, IT system capabilities and other technological services. In order to protect these suppliers, defend U.S. innovation interests and bolster national security, the DoD developed the Cybersecurity Maturity Model Certification (CMMC) to assess, grade and measure the maturity of IT controls for these suppliers operating in the industrial defense sector.

The model considered non-government organizations in its formation, making it adaptable to small businesses at lower CMMC maturity levels. The DoD also paired a certification element to the CMMC model, which can either be all-encompassing or target specific segments of an organization, allowing DoD suppliers or other businesses to demonstrate their level of maturity to show federal contract compliance or attract new business.

At the highest level, the CMMC seeks to determine adequacy of controls over two specific data types:

- **Federal contract information.** Data that the U.S. government either directly creates or directly provides to another party to create or manage a service for the federal government. This data should not be publicly available.
- **Controlled unclassified information.** Non-classified data that requires processing and public release strictly follow applicable laws, regulations or government policy

CMMC MODEL

CMMC MATURITY LEVEL	DESCRIPTIONS	CMMC PROCESSES
Level 1	Performed	No maturity processes are assessed at Level 1. Level 1 practices are performed, but there are no Level 1 process assessment requirements.
Level 2	Documented	Seeks to ensure an organization has established and documented practices within CMMC domains, which further allows the organization to execute the CMMC practices in a uniform manner and to realize expected outcomes. This maturity level requires establishment of a guiding policy that declares the specific objectives and importance of each CMMC domain.
Level 3	Managed	Establishes, maintains and resources a plan for managing all CMMC domain activities. The plan may include specific mission statements, detailed goals, a project plan, needed resources, mandatory training, and stakeholder participation requirements. Organizations must also adequately resource CMMC activities as defined by the plan.
Level 4	Reviewed	Requires routine review and measurement practices to determine practice effectiveness. Organizations must also execute corrective actions as necessary and formally notify higher-level management on the status of identified issues on a routine basis.
Level 5	Optimizing	Standardizes and optimizes process implementation throughout an organization. Development of standardized procedures as dictated by senior management will occur, and organizations must communicate and streamline this information throughout various organizational units.

that further determine the data lifecycle, how it is made available and to whom. Examples include network architecture diagrams for federal systems or compensation rates for contractors.

Additionally, the CMMC wants to reduce the likelihood and proliferation of advanced persistent threats.

The CMMC model moves one level deeper to measure cybersecurity maturity through a hierarchical assessment of domains, which are further subcategorized into processes, capabilities and capability practices. Organizational processes and capability practices are individually assessed and certified on a level of 1 to 5, with each level containing a distinct set of controls (CMMC practices) that are to be assessed and certified.

The accompanying chart shows how to obtain achievement at each level. Depending on your current security posture and adoption of best practices, attaining CMMC may prove easier than expected—or more difficult. It all depends on where you fall in the maturation cycle. ●

Adam Kohnke, CISSP, is the information security manager at the Infosec Institute in Madison, Wis.

Learn more about each level and what's required to achieve it in the August Insights e-newsletter.

DoD Adds HCISPP, CCSP to Approved Baseline Certs

The HCISPP® and the CCSP® certifications recently were added to the DoD 8570 Approved Baseline Certifications.

The HCISPP has been approved for the following categories:

- Information Assurance Manager Level 1 (IAM 1)
- IAM Level II (IAM II)

The CCSP has been approved for the following categories:

- Information Assurance System Architect and Engineer Level III (IASAE III)
- Information Assurance Technician Level III (IAT III)

To review all (ISC)² certifications required for certain levels of DoD Information Assurance roles, please visit https://www.isc2.org/Training/US-Government.

CONTENTS

Q&A

HOW I GOT HERE

Have I Been Pwned? Founder Troy Hunt on Finding Success

INTERVIEWED BY DEBORAH JOHNSON

Who gave you your first big break in cybersecurity?

It came very accidentally. I was working at Pfizer—we had a lot of outsourced development and a lot of atrociously bad software security then. So, I started writing blog posts for software developers about security. The first thing that really got me traction on cybersecurity was writing the OWASP (Open Web Application Security Project) Top Ten for ASP.NET.

What made you launch Have I Been Pwned?

I was doing a batch analysis on data breaches, and one breach I was looking at was Adobe. I was in the Adobe data breach twice, which I found quite fascinating. I'd never even given my data to Adobe; I had given it to Macromedia. Adobe bought Macromedia, so my data flowed to them and then, suddenly, I'm in this data breach. And I thought, "Wow, if this is news to me, surely it's news to other people as well, so maybe this is a useful service."

Has its success surpassed expectations?

It exceeded my expectations within the first two weeks, and we're approaching eight years now. I don't know that success is the right word for it. Popularity, perhaps, for the service. It has exceeded those expectations.

If you were hiring, what is the absolute-must trait a candidate must have to excel in this industry now?

Let me give you two. Competency is extremely important, but competency is not necessarily experience. I think there are plenty of folks out there who are very young and new in their careers, but they are very good at what they do.

I feel also that the passion is important. I think back to all the times that I was interviewing people for technology roles, and clearly for them it was a 9-to-5 job and they were not all that passionate for it.

So, I don't care too much about years of experience. I definitely don't care too much about formal qualifications, having dropped out of university myself. What I really care about is people that can do stuff and love it. ●

This interview has been edited and condensed for length.

TROY HUNT

Hunt is a Microsoft Regional Director and founder of the website Have I Been Pwned? that attracts more than 10 million unique visitors daily. Based in Australia's Gold Coast, Hunt designed software for Pfizer for 14 years and later created ASafaWeb, an automated security analysis tool for ASP.NET applications. A popular blogger/vlogger and public speaker on cybersecurity issues, Hunt received the 2020 (ISC)^2 Senior Professional Award for the APAC Region.

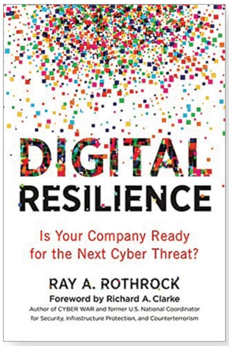
CONTENTS

RECOMMENDED READING

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

Digital Resilience: Is Your Company Ready for the Next Cyber Threat?

BY RAY A. ROTHROCK (*AMACOM, 2018*)



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

CYBERATTACKS on businesses and institutions grew by 51% in 2020, according to a study by Positive Technologies, a global security solutions provider. The trend continues, and no organization is invulnerable. Resilience is key, says cybersecurity expert and investor Ray Rothrock, whose book offers guidance to warding off or recovering from an attack.

Rothrock provides no magic checklist. Rather, he discusses security by design, such as building the infrastructure with security in mind while thinking like an attacker. His focus is on containments and implementing a means of data recovery and forensic analysis, and less—yes less—on prevention. Spending to mitigate the attack and ensure the resilience and recovery of the enterprise is the key. The one topic not included is cyber resilience requirements for regulators.

His focus is on containments and implementing a means of data recovery and forensic analysis, and less—yes less—on prevention.

Digital Resilience: Is Your Company Ready for the Next Cyber Threat? presents strategies that are effective, with guidance on how to design organizations and systems to better absorb disruptions. This is a mental framing and shaping of an issue that is instilled to obtain a better sense of cyber risk amongst decision makers.

This book, when overlaid with the latest guidance from the National Institute of Standards and Technology, NIST SP-800-160, supplies the reader with a strategy and approach to secure a network and mitigate risk where possible. ●

Ransomware in U.S., U.K. Most Likely to Hit Government Systems

A State of Ransomware report from January through June by data privacy and security vendor BlackFog shows most U.S. and U.K. victims during the first half of this year came from the government and education sectors. If 2020 is any indication, expect a ramp-up in attacks come October.

ATTACKS BY INDUSTRY	
Government	25
Education	24
Services	23
Manufacturing	17
Healthcare	16
Technology	14
Retail	8
Utilities	6
Finance	3
Other	10

ATTACKS BY COUNTRY	
U.S.	70
U.K.	19
Canada	8
France	7
Netherlands	4
Japan	4
Brazil	4
Rest of World	50

Source: BlackFog Ransomware Report, June 2021

CHAPTER SPOTLIGHT

Where One Opportunity Closes, Another Opens for Hellenic Chapter

> “What we have observed through these interactions is the need for more technical training, as lack of technical skills is apparent.”
>
> —*Dimitrios Patsos, (ISC)² Hellenic Chapter President*

Photograph by Getty Images

LIKE OTHER (ISC)² CHAPTERS, the Hellenic Chapter was forced to pivot when the pandemic imposed curfews and prevented in-person events. Rather than halt plans, it moved everything online at a time when programs like Safe and Secure Online were more important than ever.

The Chapter’s first virtual cyber safety presentation for parents and the general public was held in April 2020 and, based on its success, chapter members held three more publicly available live presentations and one private one.

This was a big step for Greece’s only official (ISC)² chapter, founded by 27 cybersecurity enthusiasts who in the past six years have expanded the group to 260 registered members from areas of cybersecurity, data protection, privacy and information technology including professionals and students.

The Chapter has embraced the Center for Cyber Safety and Education’s Safe and Secure Online program for schoolchildren, parents, senior citizens and anyone interested in cybersecurity. In June 2019, chapter members translated Safe and Secure Online material into Greek and by April 2020, all translated material was available for download on the Center’s website.

In total, the Chapter has reached more than 160 individuals, making a positive impact on the local community and helping to make the cyber world a safer place for everyone.

“The feedback we get on every event is very encouraging, as all attendants recognize how well structured and understandable this educational material is,” said Chapter President Dimitrios Patsos. “What we have observed through these interactions is the need for more technical training, as lack of technical skills is apparent. We have been internally working on this and plan our way to provide specific workshops to that end, accompanied also by some step-by-step instructions for basic things.”

Earlier this year the Chapter partnered with another Greek nonprofit organization to create animated short videos on digital rights and cybersecurity training and awareness. All are in Greek and will be freely available on the Chapter’s website.

The next initiative is to reach into academic and government circles to teach college students and employees how to stay safe online. ●

(ISC)² GLOBAL Achievement Awards

Announcing This Year's (ISC)² Global Achievement Award Recipients

Congratulations to the following security professionals being recognized as Global Achievement Award winners for 2021. These awards recognize individuals who have made outstanding contributions to cybersecurity and the information security industry, honoring their tireless efforts and standards of excellence. Honorees were nominated by qualified colleagues, mentors and peers.

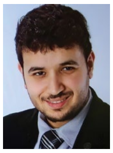
(ISC)² F. Lynn McNulty Tribute Award

The (ISC)² F. Lynn McNulty Tribute Award recognizes an individual for their outstanding dedication, service and commitment in the government information security workforce and/or strengthening the security posture of the country's information resources and infrastructure. This award highlights information security leaders who uphold McNulty's legacy as tireless advocate for the security of the nation and a persistent champion of information security in government. The 2021 honoree:

Kelvin Coleman is being recognized for his role in launching Cybersecurity Awareness Month, a joint effort by the NCSA and U.S. Department of Homeland Security in October 2004. Participation has grown annually to help citizens protect connected devices at home and work.

(ISC)² Senior Professional Award

Recognizing individuals who have significantly contributed to the enhancement of the information security workforce by demonstrating a leadership role in an information security workforce improvement initiative, program or project. The 2021 honorees:



- Americas: **Marouane Balmakhtar**, CISSP, principal technology strategist for T-Mobile, for a 5G cybersecurity and security awareness initiative.

- Asia-Pacific: **InJung Kim**, senior researcher, the Affiliated Institute of Electronics and Telecommunications Research, for establishing a roadmap for Korea's cybersecurity technology that ensures security, transparency and trust.

- EMEA: **Soney Paul Bahanan**, information security manager for NMC Healthcare in the United Arab Emirates, for his role in the Abu Dhabi Health Information Cyber Security Standard to strengthen privacy and security within healthcare.

(ISC)² Mid-Career Professional Award

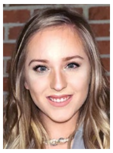
Recognizing individuals at their mid-career stage who have demonstrated commitment and achievement in managing or implementing a vital component of a cyber, information, software, infrastructure program/project. The 2021 honorees:

- Americas: **Diondria L. Holliman**, CISSP, IT cybersecurity analyst, Medtronic, for successfully impacting the UBS Block program across 95,000 employees in 160 countries to prevent data exfiltration. Co-founder and CISO of the Cyber Society and The Wonder Hub organizations devoted to advancing minorities in cybersecurity.

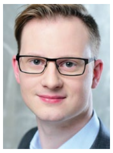
- Asia-Pacific: **Neha Malhotra**, CCSP, CISSP, vice president, Cyber Security Attack Surface Management for managing the implementation of an ambitious global vulnerability management and secure configuration management optimization program.

(ISC)² Rising Star Professional Award

Recognizing the accomplishments and contributions of an up-and-coming professional who has made a significant impact in the information security industry early in their career. The 2021 honorees:



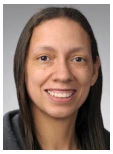
- Americas: **Kathryn M. Murphy**, cybersecurity engineer for MSAG, for her role in the Department of Defense's Comply to Connect project to identify, authenticate and control all devices attached to the DoD Information Network.



- EMEA: **Alexander Kuehl**, CISSP-ISSMP, CAP, SSCP, information security expert at Kuehne + Nagel International in Germany, for his significant role in the company's U.K. contract.

(ISC)^2 Government Professional Award

Recognizing government information security leaders whose commitment to excellence has helped to improve government information security and to advance an in-demand workforce. The 2021 honorees:



- Americas: **Erica M. Mitchell**, CISSP, Critical Infrastructure Key Resources team lead at the Army Cyber Institute, for her role in the Jack Voltaic Cyber Research Project focused on critical infrastructure resilience.

- Asia-Pacific: GP Capt. **Amorn Chomchoey**, CISSP, acting deputy security general, National Cyber Security Agency of Thailand, for his role in using gamification to improve Royal Thai Air Force cybersecurity operations.

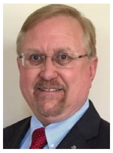
- EMEA: **Angella Tugume**, CISSP, risk analyst for the National Information Security Framework within the Government of Uganda Agencies, for leading assessments and operational guidance for 20 government agencies seeking NISF compliance.

(ISC)^2 BOARD AWARDS

Recognizing outstanding contributions and achievements in the field of cybersecurity over the course of a career. The following award recipients for 2021 were selected by the (ISC)^2 Board of Directors.

(ISC)^2 Harold F. Tipton Lifetime Achievement Award

The Tipton Award is presented by the (ISC)^2 Board of Directors as the highest tribute bestowed in the information security industry. Named after Harold F. Tipton, CISSP, known as the "George Washington of information security," the award honors his memory and the tradition of passionately promoting and enhancing the information security profession by serving over the long term with excellence and distinction. The 2021 recipient:



Rich Owen, CISSP, CEO of Johnny Security Seed, LLC, for his many years contributing to the information security industry, particularly when there were limited resources to build quality programs, including one built at the Johnson Space Center basically from scratch. The Mission Operations "Automated Information Systems Security Manual" (JSC-23982) was one of the first programs to define security as protecting confidentiality, integrity and availability. Owen then went on to be a pioneer in early use of risk-based decisions for the protection of information, for which he was recognized by the NASA Administrator. He continues to share what he's learned over decades through his company, oftentimes at reduced costs.

Kaminsky's research on botnet attack patterns enabled the community to detect the Conficker botnet and to develop best practices for developers.

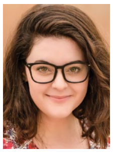
Fellow of (ISC)^2 Award

The Fellow of (ISC)^2 Award was established to honor and distinguish an elite information security professional who has made outstanding contributions throughout their career to the information security profession. The 2021 recipient (given posthumously):

Dan Kaminsky, co-founder and chief scientist, HUMAN (formerly White Ops), was a top security researcher who passed away earlier this year. He had helped to fix a key flaw of DNS system in a responsible and coordinated manner that earned him the title of "internet security savior" and "a digital Paul Revere." Kaminsky's research on botnet attack patterns enabled the community to detect the Conficker botnet and to develop best practices for developers. Additionally, he advocated for privacy rights.

(ISC)^2 CEO Award

The (ISC)^2 CEO Award recognizes members who have made a significant impact on the cyber community by contributions to (ISC)^2 through dedicated and exceptional volunteer efforts. The 2021 recipient:



Megan West, CISSP, X-Force Cybersecurity Incident Responder, IBM X-Force, for "Cybersecurity Meg," created in late 2020 across multiple social media platforms to share free cybersecurity content that aspiring professionals can harness to acquire their first job in the field. By sharing her own expertise in incident response and more

CONTENTS

general experiences in cybersecurity, West empowers a more diverse set of candidates to pursue cybersecurity and acquire popular certifications such as the CISSP and CompTIA Security+. West also places a large emphasis on mentoring women and people of color who are pursuing cybersecurity careers.

(ISC)² Diversity Award

The (ISC)² Diversity Award honors an individual who represents the core values of (ISC)² through significant contributions in driving a more diverse workforce in the cybersecurity community. The 2021 recipients:

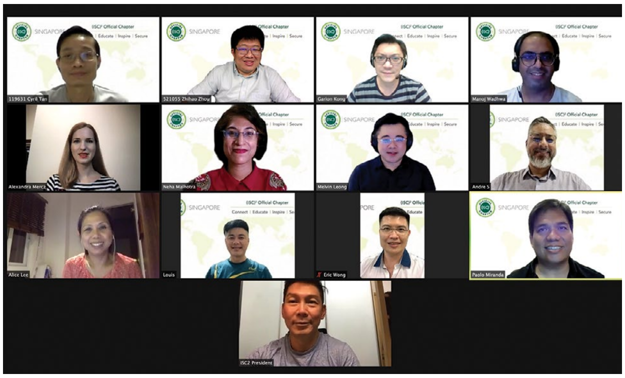
- Americas: **Julian Waits**, general manager of cybersecurity for Devo Technologies, for being a mentor to young, minority cybersecurity professionals. In his 30-plus-year career in cyber, Waits has mentored more than 50 individuals and hosts a podcast called *Cyber Unfiltered*, where he addresses diversity in cybersecurity.

> In his 30-plus-year career in cyber, Waits has mentored more than 50 individuals and hosts a podcast called *Cyber Unfiltered*, where he addresses diversity in cybersecurity.

- Asia-Pacific: **Neha Malhotra**, CCSP, CISSP, vice president, Cyber Security Attack Surface Management for Credit Suisse in Singapore, for encouraging and mentoring others to join cybersecurity and serving as a role model in information security for the past nine years. In 2020, she spoke at global and regional cybersecurity conferences, gave virtual talks, podcast interviews and panel discussions on, among other topics, women in cybersecurity and IT. Malhotra also is actively involved with numerous Women in Security global and local communities and initiatives.

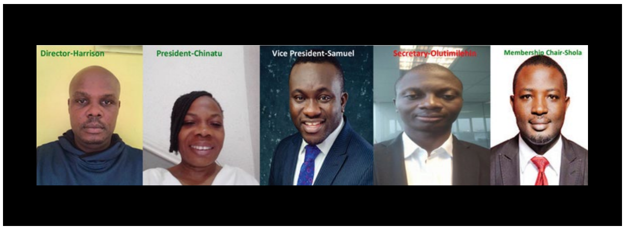
(ISC)² Chapter Recognition Awards

The (ISC)² Chapter Recognition Awards are presented to official Chapters of (ISC)² within each region that best promote the vision of (ISC)² by inspiring a safe and secure cyber world. Each Chapter has demonstrated a well-rounded offering of activities and services designed to benefit its members and affiliates, while making a significant contribution to the profession and its local community through the core focus areas of the (ISC)² Chapter Program of Connect, Educate, Inspire and Secure. The 2021 recipients in each region:



Members of the (ISC)² Singapore Chapter

- Asia-Pacific: **(ISC)² Singapore Chapter** – The Chapter continues to gain notoriety by developing engagement initiatives in partnership with local schools and organizations to conduct career talks to promote outreach, and renewed its partnership with the Association of Information Security Professionals, which will allow Chapter members to network and collaborate professionally with other cybersecurity organizations. The Chapter also successfully began its mentorship program and works daily to inspire the next generation of cybersecurity professionals.



Members of the (ISC)² Nigeria Chapter

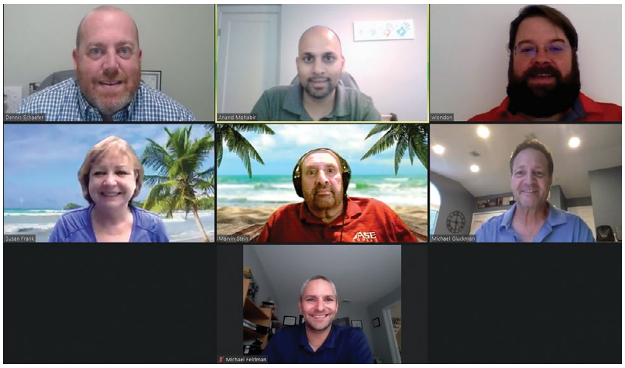
- EMEA: **(ISC)² Nigeria Chapter** – One of the most active Chapters in the EMEA region, the Nigeria Chapter hosted several programming events in a series focused on educating the Chapter's membership and local community, including several panel discussions and a mini-series focused on Cyber Security Awareness Month titled "Do Your Part in the New Normal, be CyberSmart." The Nigeria

The Nigeria Chapter's diligence in offering educational opportunities to members proves that no matter the circumstance, (ISC)² members have a drive to continue learning and educating the community to stay ahead of what may come.

Chapter's diligence in offering educational opportunities to members proves that no matter the circumstance, (ISC)² members have a drive to continue learning and educating the community to stay ahead of what may come.

(ISC)² Argentina Chapter president Hernan Coronel

- Latin America: **(ISC)² Argentina Chapter** – The Chapter leveraged social media to increase visibility and grow membership during unprecedented times. The Chapter, along with five other LATAM Chapters, hosted a regional virtual conference (CyberSec Talks) where more than 700 people from more than 20 countries registered to attend the two-day event, proving that Chapters that work together to connect members, educate the public and inspire future leaders can make a big impact.



Members of the (ISC)² Long Island, NY Chapter

- North America: **(ISC)² Long Island, NY Chapter** – The Chapter, which only received its official charter in 2019, worked to build a strong and agile foundation to shift its needs to fit the changing atmosphere during the COVID-19 pandemic. Members hosted virtual Chapter meetings while growing attendance—providing both educational sessions as well as networking opportunities (like capture the flag) for members. The Chapter has built strong relationships with companies and organizations in the local community, proving that even newer Chapters can have the strength to inspire and connect the local community in hopes to inspire a safe and secure cyber world.

CENTER FOR CYBER SAFETY AND EDUCATION AWARDS

Julie Peeler Franz "Do It For The Children" Volunteer Award

The Center for Cyber Safety and Education's Julie Peeler Franz "Do It for The Children" Volunteer Award recognizes an individual who has significantly contributed to the betterment of internet safety. With a passion for cyber safety education and a desire to give back to their community, this recipient is considered an example and role model to the security community. The nominated individual must have volunteered for the Center for Cyber Safety and Education within the last 12 months. This award is given to a volunteer whose contributions have directly impacted how children, adults and seniors alike navigate the internet safely. The 2021 recipient:

Roela Santos of Virginia, for her long-time support of the Center's programs and being solely responsible for securing both the Raytheon and SAIC information security scholarships that over the last six years have awarded $424,000 to 56 students.

Partner of the Year

The Center for Cyber Safety and Education Partner of the Year Award recognizes a company or organization where it and/or its employees/members donate their time, talent and treasure to support and advance the Center's programs to deliver vital cyber safety programs and/or scholarships to inspire a safe and secure cyber world. This must be a group or company effort of support not that of a lone employee or member. The 2021 recipient:

Capa8 of Mexico, for spearheading and helping fund the translation and conversion of the Garfield programs from English into Spanish including translation, graphics and cartoons (revoiced). Special recognition given to Capa8 co-founders and directors **Juan Pablo Carisi** and **Ana Cecilia Perez Rosales.** ●

CONTENTS

ADVOCATE'S CORNER

War, Famine, Pestilence, Data Breach

Many view rapid change as a relatively modern phenomenon because of the fast-paced digital world we all live in. In fact, exploitation of vulnerabilities by threat actors has been going on for thousands of years.

BY TONY VIZZA, CISSP, CCSP

A FEW HOURS' DRIVE outside of Sydney, Australia, are the central west and Riverina regions of New South Wales. These regions teem with wheat, barley, oat and canola farms as well as sheep and cattle pastures. In recent years, a devastating drought in these areas brought many farmers to ruin. This was followed by the enormous bushfires that made global news at the end of 2019. Almost immediately after this, the COVID-19 pandemic pushed the entire globe into uncertainty and, tragically, immense loss of life.

While many farmers in these parched and burnt regions were wondering, "What next?," a miracle occurred. These regions received their first substantial rains in many years. Rivers and dams were finally filling, with the hope that perhaps the people of the land had finally turned a corner. Farmers and their families popped champagne bottles to celebrate the drought's official end.

Fast forward a few months, where bumper crops are being harvested. Grain bins are full. Livestock are healthy. The world is inching closer to a sense of COVID normal. People are optimistic.

Amid these better times, few could have predicted that a plague of mice that media outlets have described as "biblical" would eat through grain stores, stock feed and practically anything else that rodents could find as edible. These swarms of mice have caused hundreds of millions of dollars in damage and are one of the biggest plagues ever recorded in Australia. The mice have sparked health concerns due to drinking water contamination and have forced still-pandemic-reeling governments to provide farmers with free grain treatment and pesticide. In the wake of this plague, farmers are also having to contend with the threat of venomous snakes that feed off the rodents. Yet another threat to contain.

It was in the context of the Colonial Pipeline ransomware attack and countless other cybersecurity incidents to emerge that I started to appreciate the idea that any environment, regardless of the nature, is fundamentally insecure. Consider the farmer. Agriculture is one of the oldest industries in existence and critical to human survival. Yet, it operates at the complete mercy of the environment, something that a farmer has little to no control over. Despite the thousands of years of history of agricultural achievement throughout the world, there remains a plethora of new and emerging vulnerabilities, threat actors and methods to exploit vulnerabilities when the time is right.

There is a quotation, often misattributed to Thomas Jefferson, that "Eternal vigilance is the price of liberty." For farmers, despite the innovations in agriculture over the course of thousands of years, successfully toiling over the land still comes down to sun, rain, good fortune, and eternal vigilance protecting fields from threats and managing vulnerabilities and risks across the food lifecycle as best as they can.

For cybersecurity professionals, it may perhaps involve a little less sun and rain, but it certainly does continue to involve eternal vigilance—from insider and outsider threats; from vulnerabilities that crop up by the second; from risks that are unknown and not immediately apparent. And a pinch of luck. ●

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

CONTENTS

(ISC)²

Benchmark Your Organization's Security Posture & Best Practices

How do your internal practices and security investments stack up against other organization from around the world? Find out in CyberEdge Group's 2021 Cyberthreat Defense Report, sponsored by (ISC)².

Among a long list of key findings in the report, results reveal cybersecurity teams have faced unprecedented challenges:

- A record **86%** of organizations experienced a successful cyberattack, **up from 81% the prior year**, the largest year-over-year increase in six years.
- A record **69%** of organizations were victimized by ransomware, **up from 62% the prior year**.
- A record **87%** of organizations are experiencing a shortfall in skilled IT security personnel, **up from 85% the prior year**.

Download the full 2021 Cyberthreat Defense Report to benchmark your organizations security posture and best practices against your industry peers.

CYBEREDGE GROUP

2021 Cyberthreat Defense Report

North America | Europe | Asia Pacific
Latin America | Middle East | Africa

« Research Sponsors »

PLATINUM

(ISC)² Gigamon imperva Menlo Security perimeter81

GOLD

KnowBe4 MICRO FOCUS thycotic

SILVER

APPGUARD BINARY DEFENSE Cymulate interos

Get the Report

2021 Cyberthreat Defense Report - Sponsored by (ISC)²

Onboarding Strategies to Hold On to Talent

BY DEBORAH JOHNSON

After a time-intensive and possibly expensive search, you've hired a new employee. Now, it's time to set them on the best course for everyone's success.

"Simply do not sit them in a room and inundate them with either written material or online modules," warns Carol Leaman, CEO of Ontario, Canada-based training consultants that comprise Axonify, in a phone interview. Research into information retention shows "sitting somebody down and fire-hosing them with all the information you think they need to know to perform effectively simply isn't effective."

Instead, Leaman advises to prioritize and use short bursts to deliver key learning points. "If you intersperse other activities with something new, do four or five things at most, and then spend some time reinforcing those things," she says.

Successful onboarding can take time, perhaps several weeks or longer. The Society for Human Resource Management recommends check-ins with new hires after the first month and then again at six months. By then, the organization claims, nearly 90% of new hires will have weighed whether to stay or go.

It's crucial to know where the new team member is coming from. While you need to clearly spell out your expectations, be aware that the new hire has goals too, cautions Leaman.

"People coming into the workforce today have an expectation that they're going to get something out of it," she says. "They come in with [their own] plan. While it may not be fully formed, they've got a career growth objective, and they're looking for you to help them get there."

Also, acknowledge the generational differences of today's workforce. "It's important to create a healthy work environment that's inclusive to all generations," counsels the Human Capital Institute on its blog. From Baby Boomers to Gen Xers to Millennials to older members of Gen Z, the post says, "Things like their preferred forms of communication and the benefits that are important to them will look different for people who are at separate stages in life."

Beat the onboarding odds

Only 12% of employees strongly agree their organization does a great job of onboarding new employees, according to Gallup's State of the American Workplace Report. An unsuccessful onboarding experience costs the company time, money and productivity.

Here are some key steps for effective onboarding gathered from various HR professionals:

- Be ready and welcoming on an employee's first day.
- Clearly communicate goals and expectations.
- Regularly share the company's culture and vision.
- Set up a mentor or partner for the new team member.
- Start new hires on projects based on their experience and their grasp of the work.
- Ensure management and senior leaders connect with new team members during the onboarding period.
- Give onboarding sufficient time to work.

Structured and supportive onboarding should give you and the new employee better odds for success. ●

Photograph by Louise Roup

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

CONTENTS

CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

The BUZZ is Real

"The Next Big Thing"
- Certification Magazine

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

Build on Your CISSP Expertise and Master Cloud Security

You've proven your expertise in cybersecurity…now prove yourself as the authority in cloud security for your organization.

The Certified Cloud Security Professional (CCSP) credential was designed to build on your deep technical and managerial CISSP knowledge and position you at the highest level of mastery for cloud security.

- **Grow with (ISC)²** – Validate your specialized skills and invest further into your membership with no additional fees. CISSPs already meet the experience requirements and your CPE credits are transferrable.
- **Cutting-Edge Credibility** – CCSP positions you as an authority in cloud security, highly adept in staying on top of the latest technologies, developments, and threats.
- **Broad Agility** – CCSP's vendor-neutral and multivendor qualifications may be applied across a range of cloud platforms, making your individual skillset more marketable.
- **Soaring Demand and Earning Power** – The demand for cloud security skills is projected to grow 115% over the next 5 years and command the highest premium at US $15,025.

Make Your Move

TO PAY OR NOT TO PAY

That is the ransomware question

BY JULIEN LEGRAND, CISSP

THERE ISN'T A CYBERSECURITY PROFESSIONAL out there who hasn't considered what to do if their organization is hit by ransomware. Almost weekly now there's a record-setting ransom or novel attack mode reported to authorities and by the news media.

Criminal syndicates, including those attached to nation-states, are continually upping the ante in both the price for a precious decryption key as well as a target to disrupt. No longer targeting healthcare and law enforcement, ransomware developers are moving up the stack to hold hostage fuel and food supplies, our small businesses and critical infrastructure.

The year may not be over, but it appears ransomware will be the dominant story for 2021.

Recent Gartner research predicts that by 2025, 75% of IT organizations will face one or more attacks, with a dramatic increase in ransomware attacks pointing to sevenfold or higher growth rates. With those odds, we need to talk about whether to pay or not to pay the ransom in order to get back to business—and prepare for the next attempted breach.

IMAGES BY JOHN KUCZALA

CONTENTS

RANSOMWARE ATTACKS ARE EVOLVING

Threat actors often deploy present-day ransomware as part of a more significant attack involving network penetration using stolen credentials or remote malware, subverting critical administrative accounts, access to the backup consoles and data theft. This means that ransomware's goal is not just to encrypt data. Attackers leverage the tactic to steal sensitive information for future criminal activities.

Ransomware attacks may take weeks or even months to accomplish, often leaving malicious programs deeply embedded in the target systems in an organization. According to Gartner, successful attacks deploy ransomware to encrypt critical data, including backup stores accessible on the compromised network.

Besides locking users away from their files, attackers threaten to modify, delete or post stolen information online to coerce victims to pay ransom demands.

The United Kingdom's National Cyber Security Center (NCSC) lays bare the work of state actors in distributing ransomware. Referencing the infamous WannaCry and NotPetya attacks, NCSC earlier alerted the public to the potential impact of ransomware incidents. Both of those outbreaks revealed how ransomware could spread independently throughout networks. Ransomware can virtually impact almost every connected device and service.

Another central argument drawn from the NCSC report is the motivation behind the rise of ransomware: data. Such attacks succeed because organizations struggle to operate without data. Even a brief halt on the most mundane administrative functions due to data loss can bring an entire company's operations to a standstill.

In the past, malicious hackers locked users away from their data, impacting availability in the information assurance triad. The prevalence of backups and system redundancy effectively became famous as a way of mitigating such attacks.

Today, threat actors have moved to availability, integrity and confidentiality functions. Besides locking users away from their files, they threaten to modify, delete or post stolen information online to coerce victims to pay ransom demands.

CRYPTOCURRENCY ENABLED A SURGE IN RANSOMWARE

MarketWatch revealed that crypto revenues from ransomware surged more than 300% in 2020 from the previous year. Attackers require victims to make payments to digital wallets, a method that makes it difficult for authorities to track the perpetrators.

According to the Ransomware Task Force, an international coalition of government officials, law enforcement and private-sector technologies, cryptocurrencies add to the challenge of tracking down ransomware authors due to the digital currencies' borderless nature. However, as we recently discovered, intercepting a ransom payment is not impossible; U.S. authorities did just that after a ransom was paid to get fuel flowing again for the gas company Colonial Pipeline.

The recent disabling of Colonial Pipeline's activities underscored the threat ransomware poses to critical infrastructure globally. The Wall Street Journal reported that the government paid ransom to cybercriminals who caused the shutdown. Sources privy to the incident revealed that the ransom, paid in cryptocurrency, amounted to U.S. $5 million at the time of transaction. That attack and the ensuring consumer panic resulted in regional gasoline shortages and higher prices.

Soon after, a similar attack struck global meatpacker JBS USA, disrupting food supplies in the United States and Australia before the company reportedly paid U.S. $11 million in bitcoin to its attackers. Then, over the Fourth of July holiday in the United States, the same group behind JBS deployed its "ransomware-as-a-service" to simultaneously strike more than 1,500 businesses globally, most smaller operations with limited means to pay off a total of U.S. $70 million demanded by the data hostage holders. They used what is an increasingly common vector: infecting software belonging to a vendor within their victims' supply chains.

CHALLENGES OF RANSOMWARE VICTIMS

Cybersecurity professionals admit that devastating ransomware attacks are becoming more frequent. Recent research shows that an organization fell victim to a ransomware attack on average every 10 seconds in 2020. It takes days or even weeks to recover from such incidents. In some cases, full recovery may not be possible at all.

Ransomware scammers hijack IT systems, data and operations, thereby disrupting the order and stability of communities. Simply put, ransomware attacks result in possible loss of company data, temporary or complete shutdown of operations, financial loss due to disrupted activities and remediation efforts, and damage to the company's reputation. If such incidents occur in hospitals and other critical infrastructure, it can result in severe physical damage and loss, which are all threats to economic prosperity and national security.

SHAPING UP TO BE THE YEAR OF RANSOMWARE

Though ransomware is not new, it's having a moment, with an uptick in both successful attacks and record ransoms. Here are just some of the breaches that made headlines this year. No doubt more will make this list before the year ends.

- Credible news outlets report **Kia Motors** suffers a widespread IT outage tied to a U.S. $20 million ransomware demand by the DoppelPaymer gang. The company denied the attack, let alone paying to restore systems.
- Polish video game developer **CDProjekt Red** is attacked by the HelloKitty gang, which steals source code and locks down devices. Published reports say CDProjekt didn't plan to pay the ransom because it had backups that were left untouched.
- REvil exploits a vulnerability in a Microsoft Exchange service to lock down computer maker **Acer**'s files, then leaks sensitive documents. REvil demands U.S. $50 million in Monero cryptocurrency.
- REvil demands a U.S. $50 million ransom from computer manufacturer **Quanta**. When Quanta refuses to negotiate, criminals release private product development documents tied to Quanta business partner Apple's new MacBook.
- A group called Babuk attempts to extort the **National Basketball Association** after allegedly stealing 500 GB of confidential data concerning the Houston Rockets. No ransom payments have been made, according to published reports.
- **Colonial Pipeline** is hit by ransomware that disrupts gas supplies all along the East Coast of the United States, causing chaos and panic. It paid roughly U.S. $5 million in bitcoin, some of which federal authorities were later able to trace and retrieve.
- Chemical distributor **Brenntag** is told to pay U.S. $7.5 million in bitcoin to get back 150 GB of data taken by the same criminals behind the Colonial Pipeline attack. The company ends up negotiating the ransom down to U.S. $4.4 million.
- REvil is believed to be behind another headline-grabber, this time locking up systems at **JBS Foods**, one of the world's largest meat processors. JBS reportedly paid the U.S. $11 million ransom in bitcoin, among the biggest payments up to that point.
- European company **AXA** had no sooner announced it would stop reimbursing certain clients for ransomware payments when it suffered its own ransomware attack, having up to 4 terabytes of data held hostage by the Avaddon gang.
- More than 1,400 mostly small businesses that were customers of software maker **Kaseya** are hit with ransomware in a supply chain attack. REvil is believed to be involved and demanded U.S. $70 million in cryptocurrency from the collection of victims. ●

Undoubtedly, most businesses do not know how to regain their systems and data once a ransomware attack threatens to permanently destroy the data. This uncertainty has led many executives to pay threat actors, even with other cheaper and safer alternatives to pursue. As Gartner reports, the nature and scope of ransomware attacks are often misunderstood. This observation leads to insufficient precautions and protections against ransomware and inadequate responses to successful attacks.

PAY OR NOT PAY

Ransomware payments may sometimes appear the safest and the most suitable course of action for an organization under an attack. Regrettably, too often taking this path does not yield expected results. Decryption keys, if issued, don't always work. And paying a ransom is duly noted by cybercriminals now apt to target your systems again.

A cautionary tale detailed by the U.K.'s NCSC revealed that an organization paid a ransom and recovered its files using the supplied decryptor. The victim did not identify the root cause to secure the network, resulting in another attack from the same group in less than two weeks, using the exact mechanism as before. The unnamed company felt it had no other option but to pay the ransom a second time.

Paying the ransom might unlock critical systems in the short term, but it can cost organizations more in the long run. Research shows that one in every four organizations is paying attackers to get encrypted files back, but doing so only costs more and could haunt victims in the future.

The average cost of a ransomware attack for victims that paid is almost U.S. $1.4 million, while those that did not give in to a ransom demand spent half of that, totaling $732,000, according to a ZDNet report. Getting an encryption key from criminals is not a simple fix. Apart from the ransom payment, organizations must restore the networks.

Paying ransomware gangs also marks you as a victim willing to pay. This means that criminals could target you again to make a quick buck. If paying the ransom becomes known to the public, it can negatively impact the company's reputation due to a lack of trust in how the organization handles information security. On the other hand, restoring data from backups and system redundancies demonstrates that a firm has a way to get back to normal operations without giving in to attackers' demands.

Also, paying criminals ransoms could fund other illegal activities. The money may be used for purposes of terrorism and war. For instance, North Korea reportedly fired a salvo of ransomware attacks targeting other countries to hunt for cash through cryptocurrency extortion. The country, which has previously relied on other criminal activities like currency counterfeiting, arms exports and drug trafficking, is now turning to cyberattacks as an efficient and "safe" way to obtain funds.

PREVENTING RANSOMWARE ATTACKS

There is no hard-and-fast rule for mitigating ransomware attacks or determining who will be hit next. Like other data breaches, ransomware attacks start opportunistically. Therefore, ransomware prevention revolves around a multi-layered security strategy.

Early detection of suspicious activities. Gartner recommends early detection of suspicious activities as the first line of defense against ransomware. In this situation, organizations should implement reliable antimalware and antivirus software across almost all systems, from enterprise servers to employee devices.

Anomaly detection through behavior analysis. Organizations can leverage artificial intelligence and machine learning to detect abnormal patterns, such as a significant change in data downloads, and alert security specialists. Modern endpoint security tools can prevent attacks and ensure other controls like user behavior analysis and real-time data backup.

Follow cybersecurity best practices. Ensure your network and systems are secure enough by applying patches, changing default passwords, applying multifactor authentication, and installing firewalls and intrusion detection and prevention systems. Without a doubt, ransomware peddlers are opportunistic and always looking for the weakest links. They pick victims from a list of companies that had their email lists leaked, forgot to patch their operating systems, or left network ports open.

Back up crucial information. It is advisable for organizations to regularly back up their systems and information. Additionally, backup stores should be in a separate network from the production one so, in the event of a data breach, service and system restoration can take place with the least disruption.

TREAT BOTH CAUSE AND SYMPTOMS

For most ransomware victims, their priority is justifiably to get their data back and return a business to regular operations. However, organizations need to note that ransomware is often a visible symptom of a persistent network intrusion. Even after removing the malware and restoring data from backups, companies should look for backdoor access to networks and review administrative privileges and access to prevent criminals from redeploying the ransomware.

To install ransomware, attackers may have managed to gain backdoor access to your network as well as your administrator privileges and login credentials. ZDNet posts that if attackers have that, they can quickly deploy another attack if they wanted to, even after a victim pays the ransom. ●

Julien Legrand, CISSP, CEH, CISM, CISA, CRISC, CCNA is a cybersecurity architect at Thales.

ADDITIONAL (ISC)² RESOURCES FOR RANSOMWARE

Earlier this year (ISC)² allowed anyone to access its Professional Development Institute course on ransomware—for free—through the end of July. There are still plenty of resources available to help prevent ransomware from infiltrating your networks and machines. Here are some of them:

▶ PDI COURSE

Ransomware: Identify, Protect, Detect, Recover

This course remains free for (ISC)² members and yields two CPE credits upon successful completion of a post-course assessment. Recommended for cybersecurity professionals with a beginning to intermediate knowledge of ransomware concepts.

https://www.isc2.org/Development/Express-Learning-Courses/Ransomware-Identify-Protect-Detect-Recover

▶ ARTICLE

Ransomware 2.0, Cybercrime & Cloud Security

This article applies "Sutton's Law" (named after a 20th-century bank robber) to show how ransomware is likely to be of greater concern to cloud security "because that's where the data is."

https://www.isc2.org/Articles/Ransomware-Cybercrime-and-Cloud-Security

▶ BLOG POST

Six Steps to Protect Your Organization from Ransomware

This is just one of more than 35 blog posts devoted to ransomware on the (ISC)² blog. Be sure to read others posted during June's #ransomwareweek to learn the latest in attack techniques and new guidances.

https://blog.isc2.org/isc2_blog/2021/06/six-steps-to-protect-your-organization-from-ransomware-ransomwareweek.html

(ISC)² The Definitive Guide to Cybersecurity and Business Prosperity

The Definitive Guide for Cybersecurity and 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.

Smart technologies have enormous potential to improve both human life and the health of the planet. For example, satellite-based applications can aid rural farmers to irrigate their crops efficiently[4]. Prosthetics can be 3D printed. Autonomous vehicles can be employed by the elderly to support better mobility. The Internet of Things (IoT) can even help to lower CO2 emissions[5] by optimizing energy consumption and reducing traffic congestion.

However, many new challenges and risks have also surfaced. Cyberattacks have become a common hazard for individuals and businesses. The World Economic Forum Global Risks Report 2020[6] ranks them as the seventh most likely and eighth most impactful risk, and the second most concerning risk for doing business globally over the next 10 years.

The need for strong cybersecurity is apparent.

‘Verify, Then Trust’

Think twice before reaching out—and responding to—online connections

BY CATHERINE KOZAK

WITH JUST A ROUTINE INVITATION to connect on LinkedIn, Peter Warmka, a former senior intelligence officer with the U.S. Central Intelligence Agency, has an effective way to get across his point with cybersecurity professionals who attend his presentations.

Many of those trained skeptics he contacted ahead of time are quick to respond to his request to connect. Once they accept his invitation, he exchanges a few direct messages. “Then I send them out a message that has an attachment, and I ask them to take a look at the attachment and provide some feedback,” Warmka, the founder of Orlando-based Counterintelligence Institute, recounts in a recent telephone interview. In other words, he explains, the message was an appeal: Can you help me out?

ILLUSTRATION BY ENRICO VARRASSO

CONTENTS

A surprising number of cybersecurity professionals open the attachment, he says. But the message and its content are a fake sent by an avatar Warmka created from looking at attendees' accounts. Some respondents even ask the fake connection to resend to their personal email when the attachment won't open.

"I've had a number of people do that, including directors of security for major companies," he says.

Warmka, who is also the author of the nonfiction book *Confessions of a CIA Spy – The Art of Human Hacking*, isn't looking to embarrass anyone as much as to get them to acknowledge their own vulnerabilities—including connecting to people they don't know.

"A lot of people have this thing, like 'I would never do that.' Or 'I would never fall victim to that attack,' or 'No one's going to target me,'" he says. "But then when it happens, they realize 'Oh my gosh, it *can* happen.'"

On the heels of a recent string of massive and debilitating ransomware attacks, in addition to numerous huge data breaches, the cybersecurity industry lately has been looking inadequate—at best—under media klieg lights.

"We are racing toward—in fact have already entered—an era of visceral cyberattacks that threaten Americans' way of life," The New York Times declared in a piece published June 7.

Cybersecurity professionals are no babes in the dark digital woods, but the ubiquity and aggressive phishing through social networks can spear even the savviest IT specialist. The key is to be prepared. And wary.

> "So, your desire to be informed and to see information often overrides your gut instinct, which is telling you: 'Maybe I should slow down.'"
>
> —*Shelly Epps, security program director, Duke University Health System*

TESTING GULLIBILITY

Similar to Warmka's slap of reality, albeit with more buy-in from the recipients, Shelly Epps, the security program director for Duke University Health System, conducts a simulated phishing program that trains the organization's 40,000 email users to recognize and report suspected phishing attempts.

Participants are tested with simulated phishes, such as an email that says they've won a U.S. $20 gift card as part of their corporate engagement, Epps explains. If the receiver clicks on the underlying link, an in-time message appears informing them, 'This was a simulated phishing test.' Lesson learned, in a non-punitive (and safe) way.

But social networks are a different animal—one more difficult to control when the activity involves personal platforms accessed through corporate devices. By virtue of email and online networks' dynamism, Epps says security analysts and executives are also susceptible to targeted phishing attacks. All the more reason to take their own advice: apply software updates, stay up to date on the latest exploits, and think twice about current email and social network usage.

"What you really want to do is make sure that you're on guard, that you're evaluating and assessing the risks that are in front of you," she cautions. "Part of the reason phishing works is because many people trust when they see something that looks valid. It also works because people are insanely busy.

"So, your desire to be informed and to see information often overrides your gut instinct, which is telling you: 'Maybe I should slow down,'" she adds.

THE SAME RULES APPLY TO YOU, TOO

A return to basic, tried-and-true security hygiene is in order, says Tarik Saleh, a senior security engineer and researcher at Amazon. That includes keeping up with adversaries' newest tactics and techniques to impersonate and infiltrate.

"Even under the guise of [an interview] is an interaction that we as cybersecurity professionals have to factor into when we're doing our own risk analysis to protect ourselves,"

CONTENTS

Saleh says. "I mean, cybercriminals can definitely masquerade as legitimate sources, such as a reporter or a software vendor or even on LinkedIn as people who are hiring for jobs, like recruiters."

Saleh, a cybersecurity industry veteran, emphasized that he is not speaking as a representative of Amazon, where his charge includes malware and forensics, but from his years of experience navigating through the thicket of evolving threats.

Cybersecurity professionals need to do their own individual threat modeling, he says. Look with a cool eye at your likelihood of getting attacked. Step back and consider the platforms you use, and the likelihood of data posted on those platforms being weaponized against you. Or your email account being hijacked. Consider all the risks and what they might look like.

"And then we build defenses against it," Saleh says. "That's all we're really doing here: applying what we (do) for the business world to ourselves."

> "Basically, the more helpful, the more community-bound you are, the more exposed you are. Cyber attackers don't go to one site and find one thing about you, and that's it."
>
> *—Lance Spitzner, director of research and community, SANS Institute*

CHECK YOUR OWN EXPOSURE

Part of building guardrails against cybercrime is determining your tolerance for risk and the benefits of being engaged online, says Lance Spitzner, director of research and community at the SANS Institute, a Maryland-based cybersecurity educational and training facility.

"It's a bit of a double-edged sword because if you're in cybersecurity, and you're wanting to contribute to the community, and help the community, you're going to be visible. You're going to have a social media presence," Spitzner explains. "You can take steps to limit it, but you're going to have a digital footprint. And cyber attackers, depending on how motivated they are, can pick up those pieces and put a puzzle together."

Short of going offline, risk will be a given. Even people who never touched a cellphone or a computer could have their hacked data—from toll booth cameras, from their doctor, from their bank—available on the dark web.

"There's no way you can eliminate it," he says of risk. "Basically, the more helpful, the more community-bound you are, the more exposed you are. Cyber attackers don't go to one site and find one thing about you, and that's it."

Take one of today's most popular social media apps: Facebook-owned Instagram.

Even if you set your account to private, if you accept a follower with a fake account or malicious intentions, they can gather valuable intel from what you post. For instance, they see you have a car. They deduce where you likely bought the car. They call the dealer pretending to be you and get information about when it was last fixed. And then they email you, pretending to be the dealer.

"It gets really complex really fast," Spitzner says. The less you post about yourself personally, the less exposed you are. That said, you can't control what other people post about you.

"The issue is not so much, 'Well, there's more data and there's more vulnerabilities,'" Spitzner says. "What's changed is the threats. In other words, cyber attackers, cybercriminals, have learned to make more money from incidents. You see an explosion in ransomware … [It's] almost like a feeding frenzy."

Then there's text messaging via phone or desktop apps like Slack, which has risen in popularity to reduce voice and email exchanges. These modern communications tools are also attractive to attackers targeting both young and older users, Epps says, adding that she is speaking from her years of experience, not as a representative of Duke Health.

"With everything that you do, you really want to be thinking about a layered, defense-in-depth posture," she says. In addition to awareness training, consider applying filters to flag malicious activity via email that quarantines suspicious mail. If malware does get through, have a mechanism to segment infected machines from the rest of the network to help stop the spread.

CONTENTS

"You're always going to get malware that hits computers on your systems," Epps says. "What you want to do is prevent the majority of it. And, for whatever does come through, make sure that the impact is minimized."

Epps' organization follows the basic framework for cyber technology established by the National Institute of Standards and Technology (NIST): identify, protect, detect, respond and recover.

"It's really important that security teams are doing all of these things concurrently and learning from what's happening," she says.

Password management and outdated software have proven to be two of the more persistent human-caused failings that contribute to cyber vulnerabilities. The recent Colonial Pipeline breach, for instance, was caused, in part, by the lack of multi-factor authentication that allowed ransomware to infect the energy company's networks and halt production.

"Managing passwords is really difficult, even for individuals," Saleh says. "It's extremely difficult when you have, like, 10 different systems and you're supposed to have these unique, crazy, complex passwords for each one, but you're not supposed to write it down. You know, this is a hard problem to solve, and a lot of companies are trying to figure it out as well and a lot of companies are making mistakes along the way."

Then there's the perennial problem with applying updates and security patches in a timely fashion, he says. Sometimes it's because the company doesn't have the resources, whether equipment, money or staff. Sometimes it's just too risky to rush into it.

"There are certain systems out there that companies may have where if you apply that software update, you could break their entire platform or their entire application," Saleh says. "That's how fragile things can be. So, adversaries and bad actors take advantage of the weaknesses and bad processes and lack of patching available. And they capitalize on it, based on whatever their motivations are."

> **"There are certain systems out there that companies may have where if you apply that software update, you could break their entire platform or their entire application. That's how fragile things can be."**
>
> *—Tarik Saleh, senior security engineer and researcher, Amazon*

'VERIFY, THEN TRUST'

It's important to understand what makes an attractive target, Warmka says. Who are you working for? How might a threat actor utilize you to gain access to the ultimate target? What do you care about and identify with?

Cybercriminals want to know "what makes you tick as a person," he says. "It's not you reaching out to somebody who might be nefarious; it's when somebody who is potentially nefarious reaches out to you."

Not only is it easy to fake a profile photograph, Warmka says, it is also easy to fake professional credentials.

He recently discovered that a supposed security professional who wanted to connect claimed to have CPP and CFE credentials. He checked by contacting the credential issuer, and the person had neither. (He also always does an online reverse photo search to see where else they've been posted.)

To stay safe, he says, flip the famous Russian proverb, "trust, then verify," to "verify, then trust."

"It doesn't sound nice, but I refer to the threat actors basically as wolves—they're out there trying to catch the lamb for their meal," Warmka says. "And we're not going to defeat the wolves.

"The wolves are always going to be there," he adds. "All we can do is harden ourselves as a target, whether we're an individual or a company, so that that wolf will move on to a lamb that's more vulnerable." ●

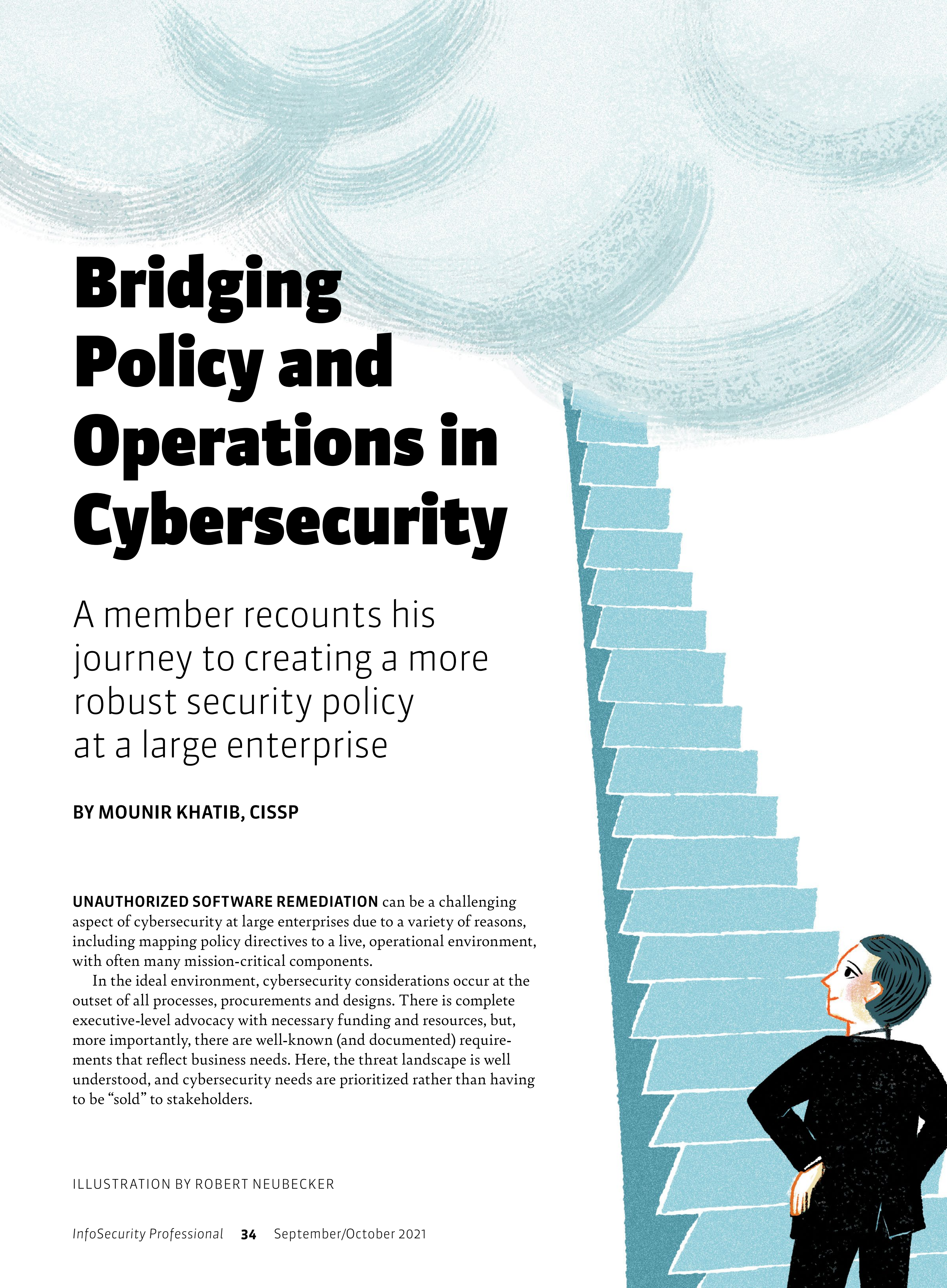
Catherine Kozak is a past contributor to *InfoSecurity Professional* magazine who lives and works on North Carolina's Outer Banks.

CONTENTS

Bridging Policy and Operations in Cybersecurity

A member recounts his journey to creating a more robust security policy at a large enterprise

BY MOUNIR KHATIB, CISSP



UNAUTHORIZED SOFTWARE REMEDIATION can be a challenging aspect of cybersecurity at large enterprises due to a variety of reasons, including mapping policy directives to a live, operational environment, with often many mission-critical components.

In the ideal environment, cybersecurity considerations occur at the outset of all processes, procurements and designs. There is complete executive-level advocacy with necessary funding and resources, but, more importantly, there are well-known (and documented) requirements that reflect business needs. Here, the threat landscape is well understood, and cybersecurity needs are prioritized rather than having to be "sold" to stakeholders.

ILLUSTRATION BY ROBERT NEUBECKER

Most environments, one can venture, are less than ideal and have room for improvement, especially large enterprises with their associated inertia and complexity. Environments are often described as "organic" (where top-down planning wasn't possible due to a variety of reasons) and "distributed" (aiming to provide security solutions as disparate needs and priorities arise).

From experiential evidence, many of these large environments recommend security as "baked in" (included in initial requirements) and decry "bolted on" (added after the fact, often to meet regulatory requirements or emerging threats). However, the result is usually a mishmash of bolted-on with a sprinkling of baked-in, sometimes leading to redundancy. This is partly due to deliberate enterprise security design and heavily influenced by vendors working diligently to outcompete each other with increasing vertical alignment.

Because of these often bottom-up approaches, multiple systems provide some of the necessary data; however, they do not all represent the information in a substantially similar fashion. These overlapping systems are unlikely designed to cross-communicate, harmonize and deduplicate in a straightforward manner across vendors, understandably; more surprisingly, this is often an issue even with products from the same vendor.

UNAUTHORIZED SOFTWARE REMEDIATION AND DATA HARMONIZATION

This is the stage for this discussion—a large, organic, distributed enterprise with bolted-on security. More specifically, the focus is unauthorized software remediation, which involves identifying software that is not on the approval list or that has been identified as having significant vulnerabilities through standard endpoint scanning.

A significant component of operationalizing security policy is establishing a bidirectional translation between what policy dictates—in this case, approvals or denials—and what the environment captures. This translation activity, and subsequent capture for data harmonization, drives the main operationalization of policy.

In this example, there are multiple techniques to remediate unauthorized software, some automated scripting and some manual technician/administrator-driven. However, the primary issue is what is fed into these downstream removal processes. This is where the translation is critical. What leadership says to remove from the environment (policy) only matches what is in the environment through this example of data normalization.

In Figure 1 *(see p. 36)*, the outlined notional process consists of inputs, processing and outputs. Let's dig into each component to show their importance to optimal outcomes.

Inputs

First, a reference policy (approve/deny) and system management data are needed, which could be from a variety of vendors such as HCL, Microsoft and VMware, or custom-developed, in-house utilities. The policy's approval or denial lists are flattened into an easily digested structure, such as a spreadsheet file containing information related to the software title, version number and current (and former) approval status. System management data is complex and should be stored in a relational database to facilitate correlation and archiving.

Another primary course of data input is a security authorization repository, essentially a GRC toolset that can be a suite of tools or a document tree in a content management system like SharePoint.

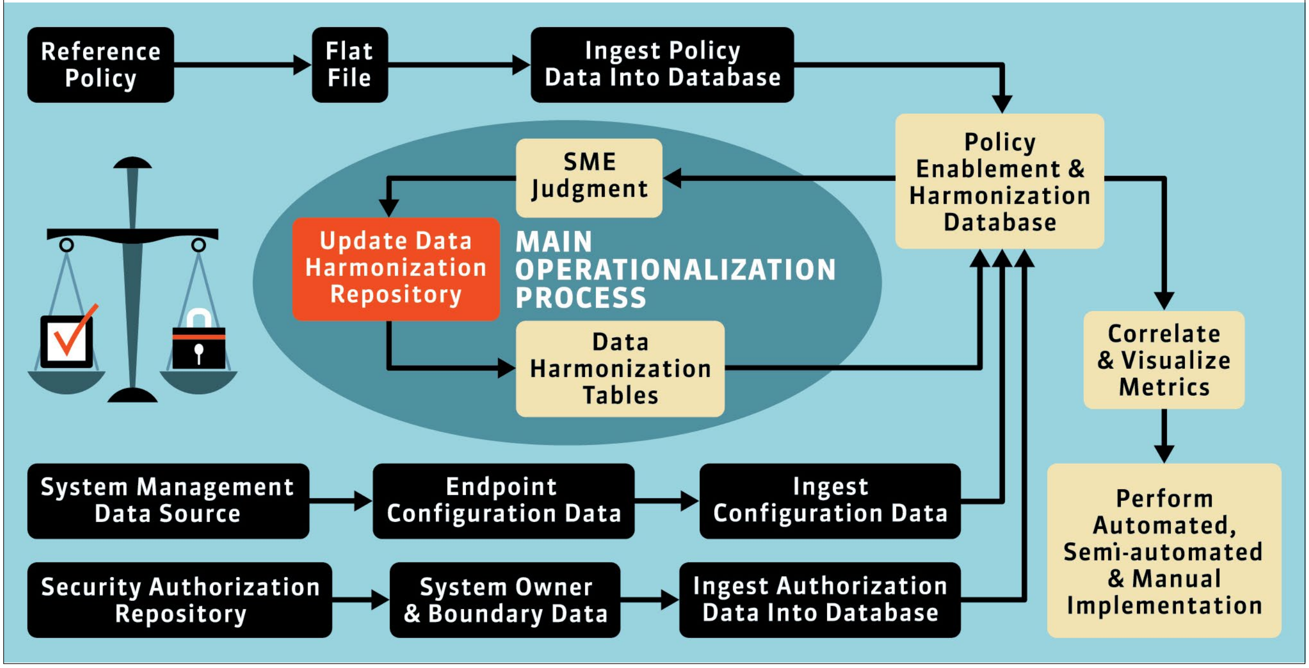
From here, a daily journal of changes power reports showing progress toward remediation. The security authorization repository is also complex and stored in a relational database. It mainly serves to provide ownership information and also exception status through POAMs (Plan of Action and Milestones), which allow for temporary deviations from policy due to perceived business needs or constraints.

Processing

Here is where things get interesting. For the sake of this case study, it is assumed there is no harmonization between the three aforementioned input categories. There might be one or more sources of each category, suggesting possible duplicates or overlap.

FIGURE 1 –
RECONCILING POLICY DECISIONS WITH ENTERPRISE CYBERSECURITY DATA

Translating executive policy into operational tools requires a significant investment of energy in finding, correlating, deduplicating, judging and storing information. This diagram depicts the ingestion of data from multiple sources, including policy decisions. It then provides correlations to determine the state of the environment with respect to that policy, given the system management and security information that is available. The output is primarily used for remediation, creating a (hopefully) downward trending metric in policy-to-environment variance.


Reference Policy
Flat File
Ingest Policy Data Into Database
Policy Enablement & Harmonization Database
SME Judgment
Update Data Harmonization Repository
MAIN OPERATIONALIZATION PROCESS
Data Harmonization Tables
Correlate & Visualize Metrics
System Management Data Source
Endpoint Configuration Data
Ingest Configuration Data
Security Authorization Repository
System Owner & Boundary Data
Ingest Authorization Data Into Database
Perform Automated, Semi-automated & Manual Implementation

Infographic by Robert Pizzo

This seems extraordinary (or insurmountable), but it isn't uncommon in a large, organic, diverse environment that utilizes multiple vendors and tools to accomplish its security goals. There are statistical approaches that can be used—fuzzy lookups, artificial intelligence/machine learning, etc.

While one (or more) of these might be an elegant and potentially more automated way of harmonizing data, even minor errors can be catastrophic to operations in a mission-critical environment.

Moreover, statistical techniques require significant upfront verification prior to utilization, again to ensure that operations are not disturbed. In this case study, the environment is live and cannot, for any deterministic reason, have operational disruptions.

This is where subject matter expertise (human judgment) plays an essential role. All of the ingestion, processing and outputs in Figure 1 can be automated, except for the one place where SME judgment drives a manually generated table that maps every variation of some software title and version information across every data source to the reference policy.

Think of this setup as a Rosetta Stone (the ancient granite slab, not language learning software) of sorts. It seems like a monumental task, and it is, at least in the beginning. The initial seeding of the data is the most intensive part. However, once the harmonized information is captured, the maintenance of those harmonization tables is a small fraction of the initial effort. And, since a human is incorporated, significant research and risk analysis can be conducted at each entry point, moving away from a simple match to providing an enterprise risk-aware approach. This is the key component of this example of operationalization—a brute force approach. Sometimes it is necessary to work harder and smarter.

Outputs

Extending the metaphor, the main output is the Rosetta Stone database that maps all data sources to

FIGURE 2 – **CLOSING IN ON THOSE GAPS**

In order to fully operationalize policy, you must know where there are gaps in process, people, products and policies. The following table provides samples from which to build your own analysis.

BEFORE	AFTER
Remediation targets were selected arbitrarily.	Remediation targets are selected by prioritizing quantity and risk.
Implementing policy changes for unauthorized software was long-horizon (weeks, months).	Implementing policy changes for unauthorized software occurs in real time.
Remediation progress was anecdotally captured.	Remediation progress is captured daily.
Remediation “leftovers” were indeterministic.	Remediation “leftovers” can be identified and updated daily.

each other. Statistical matching can now be applied between policy (approve/deny lists) against the collected enterprise data that always results in a 100% match. Anything less generates a feedback loop requiring the subject matter expert to examine the seed data or subsequent delta until everything aligns again.

Other captured data includes daily changes in installations reported by system management tools, which are used to drive dashboards to keep executives informed with remediation progress. This is a great way to show return on investment.

Additionally, the Rosetta Stone data can be utilized by other stakeholders for a variety of data service needs. This way, the enterprise only has to complete this one (relatively small) manual effort that can be reused. The clients of the data can report any discrepancies, which can help move matching back to 100% through the feedback loop.

Results

In the standard engineering approach, a gap analysis is necessary to fully operationalize policy. Figure 2 *(above)* provides a sample of “before” and “after” states.

The environmental security posture, as related to unauthorized software, improves significantly as more data is seeded and maintained in the Rosetta Stone database.

Discussion

No project, let alone one on this scale, is performed in isolation. That is why there needs to be a discussion detailing this approach and anticipated outcomes, so all stakeholders understand how this approach relates to other technologies and existing policies.

Many data normalization platforms exist today, and it is advisable to conduct context-specific research. A chosen platform should meet specific business needs to gather and deduplicate quality datasets. Artificial intelligence or machine learning applications might benefit some enterprises. Only individuals know what will work best in their respective environments and whom to assign a task no technology can address.

While one is always looking for the most advanced techniques and tools to defend against the ever-expanding onslaught of attacks and exploits, the human element (usually related to inadequate training leading to adverse outcomes, à la phishing) must be considered. In this case, that element’s expert judgment provides a solid foundation gluing together an organic enterprise’s data to operationalize policy that markedly improves the security posture. ●

Mounir Khatib, CISSP, PE, PMP, Security+, Network+, MCSE, is a cybersecurity engineer who for almost 20 years has provided strategic and tactical consulting services to commercial and government enterprises.

This article was prepared by the author in their personal capacities. The views and opinions expressed in this article are those of the author and do not necessarily reflect the official policy, opinion or position of their employer.

WINNING MORE BATTLES WITH FREEWARE

Frameworks that will keep you from abandoning threat modeling

BY KUMAR SETTY, CISSP, HCISPP

IN 216 BCE, the Battle of Cannae was fought in southeast Italy between Carthaginian forces under the general Hannibal Barca and Roman legions led by generals Lucius Paulus and Gaius Varro.

After Rome won the First Punic War, it became the dominant naval power in the Mediterranean Sea. Rome colonized Iberia to mine its silver, further enriching the Republic. Hannibal, as he would be known, understood Roman strategy and decided to take the fight to the heart of the Roman Republic, beginning with an invasion of Iberia.

There he procured silver, supplies and food and used these provisions to cross the Alps into Italy with his army and war elephants. After winning some decisive battles, Hannibal marched through to southern Italy, where he used his silver to convince Greek and Italian vassals of Rome to join his army. He then encamped at Cannae.

ILLUSTRATION BY JEFF MANGIAT

CONTENTS

He chose Cannae because it was the center of farming and grain production for the Roman heartland. Hannibal specifically chose a region in Cannae near the area's only water source. This applied tremendous pressure on the Roman legions, which found themselves outflanked.

Hannibal's troops beat a formidable foe (at least for now; Rome would eventually annex Carthage following another drawn-out campaign). Rome lost the Battle of Cannae because it underestimated its adversary. The Romans never imagined an army would cross the Alps from North Africa (audacious move) with elephants (unique attacker tools). Nor did they anticipate what to defend (Iberia, the Alps and southern Italy) and where they would be attacked (from the sole source of water in Cannae).

Unlike any adversary the Roman Republic had ever encountered, Hannibal understood his own capabilities and Rome's. He wisely utilized his assets. He knew Roman strategy and battle formations. He understood Rome's weaknesses and who might be willing to betray Rome. He employed assets to gather intelligence prior to engaging Rome in battle.

In other words, Hannibal found the right attack surfaces through his own version of threat modeling.

A security professional needs the ability to "predict" the future—future threats, future attacks, and future frauds and enablers.

WHAT IS THREAT MODELING, REALLY?

Many times, when organizations discuss threats and risks, they focus on recent or historical events without considering new risks and attacks. They fail to think like an attacker.

Threat modeling is a process through which cybersecurity professionals identify threats and vulnerabilities, quantify the likelihood and impact, and then formulate techniques to mitigate attacks to protect an organization.

There is no canonical process for building a threat model. The sheer number of attack surfaces, changing technology, vulnerabilities, dynamic risk profiles and attacker combinations obviate this possibility. It is not possible to build a crystal ball that can perfectly anticipate all threats. However, building a threat model should be systematic and structured. This is important because in order to continuously improve and refine a threat model, another team or professional should be able to understand the inputs and rationale behind the original model.

And it shouldn't break the bank.

A PROCESS TO HELP PREDICT THREATS

In providing security consulting for several organizations, I often encounter a common deficiency in the risk analysis and planning process: abandonment of useful tools to foresee, model, and appropriately and proactively respond to potential threats.

The issue often boils down to information overload coupled with time constraints. There simply are too many tools and methodologies available, and not enough time for proper selection. Security professionals do not know where to begin; so, they skip this arduous-but-important process.

Through my own research and experience, I built and implemented a sustainable threat modeling process for new or established organizations.

A security professional needs the ability to "predict" the future—future threats, future attacks, and future frauds and enablers. I put "predict" in quotes because it's impossible to forecast the future with certainty, but with the right tools and methodologies we can at least ask the right questions to clarify thoughts and guide strategic plans.

This ability to accurately anticipate the future also enables more prudent spending of limited resources. There are plenty of tools used for active monitoring, detection and response. But which work best?

CONTENTS

ASK AROUND AS PART OF INTELLIGENCE GATHERING

If we want the organization to be able to proactively counter a novel threat, then it's a good idea to gather intelligence about the entire organization. A completely siloed approach simply will not work.

One of the first steps in establishing a threat model is knowing where an organization may be most vulnerable by gathering information from those on the front lines. Such information-gathering should use formats that foster candidness and accommodate different preferences, communication styles and personalities.

Sometimes people volunteer more information and unique insights when they fill out a survey.

Others benefit from group discussions and interviews that provide a forum for airing ideas and, yes, grievances with past efforts. Additionally, these discussions may corroborate any information provided from separate individuals.

Based on my own experiences, I developed a table with starting points for quickly developing an elementary threat model. (See *Seeking Suggestions: Creating an Initial Threat Model from Feedback*, p. 42.)

It is not as important to generate copious paperwork as it is to understand the organization's posture, threats and countermeasures. You may not account for all the threats and countermeasures, but at least you have documented your understanding and you might identify any knowledge gaps. In essence, you will know what you don't know.

SELECTING A METHODOLOGY

The structured approaches for threat modeling are frameworks or methodologies (both interchangeable terms) that constitute a veritable alphabet soup of acronyms and special lingo. Some will be familiar; others may not. Here is a rundown of the main frameworks and what they entail:

NIST Threat Modeling Methodology

The U.S. National Institute of Standards and Technology (NIST) has its own data-centric threat modeling methodology, which consists of four steps:

1. Identify and characterize the system and data of interest.
2. Identify and select the attack vectors to be included in the model.
3. Validate the security controls for mitigating the attack vectors.
4. Evaluate the threat model.

If you are looking for a great example of how to apply a threat modeling methodology in practice, this is a good resource.

OCTAVE

OCTAVE, which stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation, is a threat modeling methodology developed at Carnegie Mellon University. It focuses on organizational rather than technological risks and consists of three phases:

1. Build asset-based threat profiles.
2. Identify infrastructure vulnerability.
3. Develop a security strategy and plans.

PASTA

PASTA, or Process for Attack Simulation and Threat Analysis, is a seven-step process focused on aligning technical security requirements with business objectives. Each step is fairly involved. The overall sequence is as follows:

CONTENTS

1. Defined objectives
2. Defined technical scope
3. Application decomposition
4. Threat analysis
5. Vulnerability and weaknesses analysis
6. Attack modeling
7. Risk and impact analysis

STRIDE

STRIDE was developed at Microsoft in the 1990s and popularized by developers and project managers. STRIDE emphasizes the six categories of threats that violate one of the properties of the CIA triad (confidentiality, integrity, availability):

1. Spoofing identity: An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.
2. Tampering with data: Data tampering involves the malicious modification of data.
3. Repudiation: Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise. Nonrepudiation refers to the ability of a system to counter repudiation threats.
4. Information disclosure: Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it.
5. Denial of service: Denial of service (DoS) attacks deny service to valid users.
6. Elevation of privilege: In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.

DREAD

DREAD was created as a supplement to the STRIDE methodology that enables analysts to rank threats once they have been identified. DREAD is an acronym for the five questions asked regarding each potential threat:

1. Damage potential: How great is the damage if the vulnerability is exploited?
2. Reproducibility: How easy is it to reproduce the attack?
3. Exploitability: How easy is it to launch an attack?
4. Affected users: As a rough percentage, how many users are affected?
5. Discoverability: How easy is it to find the vulnerability?

MITRE ATT&CK

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations from cybersecurity professionals. This framework is constantly being updated and there are variations that can be "spun off," which concentrate on a specific area, such as cloud computing or mobile security.

Version 9 was just recently released. The ATT&CK framework is an excellent resource for understanding attacker techniques and it is a great starting point for integrating common attacks into a threat model. There are also many resources available to get started on using this methodology.

If you are a visual person, the Enterprise Matrix is an excellent tool for understanding the different stages of attacks from reconnaissance to exfiltration to impact and all the techniques and sub-techniques within each attack category. *(To learn more on this framework, read our feature "Under Att&ck.")*

TABLE 1 – SEEKING SUGGESTIONS: CREATING AN INITIAL THREAT MODEL FROM FEEDBACK

Here are some questions you can pose to stakeholders to determine the biggest threats posed by and toward your organization.

QUESTION	TASKS	OUTPUT(S)
#1. **Know yourself.** What are you trying to protect?	1. Identify the overall system boundary and identify the flow of information into and out of these boundaries. 2. Enumerate the physical, logical assets—servers, databases and other components. 3. Identify any intangible assets that are critical to the business.	1. Data Flow Diagram. 2. Asset List. 3. Surveys sent to individual stakeholders. 4. Notes from group sessions.
#2. **Know your enemy, know your friends.** Who are the attackers (internal and external)?	1. Identify potential threat actors, threats, and attack scenarios. 2. Brainstorm motivations of an attacker through cooperation with different teams and groups. 3. Identify business risks and results of other assessments such as a fraud risk assessment. 4. Who wants to steal or damage the assets? 5. Who are you most concerned about?	1. Adversary Model – resources, access, risk tolerance and objectives. 2. Attack scenarios or “abuse cases.” 3. Surveys sent to individual stakeholders. 4. Notes from group sessions.
#3. **Know your enemy, know your friends, know yourself.** What type of attack surfaces are present? Where will the organization be attacked?	1. Identify the methods, tools, where an attacker or other systems interact with the system. 2. Identify all the third-party integrations and dependencies.	1. Vulnerability Model – Using the Adversary Model above as an input, map vulnerabilities. 2. Interface or integration diagram – high-level and low-level. 3. Surveys sent to individual stakeholders. 4. Notes from group sessions.
#4. **Know it all.** What are the risks, controls, likelihood and impact? Countermeasures?	1. Using an established framework such as NIST, identify risks, controls, and calculate likelihood and impact. 2. Calculate total risk exposure by multiplying likelihood and impact. 3. Above a certain threshold for risk exposure, maybe High and Critical, document exploits. 4. Generate corresponding countermeasures for each High and Critical risk exposure.	1. NIST matrix with risks, controls, likelihoods, impact, calculated risk exposure and detailed countermeasures.

NO ONE FRAMEWORK FITS ALL

It is important to understand that there is not one, all-encompassing methodology that will apply to any business or situation. If there was, we'd all be using it.

Instead, there are many similarities among the different frameworks I've outlined. And you can use more than one to build a strong threat modeling program.

I recommend first understanding the organization, studying previous assessments, and confirming what you want to secure. I would then use the OCTAVE methodology since it has a more organizational emphasis. OCTAVE has comprehensive information for developing surveys that can be sent to individuals for completion.

I also highly recommend that you obtain an understanding of the business risks and fraud risks. These insights should flow into your customized Adversary Model.

I next suggest the NIST threat modeling framework and, from there, integrate the attacker techniques from the MITRE ATT&CK framework to complete the Adversary Model.

In the final stage, the overall model should include comprehensive risk ratings and specific countermeasures. Finally, always remember that your threat model should be a living document and should be revisited and edited on a frequent basis to accommodate changes to the organization's risk profile. ●

> I recommend first understanding the organization, studying previous assessments, and confirming what you want to secure.

Kumar Setty, CISSP, HCISPP, CISA, CCSK, ITIL, is a principal at Zakti Security Labs.

Center Launches Two New Children's Safety Programs

BY PAT CRAVEN, DIRECTOR

IF YOU'VE FOLLOWED the Center for Cyber Safety and Education for a while, you might be surprised to learn that we've not introduced any new educational programs in *five years*. In 2015 we launched the Safe and Secure Online presentation for senior citizens, and in 2016 we rolled out the first of three Garfield's Cyber Safety Adventures programs for elementary-school-aged children. Those were our last "new" programs.

Now that doesn't mean we've been just sitting around; in fact, just the opposite. The parents, senior citizen and youth (ages 11 to 14) Safe and Secure Online programs have been regularly updated and are now available in more than 20 languages. There are now three Garfield-led lessons on privacy, safe posting and cyberbullying—and they will soon be available in Spanish. Over the last five years, we have refined and built our audience and our delivery methods. Just six years ago, the Center and our volunteers provided some 10,000 cyber safety lessons a year. Now we're approaching 150,000 annually!

Demand for quality information on staying safe online continues to skyrocket, and it's time to start producing new educational programs. So we're excited to announce the official launch of Safe and Secure Online Gaming – Parents' Edition and VITA Unplugged. Both programs are available on our website for volunteers to download and use for in-person or virtual presentations.

They're designed to be completed in a group setting in 60 minutes.

Safe and Secure Online Gaming – Parents' Edition was created with the assistance and guidance of (ISC)² members and UKnightedXP, Inc., a gamer-led nonprofit working to advance gaming, education and philanthropy. This new educational program helps parents understand the mysterious gaming realm their children live in and provides practical tips to help keep them safe and secure when visiting these other worlds.

VITA Unplugged (Life Unplugged) was originally designed for secondary and high school students, but adults will enjoy it as well. The goal is for participants to examine the amount of time they spend online, on all devices, and take steps to reduce screen time. The less time they spend online, the safer (and more productive) they will be. If users recapture just one hour a day of screen time, that adds up to 365 hours a year—about 15 days—formerly wasted with endless scrolling. Imagine what any of us could do with an extra two weeks added to our year!

These two new programs are just the beginning. Sign up now for updates on all our programs at https://www.IAmCyberSafe.org/s/, and volunteer to help make it a safer cyber world for everyone. ●

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

Photograph by Getty Images

CENTER FOR
CYBER SAFETY
AND EDUCATION™

PROTECT YOUR COMMUNITY'S CHILDREN WITH GARFIELD

HOST A CYBER SAFETY DAY IN YOUR COMMUNITY.

Cyber Safety Days increase children's knowledge of online safety by 36 percent!

Bring together schools, businesses, parents and media to help your kids learn to be safe online with our award-winning Garfield's Cyber Safety Adventures.

Get involved in the future!

THE DAYS OF FLIP PHONES ARE OVER.

Most children have a smartphone by the time they're 10 years old.

40 percent of elementary school children have connected online with a stranger, and **11 percent of those children met that stranger.**

BRING CYBER SAFETY DAYS TO YOUR COMMUNITY TODAY!

For more information, contact us at Center@isc2.org or www.IAmCyberSafe.org/Cyber-Safety-Days

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

When you have a compromised cloud account due to one of these types of misconfigurations, it is almost always much worse than a compromised cloud host."

—Matthew Chiodi, CSO, Public Cloud, Palo Alto Networks

Source: (ISC)²'s *Cloud Security Insights*, "What Lurks Beyond Leaky Storage Buckets and Reduced Visibility"

"Cybersecurity is a team sport. If you think that you can protect yourself alone in this day and age when you have nation-state actors who have an unlimited amount of individuals and dollars they can throw out there to find the one vulnerability in your network, it's probably an unlikely circumstance that you can survive everything they can throw at you. Make those partnerships upfront."

—Spencer Wilcox, CISSP, SSCP, CPP, CISA, CSO and Executive Director of Technology, PNM Resources

Source: (ISC)² webinar, "Working with Law Enforcement and the FBI"

"A good IR [incident response] person is exactly this: They are a quarterback. [They] call the plays and trigger the execution."

—Bryan Sartin, SVP, Chief Services Officer, eSentire

Source: (ISC)² webinar, "Become Cyber Resilient – The Next Generation of Cyber Investigations & IR"

"Plan the cloud migration in phases ... embedding security controls right from the design stage and evaluating the migration strategy on an ongoing basis."

—Minghui Wu, CISSP, CCSP, Technology Audit Manager, Singapore

Source: (ISC)²'s ebook, "20 Tips for Secure Cloud Migration"

"Never underestimate the patience of cybercriminals when trying to send you their exploits. Eventually they'll ask you that critical question, send you a link or send you a file attachment. So, you must be closely attuned to that sort of activity."

—Ryan Witt, Managing Director, Healthcare Industry Practice, Proofpoint

Source: (ISC)² Think Tank webinar, "In the Bullseye: Healthcare and Email Threat Vectors"

"In our recent member engagement, we asked software engineers what the most common causes of software project failures were; 91% of respondents stated that 'a lack of testing to discover bugs and security gaps' was responsible for problems they witnessed, and 30% said that 'poor overall project management' was to blame."

Source: (ISC)²'s white paper, "The Confessions of a Software Developer"

CONTENTS