

(ISC)² CEO CLAR ROSSO: DRIVING INNOVATION AND OPPORTUNITY

InfoSecurity PROFESSIONAL

JANUARY/FEBRUARY 2021

SPECIAL
WORK
ISSUE

The Future of Work

+

The Evolving Home Office

Boosting Employee Morale from a Distance



(ISC)²[®]

A Publication for the (ISC)² Membership



Certified Information
Systems Security Professional

An (ISC)² Certification

STRONG

Stronger Cybersecurity Starts with CISSP

Those at the forefront of cybersecurity know people play the most vital role in keeping the organization safe. The surest path to stronger cybersecurity starts with a team that is trained and certified. CISSP certification arms every team member with the expertise to design, engineer, implement and run a premier information security program.

Download The Definitive Guide for Cybersecurity and Business Prosperity

to explore the expanding threat landscape and how cybersecurity can drive business growth with expert resources in place. Discover what hiring managers can do to strengthen the team and foster success, including:

- Advocating for Cybersecurity Strategy
- Promoting Internal Partnerships
- Championing Corporate Team Training and Awareness
- Promoting Professional Certification
- And More!

[Download the White Paper](#)





**SPECIAL
WORK
ISSUE**

There are numerous ways to foster a better work-life integration, both now and going forward.

PAGE 28

FEATURES

19 The Future of Work

BY ASTRID HARDERS

Promoting cybersecurity best practices under less-than-ideal conditions will continue to be a priority for security operations.

24 The Evolving Home Office

BY ANNE SAITA

Your employees are on the move now, whether by choice or circumstance. (ISC)² members offer practical advice for keeping the company secure during these [still] unsafe times.

28 From Bummer to Bumper

BY MICHAEL HANNA, CISSP; RYANN HANNA;
BOB DUHAINY

You can produce a flourishing garden of happily motivated team members. First, though, you need to stop pushing for work-life balance.

Cover illustration
by John Jay Cabuay

Illustration (above)
by Enrico Varrasso



DEPARTMENTS

5 Editor's Note

Let's make it work.

BY ANNE SAITA

8 Executive Letter

Bringing more value to an (ISC)² membership.

BY CLAR ROSSO, CEO

10 Field Notes

The global workforce gap is shrinking; Tony Vizza predicts what will happen by 2050; LATAM chapters hold first virtual summit; 'How I Got Here' with Yves Le Roux; a good read on pen testing; and more.

16 Help Wanted

Sometimes the best move is to hire a "butterfly" over a "genius."

BY DEBORAH JOHNSON

33 Center Points


Striving to stretch cyber education to millions by 2025.

BY PAT CRAVEN

34 Buzzworthy

A roundup of what's being said and heard around (ISC)² channels.

7 ADVERTISER INDEX



*You Can
Train Like
This...*

or with
(ISC)² Official
Training Providers
**You Can Train
Like This!**

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

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

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



CISSP[®]



CCSP[®]

(ISC)²[®]

TRAINING
OFFICIAL PROVIDER

EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

How This Is Going to Work

AS I COMPOSE THIS COLUMN, my husband is fielding Tier 2 tech support calls from the dining room while I'm holed up in my home office half-listening to a Zoom class. I need to decide if I'll make it through an upcoming Teams call without Jack Hartmann interrupting. The musical artist is a staple of our child's daily special education program, and Hartmann's earworm-friendly tunes and class singalongs have prompted previous mute requests. I could just go into another room, but last time I did that, the school's Chromebook "mysteriously" stopped functioning. (If you're a longtime reader, you may recall [this kid is really, really hard on electronics](#).)

While I weigh options, my adult daughter texts to ask if I can watch her 13-month-old this afternoon while she conducts telehealth appointments with her pediatric patients. Our grandson was sent home from child care due to a runny nose and now is out for the remainder of the week, per COVID policy. Her husband, believing they had everything covered, booked back-to-back virtual meetings to meet an important deadline for which paychecks are on the line.

Seven months into this, our work-home life is not that dissimilar from the fictitious family that opens Astrid Harders' cover story on the future of work. Really, it isn't the future. This work-home-school mega merger is the now. (ISC)² members might have figured out how to rapidly secure a remote workforce in the wake of the coronavirus outbreak, but that was just the warmup exercise. Your employees now live in other regions, states or countries. They are sharing devices out of necessity. Some now work from primitive campgrounds or fancy recreational vehicles where the internet connection is iffy. Others moved to more convenient or less expensive housing with better amenities, like free Wi-Fi(!). They don't see the risks with roaming or relocating like you and I do. They also may have responsibilities—young children, aging parents, struggling partners or unhealthy roommates—impacting productivity.

Don't know about you, but I no longer plan too far ahead. I just deal with the challenges currently before me and take measures to prevent others from emerging. It's really all we can do as we continue to curb COVID's spread. So, until I achieve the ideal work-life integration outlined in our third feature, I will do as Jack Hartmann instructs every weekday morning: "Have a good morning. Have a good day. Do your very best as we work and play." ●



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

Photograph by Louise Roup

CONTRIBUTORS



Astrid Harders is a trilingual journalist and editor. She was born in Colombia and is German. She covered a lot

of rock 'n' roll while working for *Rolling Stone*, became international editor for *SoHo*, a Latin American men's magazine, dove into breaking news with *Metro*, and produced app and digital content for Univisión, *The Root*, *Deadspin*, *Fusion*, *Gizmodo* and *Onion Labs*. After living in Bogotá, Boston, London and New York City, she now is a freelance writer in Miami. She sort of realizes that data protection isn't a hit conversation topic with her toddler and husband.

Regular readers will recognize **Mike Hanna's** byline as an (ISC)² member and doctoral candidate who's written about organizational leadership in past issues. This time he outlines ways to motivate a remote workforce with his wife, **Ryann Hanna**, an experienced industrial-organizational psychologist and human resources strategy expert, and Walden University professor **Bob Duhaity**. Ryann has an extensive background in leadership coaching, human capital and organizational development in technology, banking, entertainment, logistics, hospitality and retail. Bob currently serves as a chair and committee member for research involving blockchain, IoT, satellite, cloud, UAVs, and homeland and mobile security.



John Jay Cabuay is a New York City-based illustrator. His work has enhanced the covers of magazines and

book jackets worldwide, and now our cover depicting how today's households are working and learning. Cabuay was featured in the book *100 Illustrators* by Steven Heller and Julius Wiedemann, which showcases top influencers of the global illustration scene.

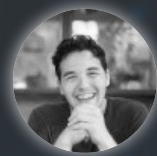




Join our industry experts for a roundtable discussion about their information security predictions for 2021

Highlights include

- ✓ Blurred lines of the cyber realm and the kinetic space
- ✓ COVID-19 vaccine-related fraud
- ✓ Impact of remote work on security
- ✓ Internet and its effect on our democracy
- ✓ Future of disinformation
- ✓ New normal for ransomware: double extortion
- ✓ Forced evolution of APTs due to public attribution



Chad Anderson
Senior Security Researcher



John "Turbo" Conwell
Principal Data Scientist



James Reynolds
Chief Technology Officer



Jackie Abrams
VP, Product

See what the future holds:
DomainTools.com/predictions

InfoSecurity PROFESSIONAL

A Publication for the (ISC)² Membership

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

isc2.org community.isc2.org **in** **🐦** **f**

READ. QUIZ. EARN.

Earn Two CPEs for Reading This Issue and Taking the Online Quiz

In order to earn the two CPEs 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/2021/Jan-Feb-Quiz>

[Learn about more opportunities to earn CPEs.](#)

ADVERTISER INDEX

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

(ISC) ² Definitive Guide for Cybersecurity and Business Prosperity	2	(ISC) ² -Sponsored COVID-19 Impact Report	17
(ISC) ² Value of Official Training	4	(ISC) ² InfoSecurity Professional	31
Domain Tools	6	Center for Cyber Safety & Education	32
IOR Analytics	9	(ISC) ² Professional Development Institute	35
(ISC) ² Community	14		

InfoSecurity Professional is produced by Twirling Tiger® Media, 7 Jeffrey Road, Franklin, MA 02038. 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

SENIOR MANAGER, CORPORATE COMMUNICATIONS

Jarred LeFebvre
727-316-8129
jlefebvre@isc2.org

CORPORATE PUBLIC RELATIONS MANAGER

Brian Alberti
617-510-1540
balberti@isc2.org

CORPORATE COMMUNICATIONS LEAD

Kaity Pursino
727-683-0146
kpursino@isc2.org

COMMUNICATIONS COORDINATOR

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

EDITORIAL ADVISORY BOARD

Brian Alberti, (ISC)²

Anita Bateman, U.S.

Felipe Castro, Latin America

Brandon Dunlap, U.S.

Rob Lee, EMEA

Jarred LeFebvre, (ISC)²

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.



2021: Driving Innovation and Opportunity

BY CLAR ROSSO, CEO, (ISC)²

On behalf of the (ISC)² Board of Directors and staff, I would like to wish you and your families a happy, healthy and prosperous new year.

Around the globe, people have ushered in 2021 filled with a mix of excitement about the possibilities, trepidation about the uncertainty and relief to have 2020 in our collective rear-view mirror.

I am a firm believer that challenge and uncertainty drives innovation and opportunity. At (ISC)² we are looking forward to an action-packed year that delivers value to you, our members, and encourages the growth and well-being of the cybersecurity industry, while delivering on our vision to inspire a safe and secure cyber world.

More specifically in 2021, our team and I are committed to tirelessly advocating for the advancement of our certifications. All around the world, (ISC)² certifications are recognized and well-respected among the cybersecurity community. They help validate your expertise and provide confidence to employers everywhere. We will continue to build on our certifications' unmatched reputations, as well as invest in the evolution of our exams, to ensure they remain relevant in this rapidly changing environment.

Next, we will be unwavering in our focus on member value. We're producing hundreds of hours of professional development opportunities, from our annual

Security Congress conference to our award-winning webinars, the Professional Development Institute, and this newly redesigned magazine you're reading now. You can get involved at any level that's right for you, from simply availing yourself of our member benefits, to participating in one of the (ISC)² Chapters we support. You have my commitment to continue to support your career and professional growth.

The third pillar is to grow our membership and the workforce. Attracting a broader and more diverse pool of candidates is critical to expanding our workforce. At (ISC)², every team member is focused on driving greater awareness of the career benefits and opportunities that exist in this industry, so that you get both the recognition you deserve in the workplace as well as the qualified colleagues you need beside you to deliver on our mission.

The cybersecurity industry is facing down unprecedented challenges as the interconnected nature of life continues to accelerate. Trends like the IoT, AI and 5G will increasingly make data protection more difficult and we'll need professionals like you to continue to innovate to ensure that security remains a core aspect of application development and data access.

There has never been a more critical time in our history to support and grow the cybersecurity profession. It's a huge part of why I joined (ISC)² last fall. I deeply appreciate the responsibility you accept daily to protect organizations and systems around the world. It's a great privilege to be part of growing the awareness of this important profession and communicating the opportunities that exist for those who want to be part of solving the challenges we face.

Again, I hope the year ahead brings you health, prosperity and a renewed perspective on what's truly important to you as we all work together to inspire a safe and secure cyber world. ●



Clar Rosso is CEO of (ISC)². She can be reached at rosso@isc2.org.

BETTER PRIVACY. LESS RISK.™



Identify and certify unregistered sensitive data usage
Eliminate hundreds of hours per year with automated analysis
Support data privacy compliance (i.e., CRPA, CCPA, GDPR, HITRUST)

Understanding your sensitive data flow is a requirement for privacy regulations and a prerequisite for managing data security risks.

IOR ATLAS automates data certification so that customers can streamline fact-finding efforts to understand business need, remove data no longer needed, and map the data they use for risk analysis and compliance reporting.

“
IOR enabled us to understand our sensitive data flows without a large team or long-term project. Now we have a solution to keep our data flow knowledge base up to date and automate risk analysis.
”

- Fortune 500 Customer

WWW.IORANALYTICS.COM

FIELD NOTES

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

NEWEST WORKFORCE STUDY SHOWS SKILLS GAP NARROWING BY MORE THAN 800,000

DESPITE ECONOMIC CHALLENGES tied to COVID-19, the latest (ISC)² Cybersecurity Workforce Study shows a first-ever decline in the global workforce gap: from 4 million to 3.12 million cybersecurity professionals needed to protect organizations from cyber threats.

This decrease, based on 3,790 surveyed cybersecurity respondents in the months following pandemic lockdowns and subsequent reopenings, comes while a majority (64%) reported some level of dedicated cybersecurity staff shortage at their own organization that left them vulnerable to cyberattacks.

As with the last workforce study survey, the Asia-Pacific region had the largest gap (2 million). Latin America came in next with a shortage of 527,000, followed by North America (376,000) and Europe (168,000). The annual global survey includes a wide variety of cybersecurity professionals representing small businesses to large enterprises, government agencies to educational institutions. The survey took place in April, May and June

2020—a time of both significant economic slowdowns and turmoil from securing entirely remote workforces.

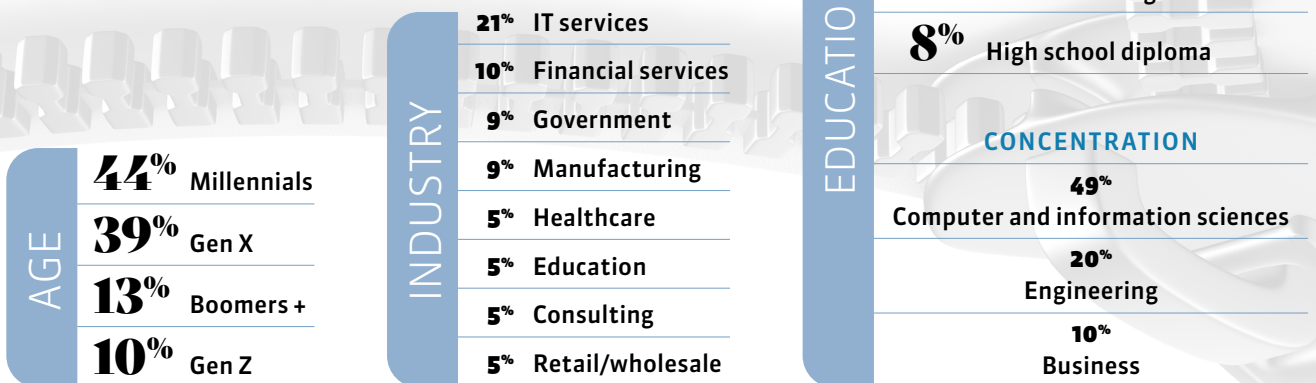
“One key objective of the study each year is to estimate the size of the global cybersecurity workforce. Another, just as vital, is to better understand the industry’s skills gap and uncover solutions for addressing the global talent shortage,” according to the authors of the report. “This includes ensuring career-long professional development for those already in the field, identifying pathways into the workforce for new entrants, and helping employers identify existing and future sources of fresh talent.”

What may account for the smaller workforce gap in 2020? Researchers believe it’s a combination of supply and demand. There are more qualified cybersecurity professionals entering the field at a time when demand dropped due to a severe slowdown in COVID-related business activity. That said, enterprises of 500 to 1,000 were more likely to expand their cybersecurity workforce last year.

To learn more, visit <https://www.isc2.org/Research/>.

The (ISC)² Cybersecurity Workforce Study at a Glance

Cybersecurity personnel represent a wide range of educational backgrounds and ages, working in a broad range of industries and organization types and sizes. Most of the 3,790 participants (72%) are male, and the largest age cohort are Millennials.





HOW I GOT HERE

FROM NETWORK SECURITY TO TECHNOLOGY STRATEGIST

Yves Le Roux, CISSP, CISM, recently received the (ISC)² Harold F. Tipton Lifetime Achievement Award and the (ISC)² CEO Award

INTERVIEWED BY DEBORAH JOHNSON

What were your biggest challenges as a new technology professional at the advent of the modern computing era?

Due to the lack of high-end computers needed for research projects at the University of Paris in 1967 and 1968, I was not only studying but also working at the French Power Utilities Research Center developing a network connecting the Control Data 6600 computer to Control Data 160A (with 96K of RAM) in two remote research centers. Consequently, I had to create the systems programs for the data exchange from scratch. I developed synchronization mechanisms transmission protocol and implemented error correcting code for integrity. It was successful, and the system went operational.

The internet's World Wide Web launched in 1991. How did that impact your work?

The World Wide Web opened the internet to everyone, not just scientists. In those early years, I spent a lot of time putting in place mechanisms for implementing a risk-dependent security system, involving security perimeters and risk-oriented policies.

What steps did you take during your long career to keep up with the changes?

To be part of the new technologies, it was most important for individuals to develop a network of specialists in the industry. In the beginning, information security specialists made up a small community, easily exchanging data about their findings.

How do those early issues compare to those that cybersecurity professionals now face?

I have seen the information security position evolve from scientists speaking only with other specialists to scientists communicating with non-specialists, even executives.

Today's security professionals have wide responsibilities. You must know the technology, but those early days of inventing the security from scratch are gone. Of course, there are always new security challenges. •



YVES LE ROUX

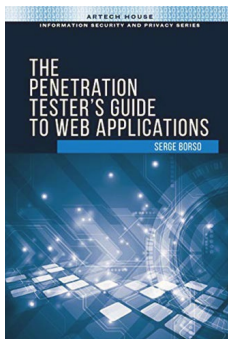
A 1970 graduate of the University of Paris, Le Roux started his career in network security at the Rothschild Group, a financial advisory company. He later joined the French Ministry of Industry, followed by Digital Equipment and Entrust Technologies. He then joined Computer Associates International as a technology strategist, retiring in 2017. He co-chairs the (ISC)² EMEA Advisory Council.

RECOMMENDED READING

Suggested by **LARRY MARKS**,
CISSP, CISA, CISM, CFE, PMP,
CRVPM, CRISC, CGEIT, ITIL

The Penetration Tester's Guide to Web Applications

BY SERGE BORSO
(Artech House, 2019)



In a straightforward approach, readers learn to bridge the gap between high-risk vulnerabilities and exploiting flaws to get shell access.

HERE IS A RESOURCE that provides both professionals and aspiring professionals with clear guidance on how to identify and exploit common web application vulnerabilities, focusing on offensive security. *The Penetration Tester's Guide to Web Applications* describes each of the Open Web Application Security Project (OWASP) top 10 vulnerabilities, including broken authentication, cross-site scripting and insecure deserialization, and details how to identify and exploit each weakness.

Based on author Serge Borso's many years of firsthand experience, his book provides examples of how to break into user accounts, how to breach systems, and how to configure and wield penetration testing tools—and he describes the step-by-step approach used by a penetration tester to attack an application. In a straightforward approach, readers learn to bridge the gap between high-risk

vulnerabilities and exploiting flaws to get shell access. Borso tackles the way to provide a best-of-class penetration testing service by demonstrating how to work in a professional services space to produce quality and thorough testing.

This resource does expect a high-level understanding of the OSI model, web development experience and experience with programming languages, and how to interpret vulnerabilities from a vulnerability management tool such as Qualys.

The Penetration Tester's Guide to Web Applications is not overly technical, is software agnostic and can benefit three sets of people: those new to pen testing, those researching the topic and those wanting to improve their techniques. ●

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

Committed to More Sensitive IT Terminology

In the last edition of *InfoSecurity Professional* magazine, a book review referred to white-box testing and black-box testing. One reader reached out to the editorial staff to remind us about the growing sensitivity of these and other commonly used terms, and their race-related origins.

We shared this with (ISC)² management and were pleased to learn about the association's plans to address this issue. (ISC)²

is already actively reviewing terminology during exam writing workshops, which are composed of members just like you.

We greatly appreciate the reader calling this to our attention. We are committed to adopting these terms and applaud the efforts to find alternatives that do not alienate any of our colleagues.

—Anne Saita, Editor-in-Chief

CHAPTER SPOTLIGHT

LATIN AMERICAN CHAPTERS HOST SUCCESSFUL SECURITY SUMMIT

Six chapters—Argentina, Chile, Costa Rica, Guatemala, Perú and São Paulo—combine efforts to stage CYBERSEC TALKS

BY FELIPE CASTRO, CISSP, PRESIDENT, (ISC)² CHILE CHAPTER

CYBERSEC TALKS 2020 took place live in mid-October, with 745 registrations hailing from 21 countries, including more than 100 visitors from countries without an (ISC)² chapter. We were excited to virtually welcome more than 170 simultaneous viewers at some point, more than at any of our previous events. There were issues, of course, such as losing a host in mid-sentence, open mic incidents, family on screen, or guests arriving late. However, by the time the dust settled, we remained on schedule throughout the entire program.

12 Hours, Two Days, Four Time Zones

Chapter members were split into four teams: content, technical, marketing and sponsors. We settled on a six-hour daily, two-day format targeting four time zones. The program would include eight sessions, three keynotes and two panels. We ran a Call for Papers to fill session slots; lined up our keynotes; and

reached out to our governments, (ISC)² headquarters and local universities for panel presentations—22 guests in total, plus nine hosts. Art, branding, website and broadcasts were centralized, with marketing and communications carried out by each chapter in whichever way was most effective locally. And to top it all, the week before the event, the then-incoming CEO of (ISC)², Clar Rosso, agreed to speak at the opening.

One of the major design considerations was the event being a showcase for individual chapters. Each chapter contributed experts, hosts and official logos that were featured during each chapter-sponsored session. We wanted local members to find their own flag on our shoulder patches, if you will, and feel that this was their own event, just bigger.

Some Challenges

The three greatest challenges we encountered revolved around time, capability and team-building. Our volunteers' day jobs sometimes

CEO Clar Rosso helped open the first virtual (ISC)² cyber-security summit in Latin America, which featured video chats with fellow members and sessions with regional cybersecurity leaders.



justly interfered with timelines, hurting event promotion. That loss, however, was offset by improved visibility from holding the event during Cybersecurity Awareness Month.

Getting resources and capabilities in place was a bigger challenge. We went for low-cost, in-house implementation, with individuals contributing as they could with domains, hosting and conferencing software, in addition to their own talent and tools for art, streaming and video editing. This helped us put on an event for minimal costs, but it also was an intense learning experience in getting everything to work as intended.

Finally, differences did arise within the team—cultural differences, lack of familiarity, working styles—yet everyone had the same enthusiasm. The early everything-by-consensus approach was tested and became more direct. This was an adaptive leadership challenge for everyone, and I am glad to say that everything worked out as, ultimately, we focused on our shared end goal.

Where to Go From Here

We continue to monitor impacts on each chapter's growth with metrics such as increases in social media followers, website visits and additional membership. Just a week after the event, there was clear evidence of such growth, though it wasn't consistent across all chapters.

Our first enthusiast-run online regional event was successful! If you are wondering whether to try something like this, I'd say go for it. If you need some insight, any of our chapters involved in the event would be thrilled to help. You can find us, and the session recordings, at cybersectalks.org. Email me at fcastro@isc2chapter-chile.org.

We already are planning for this year's summit, based on lasting relations with speakers and local professional communities, and using lessons learned from the inaugural event.

We look forward to having newly formed chapters in Latin America join us for the next edition of CYBERSEC TALKS. •

JOIN THE (ISC)² COMMUNITY!

With 30,000+ members, join the (ISC)² Community where (ISC)² members, cyber experts and IT security professionals collaborate, share knowledge and offer best practices required to manage cyber threats and risks in business today.

Join Now



CONNECT. COLLABORATE. SHARE. DEVELOP.

community.isc2.org

ADVOCATE'S CORNER

THE FUTURE OF CYBERSECURITY THREE DECADES OUT

BY TONY VIZZA, CISSP, CCSP

The world today is vastly different from the world of 30 years ago, when my interest in IT began. My first computer possessed far less processing power than even the simplest electronic device I own today. Pondering the past, I recently asked myself the question: How different will cybersecurity be in another 30 years' time?

Truth is, I don't regard myself as a particularly adept soothsayer. However, I am mindful of a quote from Confucius, who once said, "Study the past if you want to divine the future." And as an avid student of history, here are three broad predictions for the next 30 years in cybersecurity.

Cyber Safety Will Be A Top Priority

Using the aviation industry as an example, in the early days of flight, importance was placed on achieving three key results: *endurance*, through flying over increasingly vast distances; *speed*, through faster flight; and *functionality*, achieving military or commercial purposes. Only after these results were achieved, and following a spate of tragic accidents involving airliners, did the shift occur to *safety*.

In a cyber context, cybersecurity professionals have arguably achieved the aviation equivalents of endurance, speed and functionality. And while we are seeing the formation of safety-conscious approaches to cybersecurity through topics such as zero trust, and efforts from governments around the world toward safety in a cyber world, we still have a long way to go before the concept of safety becomes as homogenous within cybersecurity as it is in aviation.



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

Cybersecurity's Value Will Be Well Understood

I am often questioned by non-IT people as to whether they need cybersecurity at all. I reply with a question, "How secure would your home feel if your front door didn't have a lock, backyard didn't have a fence, or alarm didn't work?"

The answer, unsurprisingly, is "Not secure at all."

I then explain that cybersecurity controls are the digital equivalent of physical security systems. Then, I ask what could potentially happen if that person forgets to lock their front door and activate their alarm system when they leave the home. Their response: "I'll probably get broken into."

Then, I explain that having those controls isn't enough. You also need to remember to lock the door and switch on your alarm, otherwise those controls are next to useless. The focus shifts to *people* and *process*.

It's an analogy that works particularly well because property crime rates in most countries continue to fall. In Australia, for example, property crime such as breaking and entering, motor vehicle theft and robbery are 80% less likely to occur today compared to their historical peaks. Much of this is due to an increased understanding, better processes and better technology to reduce property crime risks. In time, as cybersecurity challenges continue to be better understood and as cybersecurity is better valued and understood, a noticeable decrease in cybercrime will occur too.

Privacy Considerations Will Achieve Prominence

The advances that have been realized due to IT in our day-to-day lives are too numerous to describe. However, these advances have exposed people around the world to significant privacy concerns. As a result, changes to privacy legislation, including the European Union's GDPR, the U.S. state of California's CCPA, Canada's PIPEDA, Brazil's LGPD and China's Data Security Law, have seen privacy provisions strengthened, particularly in relation to the digital world.

As awareness of the critical importance of privacy in the digital age continues to be asserted through better public knowledge, privacy issues will manifest themselves through test cases, landmark rulings, a stronger focus on the right to privacy by individuals, and stronger demands by society on ensuring products and services adhere to a privacy by design approach. This will also result in expanded employment opportunity areas such as digital privacy and cyber law. ●

Hiring the ‘Smartest’ Candidate May Not Be the Wisest Move

BY DEBORAH JOHNSON

High demand for cybersecurity professionals presents an even greater challenge if you are the one trying to fill a key position. It may be tempting to seek a previously undiscovered “genius,” but is the big thinker really the best person to add to your team?

“Smart is usually the first thing that goes through your mind when interviewing someone,” Rhiannon Beaubien told me in a Zoom interview about her post on Farnam Street titled “[Being Smart is Not Enough](#).”

“It’s not that it’s a bad place to start,” she continued. “It’s just that ... having the technical competencies is not enough. When I think back to job experiences that I’ve had, you do see that there’s a more three-dimensional dynamic that a person needs to fulfill in order to be a really good fit for a team.”

In his book, *The Secret of Our Success: How Culture is Driving Human Evolution, Domesticating Our Species and Making Us Smarter*, Harvard University professor Joseph Henrich proposes that our great strides in invention and technology have depended on communicating with and learning from each other. He breaks employees into two groups: Geniuses and Butterflies. Geniuses may be innately smarter than butterflies, but they are not very social, which limits the

reach of their breakthrough ideas. On the other hand, Henrich argues, butterflies individually may not be as intellectually bright, but they “have friends” to help enact great ideas.

He writes, “Among the Geniuses, a bit fewer than one out of five individuals will end up with the invention [by figuring it out by themselves]. Meanwhile 99.9% of the Butterflies will have the innovation. Bottom line: If you want to have cool technology, it’s better to be social than smart.”

That, though, typically runs counter to interview expectations.

Jakub Kubrynski, CEO of technical screening platform [DevSkiller](#), agrees it’s crucial for an organization to have a mix of “genius” and “social” developers. In an email exchange, he outlined his approach to achieving it. “It’s a complex task to effectively verify such skills during the recruitment process. The first one [genius] means we want someone with problem-solving skills. This part is often automated nowadays, so we can maximize the talent pool.”

For assessing communication skills, he offers this tip: Work in teams of two when interviewing candidates. “You will find out if the candidate is able to clearly explain their thoughts, ideas and thought process to solving problems. A panel of two offers a wider perspective and limits the possibility of any interviewer bias affecting hiring decisions.”

Whether going it alone or double-teaming, don’t hire solely based on a candidate’s intellectual prowess, unless that trait is sorely needed on your team. Instead, consider not just who will come up with novel solutions, but also who will have the networking skills to make sure the solutions not only come to fruition but gain traction with key user groups. ●



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



Benchmark COVID-19's Impact on Your Organization's Security Posture



How has the COVID-19 pandemic challenged your organization's security efforts? The *Impact of COVID-19 on Enterprise IT Security Teams Report* reveals the latest security trends and challenges, how organizations are responding to increased security threats, and tools and best practices cybersecurity leaders are considering for 2021.

The research shows:

- A 114% increase in remote workers during the pandemic
- 67% of responding organizations are experiencing IT security staffing challenge
- 75% claim COVID-19 has increased their preference for cloud-based security solutions
- 66% now have a BYOD policy in place, up from 41.5% pre-pandemic



Read the full report to benchmark COVID-19's impact on your organization's security posture, investments, operating budget and best practices against industry peers.

[Get Your Copy](#)

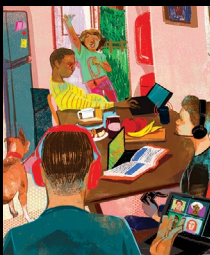
“I can’t change the direction of the wind, but I can adjust my sails to always reach my destination.”

—Jimmy Dean, American country music singer, television host, actor and businessman

We continue to live—and work—through unprecedented times. In this issue we examine how to make it work: from holding it together on the homefront to securing devices from ... anywhere. We also discuss a way to improve morale, or at least keep it from sinking into an abyss.

The Future of Work

PAGE 19



The Evolving Home Office

PAGE 24



From Bummer to Bumper

PAGE 28



the future of **Work**

Offices with millions of street addresses. Operations with higher unpredictability. And a distributed workforce increasingly vulnerable to cyberattacks.

BY ASTRID HARDERS

IT'S TUESDAY MORNING in the suburbs, where the Smith family is hard at work. Dad is in endless Zoom meetings with his lawyer associates in his home office. He gets up occasionally to adjust the Nest thermostat. Mom is sitting at her adapted bedroom desk reviewing scripts and streaming a newly released piano album via Alexa. Their teenaged daughter is half-attending an online algebra lesson in her bedroom while scrolling through her Instagram account. Her little brother, seeing how the entire family is busy, has muted his microphone and turned off his laptop's camera during his Zoomed geography class. He instead downloads a new version of his favorite video game.

By lunchtime, the Smiths will unintentionally have leaked confidential court documents, provided intellectual property thieves with a script plot, and opened up their home to cyber attackers.



In today's COVID-19 world, households are still working and learning under the same roof, continuously connected to their home's Wi-Fi. They still lack the same protections as a hermetic corporate network. Household smart devices remain potential gateways for outsiders to enter the home network and comfortably access the material being transmitted through it. In the case of the Smith family, intruders likely leveraged the home network to gain access to Dad's legal documents, Mom's script and the children's passwords, just for starters.

The Smiths' security breach is not only a problem for them; it's also an enormous problem for their employers, clients and schools. The ripple effect of a breach begun at home reaches far and wide into corporate and educational systems. And, a year into the pandemic, employees continue to work remotely. Some by choice and some by mandate.

FACING THE 'NEW NORMAL'

Companies have their hands full with revamping protocols. Before COVID, firms focused on good cyber hygiene within a corporate network: from maintaining firewalls to updated anti-malware software to phishing awareness training for all employees. Sure, there was the occasional

ILLUSTRATION BY
JOHN JAY CABUAY



“One of my clients has already decided that they’re going to get rid of their office space and go into a hotel-type situation if they need a conference room.”

—Michael D. Weisberg, CISSP, CISO and vice president of the information security practice, Garnet River LLC

remote VPN connection, but the majority of cybersecurity control happened within the office, in the context of a secure network.

Once COVID-19 hit, security teams had to make swift changes in order for employees to work securely from home. A good number of those companies suddenly saw remote work move from a corporate perk to a nationwide mandate.

Michael D. Weisberg, CISSP, the CISO and vice president of the information security practice at Garnet River LLC, received many new requests from his clients related to the new reality of working in the wake of a global outbreak.

“One of my clients has already decided that they’re going to get rid of their office space and go into a hotel-type situation if they need a conference room,” he says. “This client will have everyone working remotely. From the security perspective, that means they’re going to be adopting *their* clients’ security model, as opposed to having to protect their own office, which is a bit of a change. They cut out risk for themselves and for [their] client, who is now absolutely sure that there is protection of the information because they are the ones handling it.”

Senior network security consultant Néstor Muñoz, CISSP, who is the CISO at Miami-based Samana Group LLC, which provides managed services and project-based work on virtualization, cloud and networking, describes one of his client’s COVID response: “I have been working with a bank that had projected the digital transformation of all of its employees between five and 15 years down the road. This bank was giving zero importance to employees working remotely. Then they had to buy 5,000 laptops in March when the lockdown started, send a laptop to each one of the employees, and, the worst part, start teaching those 5,000 employees on a nationwide scale how to install a remote laptop to function.”

And while some companies were more prepared than others, the truth is nobody was fully prepared for COVID-19. “You can’t really prepare for something that is unknown. That is exactly what happened to all the companies with COVID,” Muñoz says.

SOME GOOD CAME OUT OF IT

Fortunately, working remotely has also produced positive effects for companies. “Some clients have seen a jump in productivity. The project that was scheduled for the end of the year is all of a sudden already getting done. The thing with lock-ins is that people have the time; they are being more productive because they are working in a comfortable environment,” says Weisberg. “Plus, the security team is getting less pushback.”

Ben Malisow, CISSP, CCSP, SSCP, an information security instructor and author of the *(ISC)² CCSP Certified Cloud Security Professional Official Study Guide*, also honed in on opportunities for some, even if they create more obstacles for others.

“One of the nice parts about working from home is that home can be anywhere. You are not married to a particular physical location. People are moving out of major metropolitan settings because they found that the home of their dreams is a lot more affordable two states away,” he says. “If you can keep the same job at the same pay, but that money can go further because you don’t have to be showing up to the weekly meeting every Wednesday morning, that’s fantastic. That is a true opportunity for the employees. There are trade-offs; we just have to get past the cobwebs of the traditional environment in order to see what those benefits are going to be.”

HOW CAN COMPANIES IMPROVE?

While experts' opinions and companies' needs differ, it's up to each organization to find which changes can translate into unprecedented success.

Weisberg says companies don't need to invest in thousands of laptops for their employees to work from home. By using online tools such as videoconferencing software, employees can run a "rogue" desktop using their own hardware. "The savings have become so apparent now that a lot of companies are even seeing that people have better machines at home anyway," Weisberg says. "As long as we can secure the operation by sandboxing these rogue machines, we have a higher security profile and we don't have to issue hardware."

Malisow believes in focusing on the process more than the tools. "Better than having a magic box or a piece of software, we should address how the data is being shared. If you have something really valuable or sensitive, maybe you have them hand-carry it from an office, maybe you

have them work offline, maybe you get them a laptop that doesn't connect to the internet ... and you're still going to have a risk. As long as that box can touch the outside world, attackers can get to it. Still, a good process that constrains the data, not the machine or the user, is going to be a much better way to protect the integrity and value of that data."

Apart from hardware, remote access and data protections, cybersecurity awareness needs to be adapted. "Usually, cybersecurity awareness training is a slide show that employees go through by clicking 'next, next, next.' They just want to comply with having gone through it, even if they didn't really," Muñoz says. "We are ignorant; that is why security breaches happen. The only thing that protects against ignorance is knowledge. So, we need to make sure we're teaching people in a way that they understand. Employees need to grasp the importance of this in their personal lives first. Cybersecurity awareness cannot be forced, because people will hate it and not absorb it."

And absorbing the possible threat is key, because COVID brought on a more specialized type of phishing that targets remote workers.

"You are going to be seeing more of the social engineering type of attacks," explains Weisberg. "It used to be: It's Monday, 9 a.m. You're in the office, and what would be an email or a call from the outside was pretty clear. Now, we're going to see more attacks focused on gaining access. Example: 'I'm stuck at my in-laws' house, not at my home computer, and need XYZ application. Can you give me access?'"

But all the tools and training in the world cannot protect us from ourselves. Companies need to come to terms with the reality that is human risk. "There is no software or hardware in the world that

protects us against the idiocies we all commit," Muñoz says. "We learn how to be stupid every day at a faster pace."

WHEN A ROGUE EMPLOYEE CAUSES A BREACH

Let's go back to the Smiths for a moment. After a morning of remote work, we have Dad's law firm in a panic over leaked court documents and Mom's production company furious over a script plot accidentally handed to cyber criminals. What are the law firm's partners and the production company's HR department going to do respectively about these two behind those breaches? Neither intended to leak anything, but it happened because they were working from



“There is no software or hardware in the world that protects us against the idiocies we all commit. We learn how to be stupid every day at a faster pace.”

—Néstor Muñoz, CISSP, senior network security consultant and CISO, Samana Group LLC



“There should be no expectation that a professional who’s astute in one field should have any knowledge or practice with cybersecurity concepts or procedures.”

—Ben Malisow, CISSP, CCSP, SSCP, information security instructor and author of the (ISC)² CCSP Certified Cloud Security Professional Official Study Guide

home in a fairly unsecured environment. What are the consequences?

“There should be no expectation that a professional who’s astute in one field should have any knowledge or practice with cybersecurity concepts or procedures,” Malisow says.

OK, so perhaps Mom got off with a warning and intensive cybersecurity training. Is anyone making sure her morale is not shot after this incident? What is stopping Mom from leaving the company that confronted her with something she never meant to do? And if she does leave the company, what is stopping her from telling everyone she knows, her entire production network, that this company is unjust and that nobody should ever work for them?

There is no guarantee. But what companies and HR departments in particular can do is envision these possible scenarios.

“The real issue is going to be that these companies and their end clients are going to have to come to terms with the fact that the liability still rests with the company, not the individuals who may or may not have done something that led to a breach,” says Malisow. “And if they continue to want people to work in a remote environment, it’s up to the companies to make sure that it’s safe.”

HIRING AND MANAGING REMOTELY

What about hiring new employees, onboarding them, and managing them without direct supervision? HR departments will need to get creative.

According to Malisow, the problem lies in HR departments sticking to the same old ways, pandemic or not. “We haven’t really used any data-driven metrics to figure out if the processes that we currently use for hiring and managing people are worthwhile,” he says.

Who says that in-person interviews, under the belief that they will give the hiring manager a better sense of the future employee, are the way to go? “We have absolutely no data that supports whether or not a good interview leads to longevity of employment or productivity. So far, all we know that interviews do is make sure that we’re hiring people who are good at interviews.”

Note to companies: Perhaps simply translating what used to be an in-person interview to Zoom or Skype isn’t really solving anything. Forcing an old hiring model into a new technology doesn’t make it better.

AN UNPRECEDENTED OPPORTUNITY

Whether you are a company that survived the economic challenges wrought by the pandemic, or you are an employee clinging to a job, the future might look better than initially considered.

“I think it’s a net positive, even though the motivation that got us here is negative and awful,” Malisow says. “This is a very good opportunity; we just have to be able to capitalize on it properly and use the benefits while we try to avoid the security parts.”

So maybe after there is a vaccine, after the economy has licked its wounds, after we have gotten into a mindset of forward-looking changes, families like the Smiths will have adopted good cyber hygiene habits and, best of all, heightened their quality of life by avoiding a time-consuming commute. ●

ASTRID HARDERS is a freelance writer originally from South America and located in Miami.



“I and other folks realized this isn’t just going to be us ‘getting by’ for a few weeks or months; we have to figure out how we’re going to run this company securely, sustainably, and thrive in a distributed fashion for the long term.”

—Ben Waugh, CISSP



THE EVOLVING HOME OFFICE

BY ANNE SAITA

As employees continue to work on their own terms and turf, cybersecurity teams need a sustainable approach to protections

When the COVID-19 pandemic forced corporate offices to close and employees to work from home, Ben Waugh, CISSP, thought of business continuity plans built on worst-case scenarios.

“Theoretically, this is what a lot of companies planned for, but we never

really prepared for it to be this widespread and over an extended period of time,” the chief information security officer for Seattle-based digital health interoperability platform Redox recalls.

The two-month mark, Waugh says, was when everything really sunk in.

“I and other folks realized this isn’t just going to be us ‘getting by’ for a few weeks or months; we have to figure out how we’re going to run this company securely, sustainably, and thrive in a distributed fashion for the long term.”

PHOTOGRAPHS BY GETTY IMAGES



“You really can’t go to an employee and say ‘here are 50 things you need to do to secure your home network,’ like set up a WPA2 password and configure a firewall. It isn’t practical.”



—Ben Waugh, CISSP

EARLY SACRIFICES

Research conducted following a massive and rapid work-from-home movement reflects that lack of initial preparation.

[University of Chicago researchers](#) surveyed 10,000 U.S. workers in May, June and August 2020 and extrapolated 52.3% of all employees worked from home, compared to 5.2% during the same period the year prior. And those were the ones fortunate to have something to work on, given the deep recession the pandemic triggered.

Other studies showed sharp increases in cyberattacks and risk exposures once everyone went home. For instance, 85% of CISOs surveyed among 937 IT professionals admitted sacrificing cybersecurity to quickly enable remote work, according to [cybersecurity vendor Netwrix](#). The biggest headaches immediately following an all-remote workforce were not surprising: phishing, admin mistakes and improper data sharing.

Similarly, Positive Technologies [conducted a study](#) during roughly the same period. It showed a record-breaking number of cyberattacks representing a 59% increase over the same period in 2019. Stolen company credentials doubled over the previous, pre-pandemic quarter.

This, of course, is well known to cybersecurity professionals trying to navigate the now-trite “new normal.” But protecting private and proprietary data going into and out of makeshift home offices is getting more difficult. Employees are on the move. No longer confined to commuting distances, they are relocating to far-flung destinations or less expensive areas. Or, due to financial or personal losses, they are combining households to make ends meet.

A REMOTE-FIRST, DISTRIBUTED IT INFRASTRUCTURE

Waugh had experience building a security team with remote capabilities, given that up to 80% of Redox’s 200 employees already worked from home when the pandemic hit (the remaining 20% were mostly using co-working spaces). That includes the dozen IT security professionals on his team that physically gathered at least semi-annually before COVID struck.

“As a hiring manager and security leader, it’s been great to have that capability to hire anywhere in the U.S., or even beyond; it opens up a much more diverse and talented employee pool,” he says. “Being a distributed workforce does have its challenges, though, from logistical and security standpoints. Folks do lose a lot of the relationship-building that’s important, especially for a security team that relies on collaboration to further security goals.”

Because Redox already had a dispersed workforce, the pandemic didn’t cause the same level of panic. Its remote-first, distributed IT infrastructure meant endpoint-first security already was a high priority.

Unlike traditional IT infrastructure, strong authentication mechanisms must now be in place to remotely manage, monitor and secure staff devices regardless of where they are located. These include a refocus from perimeter-based network security controls to host-based ones and multi-factor authentication for *each* application.

Waugh also recommends treating every network as unsafe, even hostile—and that includes home networks. “You really can’t go to an employee and say ‘here are 50 things you need to do to secure your home network,’ like set up a WPA2 password and configure a firewall. It isn’t





“When you no longer have direct physical control over the end user device, or the network, you are forced to contend with the human factor.”



—Chris Finch, CISSP, senior principal systems engineer, Global Governments Critical Infrastructure, Forcepoint

practical,” he explains.

Instead, he suggests providing basic tips, knowing they may not be put in practice. “You need the capability to say, ‘I know what’s going on with this device and I know how to control it to patch it, maintain configurations and get events from it regardless of where it is.’ As well, you need to be able trust the information received from that device.”

Redox standardized on Macs (though the same tactics work for Windows shops too) and deploys mobile device management software to monitor employee machines regardless of what network they happen to be on. It pushes software patches (with a typical three- to five-day window for users to apply them) and remotely manages configurations and pulls events without requiring devices to be on a local network.

An adversarial stance on home networks is necessary, Waugh argues, because an employee might swap out a secured device or add a new smart appliance to that network that a company admin can’t control. “The same is true of an office network anyway,” he reasons. “You probably have thousands of devices on that local network from people plugging in from the breakroom or another area of the building that you don’t know if you can trust.”

IN ZERO, WE NOW TRUST

That brings us to zero trust, which flips traditional security trust models that verify a device, user, application, etc., and grant privileges within a defined perimeter. With zero trust, a device is continuously verified and access restricted because that trust is never taken for granted.

Chris Finch, CISSP, is senior principal systems engineer for Global Governments Critical Infrastructure at Forcepoint (formerly Raytheon Websense), a provider of user and data cybersecurity solutions. He believes interest

in human factors and zero-trust models helped organizations transition once COVID-19 hit.

“When you no longer have direct physical control over the end user device, or the network, you are forced to contend with the human factor,” he explains.

He views mobile security as the proverbial elephant in the room, an area where teams still struggle to apply appropriate device security to stop advanced threats without frustrating users. Lean too heavily into device protections, and more users are likely to contribute to shadow IT woes.

ESTABLISHING QUARANTINE ZONES

Finch recommends minimizing the user device’s role when it interacts with corporate resources by establishing a quarantine zone. Much like a traditional remote use case, quarantine zones leverage VPN technology to establish a point-to-point connection between user and corporate networks. However, the VPN connection terminates within an isolated network segment established outside of the corporate network. As such, applications are remotely displayed as virtual desktop sessions within that cordoned area. This connection flow introduces a protocol break between the user and the corporate data, so the user device never establishes actual connectivity with the corporate network.

Remote users working within a quarantined area can cut down (perhaps significantly) on network threats, including zero-day attacks. They also allow security operations to deploy cybersecurity tools and monitor user behavior without having to manage that user device.

“We’re not inventing something new with this concept, but sometimes people have a difficult time seeing the forest for the trees. They get caught up in doing things the way they’ve always done them,” Finch says. “Just like





“More so than ever in this hybrid mode, companies need to create a hardened shell around devices themselves and make sure they can operate on a non-trusted network.”

—Ben Waugh, CISSP

with zero trust, I don't want to depend on the security of the network. In this case it's the same thing: I'm not going to depend on the security of the device someone is using. I want to move user interactions with corporate resources into a space I can control.”

Desktops and applications are increasingly offered in the cloud, so they do not have to reside on a user device. “All of the data, and transactions with that data, can exist in a controlled environment, completely transparent to the user. That really is the kind of model we need to look at for a remote workforce,” he says.

This is now possible because of thin computing and virtualization technologies that can stream applications, even full desktops, over wide area networks for a more acceptable user experience. Also needed are a point-to-point VPN that can be deployed to a user device; a firewall to establish an isolated network segment in the quarantine zone; and a remote desktop solution.

Finch himself relocated during the early months of the pandemic for better housing and milder winters. He works in the government space and has seen a change in attitude around the use of NSA-approved commercial solutions that connect remotely via VPN connections, and in multiple layers, into a data center.

“In the past, the idea of someone accessing classified data from a remote location like their home would have been a non-starter,” he says. “Those conversations are happening now.”

A HYBRID APPROACH

Throughout 2021, more employers are expected to adopt a hybrid model in which employees can work from the

office some days and from whatever constitutes “home” on others. Others will give up commercial leases or sell their buildings while maintaining an all-virtual workforce.

“In my opinion, we need to continue changing our mindset around how these hard perimeters are supposed to work,” Waugh says. “We need to change from thinking people are only safe at work and unsafe when working from somewhere else.”

“More so than ever in this hybrid mode, companies need to create a hardened shell around devices themselves and make sure they can operate on a non-trusted network,” he continues. “Because now the office network itself is at great risk of having stuff on it that's unexpected, from having devices come to it from untrusted networks. It creates a need for employees to understand what those risks are.”

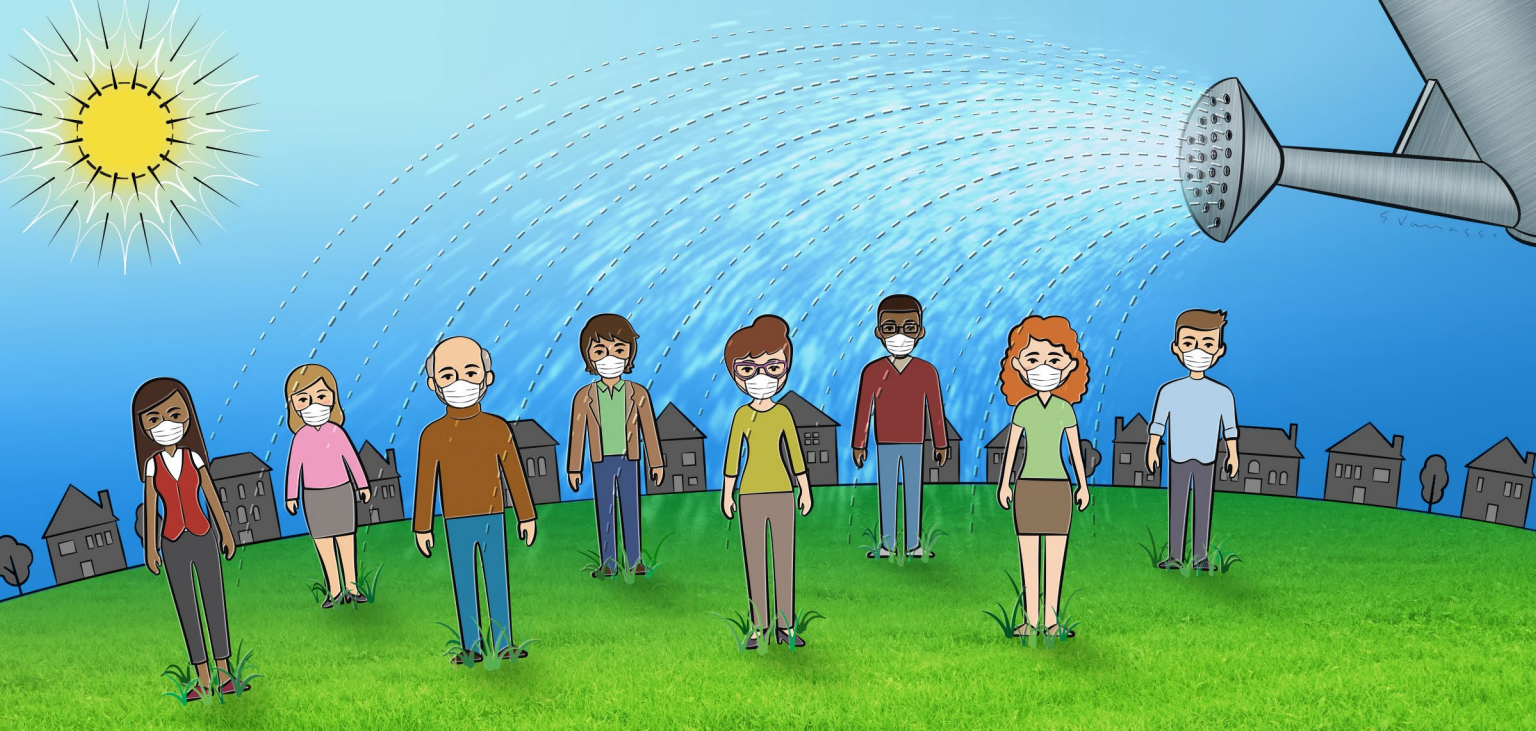
Finch agrees. “For all intents and purposes, our job is changing, and we're now charged with protecting thousands of micro networks. We have to change the way we think about cybersecurity to adapt to the way users are consuming information.”

Adds Waugh: “Most of us technical security people, if asked to describe our home networks, would talk about having this really complicated, secure setup. We have multiple VLANs and secured networks. But we are not your average employee.”

“I've seen security professionals going in and expecting employees to set up their home networks a certain way to help them be secure. Most folks aren't going to do that,” he concludes. “Keep it simple. The simpler it is to do the right thing, the more likely they are to do it.” •

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





FROM BUMMER TO BUMPER

Just like a master gardener, we all need to nurture engagement, maintain morale, build teams and flourish while [still] working from home

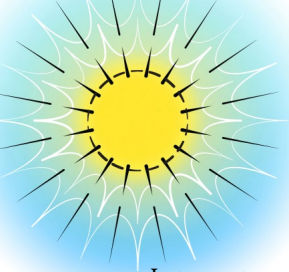
BY
DR. MICHAEL M. HANNA,
DIT, CISSP
RYANN HANNA, SPHR
DR. BOB DUHAINY, PH.D.

PRIOR TO THE PANDEMIC, most people shared similar variations to the start of their days. They may have begun with an early morning workout at the nearby gym, brewing a cup of coffee, waking up the kids, getting them ready, checking a couple emails before leaving the house, getting the kids to school, driving into the office and socializing with colleagues on breaks. That sounds like a glorious dream now, doesn't it? Or does the old way of working conjure nightmares now distant due to ongoing work-from-home mandates?

As a cybersecurity leader, you must create an environment that supports engagement and morale across varying circumstances. You do this to maintain a competitive advantage and strong employee engagement. However, your team might view work-from-home differently, feeling that edge, that engagement and that attitude continue their downward slide as months of physical isolation shift to year[s]. It's your job to promote the best in your team based on this unusual, new normal.

ILLUSTRATION BY ENRICO VARRASSO





Let us return to the morning routine and two likely scenarios in the current COVID era.

One employee continually presses the snooze button until the last possible moment, still exhausted from the prior day, skips that morning workout because the gyms are closed, rushes to brew a cup of coffee and consume any form of breakfast while the kids are running around the house and screaming at the top of their lungs. The employee gets the kids set up for school (virtually) with five minutes to spare before the first virtual meeting of the day conducted in a home office with their kids popping in and interrupting. This person struggles to get through it all, day in and day out—meet family obligations and work objectives—with no separation between work and home.

Another employee wakes up without an alarm, heads to their desk in pajamas, checks their emails with a cup of hot coffee, throws in some laundry, wraps up that big project, jumps on their in-home spin bike, conducts a group meeting, runs to an eye doctor appointment, takes that last-minute call from the boss, and then walks to the kitchen to make that new recipe they've wanted to try for weeks. They feel productive, rested and happy. They could do this forever.

Now we have visualized the new normal for two employees with similar job functions, but completely different outside obligations. Your corporate team members could be thriving, or they could be struggling to get out of “quicksand.” So how do good leaders keep highly productive members engaged so they stay, and overwhelmed ones performing optimally when everyone is working remotely under wildly different circumstances?

The buzz phrase for the last two decades has been “work-life balance.” But let's be honest; science often lags general public consumption. Behind the scenes, organizational psychologists have been tracking an evolution of this idea, which we are seeing come to fruition for all of us during COVID-19: work-life integration.

This concept isn't new; in fact, it started gaining notable traction in 2005, recognizing that while balance is a defined separation of work and home, integration is really the ultimate interweaving of our careers, family and socialization needs. This is great news for companies and leaders looking to better engage their remote workforce, because integration is a connection that allows for ulti-

Bottom line: by leveraging the practices of positive psychology to promote optimal work-life integration. Read that one more time; work-life integration, not work-life balance.

mate flexibility, empowerment and creativity.

A recent research article presented the skills beyond the technical that would ensure the success of the cybersecurity workforce. The researchers claimed that successful future cybersecurity professionals would possess traits such as strong technical and social skills, effective communication, systematic thinking, a sense of civic duty, the desire to continually learn—all while being team players.

Now through the work-from-home mandate experienced around the world, the road to a successful and strong security team depends on the environment you create to foster work-life integration, holistic development and well-being.

How, as leaders, do we promote the best possible situation for our teams? Bottom line: by leveraging the practices of positive psychology to promote optimal work-life integration. Read that one more time: work-life integration, not work-life balance.

PLANTING YOUR GARDEN

Traditional psychology is focused on identifying and treating issues. Positive psychology is an approach used to encourage and promote holistic development and well-being. Consider the professional and personal lives of your team as a garden. Traditional psychology would be the methods used to identify and eradicate weeds. If

this was the only approach we took, sure, we could say that we have no weeds, but we really only have a garden of dirt. What good is that? Positive psychology is the planting of different seeds to create a vibrant and high-variety garden.

Maintaining a competitive advantage and highly engaged team requires management skills that encourage a similar vibrancy. It is much more than hiring the strongest technical professionals. You must create an environment that promotes the best version of work-life integration and ensures the well-being of your team in an already extremely stressful and demanding line of work. Add variables introduced by COVID, and we are reaching new highs in stress. Not only do you need your team to operate at the highest level, but you also need to retain your talent in an environment where remote work is more than accepted; it is desired. Employees don't need to move anymore to work for a Silicon Valley giant.

Going a step further with the analogy, for a moment, compare our technical skills to lettuce, the foundation

WAYS TO 'BLOOM WHERE YOU'RE PLANTED'

Now's a great time to scrap work-life balance and promote work-life integration

MOST OF US are familiar with the expression “Bloom where you’re planted.” It refers to being grateful for the present, rather than rue what was, is or might be. If ever there was a time to adapt a more positive outlook, it’s now. While this is by no means an all-inclusive list, the following are five recommendations to get you started in promoting work-life integration throughout your team and organization.

1. Everyone is going through something different. Don’t assume that each member on your team is facing the same challenges. They aren’t, and it is your job as a leader to manage the circumstances of your team to achieve your goals. **You need to create a culture of safety.** It is imperative to promote psychological safety for a remote workforce, which requires a dedicated approach to accommodate individual needs. Psychological safety can be difficult to detect when employees are working remotely. Creating a safe culture whereby remote workers feel that their concerns are heard and being addressed is of the upmost importance. Remember, as a leader, you work for your team and not the other way around.

2. **Bring structure into the uncertain pandemic equation.** Working at home has created an interesting dynamic. We are actually working longer hours and finding it more difficult to “unplug” at the end of the day. As a leader, focus on workload and management practices. It is found that improperly managing an employee’s workload may significantly impact engagement. Remind your teams that not only is it acceptable to step away from your computer at the end of the day, it is desired that they do not “return” to work during the evening when they should be unwinding. Remind your team that it is also OK to run an errand or two during the day and allow them to plan for it. You’ll need to lead by example so that your team trusts that this is a genuinely accepted behavior.

3. **Keep positive and keep building relationships.** During the pandemic, it surely is tough to remain upbeat and we are certain that your social relationships have changed, but that doesn’t mean there isn’t anything we can do. Sure, you can’t chat at the watercooler or take a quick coffee break with a colleague, but virtual work environments do not need to be doom-and-gloom. It is important to stay

connected and social. Instead of allowing team members to keep their cameras off, make sure that everyone can see each other during the meeting. This makes a subtle but important difference in maintaining/building relationships and may promote a more positive outlook. One important thing to remember is that meeting leaders need to be positive. People tend to imitate the behaviors and feelings of others. Sometimes, virtual lunches and happy hours can make a difference when done right. For example, during a virtual happy hour, have an employee volunteer to show how to make a drink on camera in their home. You’ll be surprised by the outcome.

4. **Be transparent and set expectations.** Meaning and accomplishment are key tenants of the PERMA model (along with positivity, engagement and relationships), and these concepts can be supported by being fully transparent with your teams. Be honest and apparent with your expectations and priorities, while enforcing the desired processes needed during work-from-home. Setting specific expectations provides employees with a gauge to compare their outcomes with your desired results. Being fully transparent with employees will also promote personal satisfaction and a high-trust environment. These are critical outcomes to achieve if you are looking to get the best in your teams and retain your top talent.

5. **View leadership differently.** The geographically dispersed nature of remote employees requires a more effective leadership approach. Adopting a new behavioral approach with remote workers to promote social bonds and build trust among teams is needed now, more than ever. Informal communication channels should help bridge the trust gap that may surface in virtual environments and should strengthen the social networks that may not exist face-to-face.

—M. Hanna, R. Hanna, B. Duhainy

of many salads. We see it time and time again, where some security professionals will only focus and develop their hard skills. If that is all we focused on, we have only planted lettuce and at best, we can only create a salad consisting of lettuce. That's pretty boring and honestly, not very appealing for long. Positive psychology provides us the tools and methods to plant other fruits and vegetables to create a vibrant salad.

TENETS OF POSITIVE PSYCHOLOGY

The tenets of positive psychology are positivity, engagement, relationships, meaning and accomplishment, also known as the PERMA model. Each of these tenets are related to each other and in order to achieve the engagement and morale needed during our current environment, the need to promote positivity, relationships, meaning and accomplishment are greater than ever.

There are numerous ways to foster a better work-life integration, both now and going forward. (See *5 Ways to 'Bloom Where You're Planted,'* p. 30.) Whether you are a company executive, team manager or just someone struggling

to hold it all together right now, there are ways to retain or return to high productivity—maybe even higher than before most of us were forced to convert our homes into satellite offices.

It starts with some reframing around how we now motivate, and are motivated, to be our best selves.

To summarize, positive psychology focuses on what makes life worthwhile and how to succeed as an individual. Work-life integration is the holistic approach to living: as a whole, across work, home, social and personal domains. As such, positive psychology provides the foundation to promoting a thriving work-life integration model. ●

MICHAEL HANNA, CISSP, is a past contributor and holds a doctorate in information technology. Hanna is a member of the U.S. military. The views expressed here are solely those of the author and do not necessarily reflect those of the Department of the Navy, Department of Defense or the United States government. **RYANN HANNA** is an industrial-organizational psychologist and human resources strategy expert. **BOB DUHAINY** is a professor with Walden University.

(ISC)² MEMBERS:

share
your
expertise

InfoSecurity Professional, Insights and Cloud Security Insights are looking for (ISC)² members who wish to share their expertise in either technology, management or career development.

If being published is a 2021 career goal, we may be able to help you fulfill it. Send us a brief proposal of your idea and how you're qualified to write about it to get the process started. We've provided dozens of such opportunities for members in recent years—some of which have gone on to win industry awards!—and hope to showcase your work too.

Email Anne Saita, Editor-in-Chief, at asaita@isc2.org.

JOIN US AS WE KICK OFF OUR 10 YEAR ANNIVERSARY CELEBRATION!

2020

- **Garfield at Home** and **Garfield Virtual** for the Classroom Released
- Record \$208,300 in **scholarships and financial aid** awarded bringing total to **\$1.5 Million** in scholarships awarded thus far



2018-2019

- Released updated **Parents, Children 11-14** and **Senior Citizen** presentations
- Center holds first **Cyber Safety Day** for children of New Orleans during (ISC)² Security Congress
- Center launches **new website** IAmCyberSafe.org and begins **cyber safety community blog**
- Safe and Secure Online released in multiple **languages**



2017

- Largest **Global Information Security Workforce Study** (GISWS) released with 19,641 infosec professionals from 170 countries
- **Children's Internet Usage Study** released
- Garfield's Cyber Safety Adventures **Posting** and **Cyberbullying** Lessons Released



2016

- Center begins partnership with Jim Davis to develop **Garfield's Cyber Safety Adventures**
- Garfield's first lesson on **Privacy** released
- Foundation rebrands to **Center for Cyber Safety and Education**
- **(ISC)² Chapter Scholarship** Program Launched



2015

- Safe and Secure Online program for **Senior Citizens** launched

(ISC)²
Safe and Secure Online

2014

- First corporate-sponsored scholarship awarded



2011

- (ISC)² Foundation launches with **Safe and Secure Online** Parent and Children programs in partnership with Childnet on isc2cares.org, and (ISC)² **cybersecurity scholarships** for graduates, women and undergraduates



10 YEARS

2011- 2021



CENTER FOR
**CYBER SAFETY
AND EDUCATION**

IAMCYBERSAFE.ORG/GIVE

CENTER POINTS

FOCUSING ON EDUCATION AND RESEARCH INITIATIVES

Ten Years Into This, We Are Just Getting Started

THE CENTER DEVELOPS PLANS TO PROVIDE 1 MILLION SAFETY LESSONS ANNUALLY. BY PAT CRAVEN

BIRTHDAYS AND ANNIVERSARIES are always important. Whether it be your first or 100th, each one is a milestone. It's a chance to stop and look both back and forward. This year marks the 10th anniversary of the Center for Cyber Safety and Education (originally called the (ISC)² Foundation). What an incredible first decade it has been!

The Board of Directors at (ISC)² created the Center in 2011 as a way to support members in their efforts to use their expertise to help make it a safer cyber world through research, scholarships (more than \$1.5 million awarded to date) and education. The Center took (ISC)²'s vision to "Inspire a Safe and Secure Cyber World" and turned it into a call to action, to "Make It a Safer Cyber World." For nearly a decade now, the Center has provided members with the tools and resources necessary to go into their communities and help teach others—including those who are most vulnerable—how to be safe and secure online.

In the first five years, members around the world provided some 10,000 cyber safety lessons annually. In the last five years, that number has grown to 143,000 lessons delivered to children, parents and senior citizens in just one year. Last June, the Center's Board of Trustees approved our first strategic priorities plan that will guide the Center's growth and outreach for the next five years. At the heart of the

10
YEARS
2011-2021



CENTER FOR
CYBER SAFETY
AND EDUCATION™

The only way we can achieve our audacious goal is with an increase in support from members and volunteers from around the world.

plan is a super ambitious yet vital goal: Deliver 1 million cyber safety lessons *annually* by the end of 2025.

To achieve this important milestone in time for our 15th anniversary, we will need to double our reach every year between now and then.

The plan to reach our goal includes creating even more programs to reach a broader audience. We are already working to strengthen members' ability to access the current Safe and Secure Online resources in their native language (we've completed 24 translations so far).

Along similar lines, in 2021, thanks to members in Mexico and

Chile and cybersecurity provider Capa8, you will see the release of our multi-award-winning Garfield's Cyber Safety Adventures program in Spanish, with more languages to come. In addition, thanks to the support of JPMorgan Chase, we plan to release our first ever Safe and Secure Online educational program expressly for small businesses and nonprofits.

The only way we can achieve our audacious goal is with an increase in support from members and volunteers from around the world. The Center staff consists of four of the hardest working and most dedicated people I have ever worked with, but we can't do it alone. We will need more volunteers, more chapters, more schools, more sponsors, more partners and more money to bring it all together.

Over the coming months and years, you will learn of more opportunities to get involved and to give. Visit our website, www.IAmCyberSafe.org, to track progress and learn what role you can plan in this important initiative. What can you do or give to *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.

“There’s this entire invisible ecosystem, and it’s even invisible to most privacy professionals, quite frankly, and it’s somewhat troubling ... that there’s a lot going [on] that the vast majority of us aren’t seeing. As a consequence, it’s the reason why privacy practices are so important and we’re so early in this discipline of data protection.”

—Scott Giordano, Esq., VP & Senior Counsel, Privacy & Compliance, Spirion

Source: (ISC)² Think Tank webinar, “Privacy’s Increasing Role in Cybersecurity – A View from Spirion and the IAPP”

“Being a member of the healthcare cybersecurity profession is not only about business. It is being part of a team that saves human lives and protecting the patients we serve and [ensuring] the delivery of life-saving services.”

—Anastasios Arampatzis, (ISC)² content contributor

Source: (ISC)² [blog post](#)

“Technology is remaking the world, and we will never get the policy right if policymakers get the tech wrong. ... We need people that can speak tech to power.”

—Bruce Schneier, author and security blogger, during opening keynote at (ISC)²'s Security Congress 2020

“More than 70% of U.S. cybersecurity professionals say they are required to have some kind of certification, and the figure is even higher—78%—worldwide.”

—(ISC)² Cybersecurity Workforce Study, 2020

“My prediction is that there will be phishing attacks in 2120. Maybe in the form of a hologram popping up in front of you rather than an email, but they’ll still exist.”

—Graham Cluley, security blogger, researcher and podcaster, during a keynote at (ISC)²'s Security Congress 2020

“[People] make this move to the cloud and they think, ‘Oh, shoot, I’ve got to learn about managing security groups, S3 bucket policies. I’ve got to learn about VPC flow logs and looking for threat signals in my flow logs.’ And they move away from a lot of the core basics and fundamentals that they’re used to, and I’d say that’s actually wrong.”

—Jeremy Snyder, senior director of business development and solution engineering, DivvyCloud
Source: November Cloud Security Insights article “Practical Advice to Harden Multi-Cloud Environments”



(ISC)²

40 Courses
120+ CPE Credits
FREE
Member Benefit

Seeking more accessible ways to keep cybersecurity skills sharp and knowledge refreshed? (ISC)² Professional Development Institute (PDI) has you covered with the flexibility of online, self-paced courses. Dive into our portfolio of 40 online courses – **FREE for (ISC)² members** and available for purchase by non-members. Build skills and earn CPEs, no travel required.

Stay on top of your craft with...

- Express learning courses on emerging topics and trends in 2 hours or less
- Immersive courses covering a variety of cybersecurity and IT security topics
- Lab courses that put specific technical skills to the test

Start FREE Courses

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