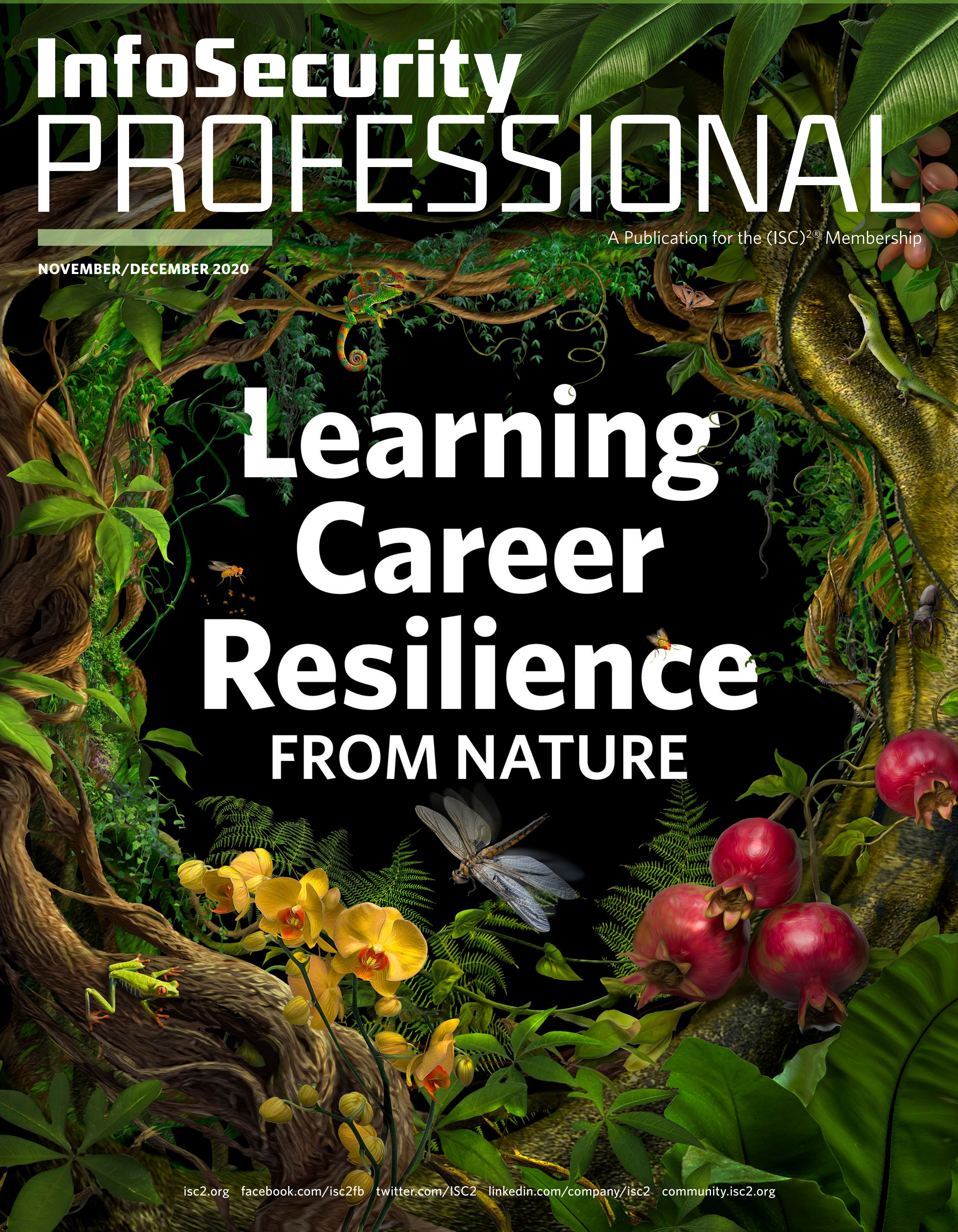
DAVID SHEARER REFLECTS ON HIS TENURE AS (ISC)² CEO

InfoSecurity
PROFESSIONAL

A Publication for the (ISC)²® Membership

NOVEMBER/DECEMBER 2020



Learning Career Resilience FROM NATURE

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

CCSP®

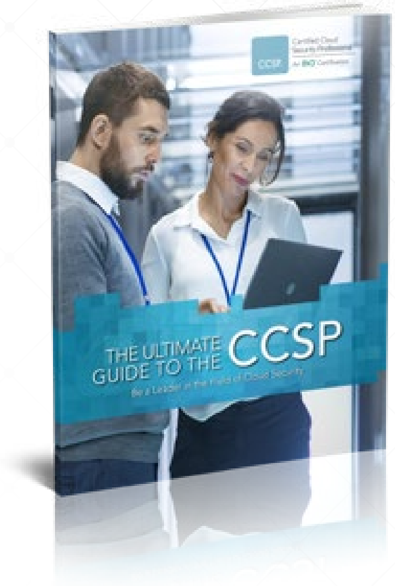
Certified Cloud Security Professional

An (ISC)² Certification

EXPAND

Your Skill Set with the CCSP

Cloud security is the top needed skill in the field. Prove you're at the forefront with Certified Cloud Security Professional (CCSP) certification. Considered the industry's premier cloud security credential, it shows you have the advanced technical skills and knowledge organizations around the globe demand.


CCSP
Certified Cloud Security Professional
An (ISC)² Certification
THE ULTIMATE GUIDE TO THE CCSP
Be a Leader in the Field of Cloud Security

Now's the time. Download the Ultimate Guide to the CCSP to see how this leading credential can expand your skill set and differentiate you as a globally respected security leader.

Ready to expand your skill set?

GET YOUR GUIDE

contents

VOLUME 13 • ISSUE 6

"CULTURE EATS STRATEGY FOR BREAKFAST"
- Peter Drucker
Did you forget something?
Yeah. We all did.

PAGE 31

features

Cover image: MARK FREDRICKSON Illustration above: TAYLOR CALLERY

departments

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.

editor's note | *by Anne Saita*

Survival of the Fittest

A WOMAN I KNOW constantly [mis]uses the term "survival of the fittest" to help explain victims of this year's pandemic. While it's true those weakened by age and disease are more apt to suffer severe consequences upon contracting COVID-19, there also are many younger and seemingly healthy humans who've succumbed to the coronavirus. And let's not forget the millions who lost jobs through no fault of their own.

The biggest determinant of survival in general is less about lifestyle choices and the advance of time than about one's ability to adapt, sometimes rapidly, to circumstances. The most adept at changing are those Charles Darwin considered the fittest—that is, those most likely to evolve rather than become extinct. Certainly, being of sound mind and body is preferable, but you don't need to have a high IQ, lift heavy weights, run really fast or tune in to some inspirational channel to thrive when times get tough. Instead, you need to sense change, anticipate setbacks and seize opportunities.

In this issue, we examine career resilience through a similar lens to show why a diverse set of skills is now required, not just nice to have; why lifelong learning means more than keeping up with CPEs; and why cybersecurity professionals should always prepare to pivot.

We also offer a different take on cybersecurity resource allocations since there's a good chance your company or industry took a financial hit this year, while cybercriminals certainly did not. And, we finish out our serial with the IT team at Acme Corporation realizing their security awareness training is doomed if they don't do one more thing.

There's always going to be one more thing to do if we're to collectively survive whatever the 2020s throw at us. But, by becoming as "fit" as possible, we can do it.

See you in the new year. ■

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

©Rob Andrew Photography

InfoSecurity PROFESSIONAL

(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

EVENTS AND MEMBER PROGRAMS MANAGER
Tammy Muhtadi
727-493-4481
tmuhtadi@isc2.org

TWIRLING TIGER MEDIA MAGAZINE TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

EDITORIAL ADVISORY BOARD

Brian Alberti, (ISC)²
Anita Bateman, U.S.
Jarred LeFebvre, (ISC)²
Yves Le Roux, EMEA
Cesar Olivera, Brazil and Canada

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

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

CISSP®

Certified Information
Systems Security Professional

An (ISC)² Certification

STRONG

Stronger Cybersecurity Starts with CISSP

Advocate for strength in your organization. Those at the forefront of cybersecurity know people play a vital role in keeping the organization safe. While we may not be able to stop every threat, there's plenty we can do to fortify defenses. And the surest path to stronger cybersecurity starts with a team that is CISSP trained and certified.

CISSP certification arms every team member with all it takes to design, engineer, implement and run a first-rate information security program. But it doesn't end there… (ISC)² membership also means your colleagues are armed with professional development opportunities and connections to help them — and your organization — stay a step ahead.

(ISC)²

Why It Is Important to Have Qualified Cybersecurity Professionals On Your Team

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.

GET YOUR GUIDE

It's Always Been an Adventure

by David Shearer, CISSP

MY TIME AT (ISC)² has been one adventure after another. From driving my family in an RV from high-altitude Colorado to highly humid Florida—during a blizzard, no less—to having a new boss almost every year and trying to satisfy 13 board members, to clearly conveying to a global membership how hard we worked on its behalf—this job was never dull.

Perhaps it's the musician in me, but I've always enjoyed the creative side of (ISC)². I pushed very hard to take the company in a much more visual direction regarding in-house studio capabilities, professional-grade commercials and product positioning.

Of course, many of these initiatives were born during one of my "managing-by-walking-around" sessions (a.k.a. Dave's drive-bys), where I typically planted a seed with our creative staff only to see them, time and time again, exceed my expectations.

- We completed our multi-year, multi-million-dollar digital transformation on time and under budget.
- We rolled out the Professional Development Institute in 2019 just in time to provide rich CPE opportunities free to members and for a fee to non-members during the COVID-19 pandemic.
- We grew the membership and enhanced the company's finances.

The Global Achievement Awards program (formerly the ISLAs) has always been one of my favorite parts of the job. Recognizing the great social impact our members around the world are making should instill pride in all of us. We also hired a strong team to lead our Center for Cyber Safety and Education with great results from our Garfield's Cyber Safety Adventures program and a scholarship program that has awarded well over $1 million to deserving men and women pursuing cybersecurity careers.

David Shearer, CISSP, is the outgoing CEO at (ISC)².

As my tenure as CEO comes to a close, I walk away proud that I can honestly say I left the organization in better shape than I found it. I feel I left it all on the field, if you will. Clearly that was my job, but that doesn't always happen.

I could not have done it without the wildly talented and dedicated (ISC)² management team and staff. I asked a lot of everyone working at (ISC)²—and they met the challenge time and again. I thank everyone I worked with over the years on the board, the management team and the staff for trusting me and putting up with my around-the-clock requests and pace of work.

I thank everyone I worked with over the years on the board, the management team and the staff for trusting me and putting up with my around-the-clock requests and pace of work.

I also want to thank the (ISC)² membership, especially those who have been and remain patient with us as we continue to enhance the association's operations and value proposition. Special thanks go to all of our business partners and supporters around the world. I've met so many remarkable people during my international travels.

Lastly, I owe the biggest thanks to my wife, Mia, for her unwavering support and patience as I spent lots of time on the road and away from home. My hope is that we both get many healthy years to catch up.

My best to everyone reading this. Keep inspiring a safe and secure cyber world. Stay well. ■

RETURN TO CONTENTS

2020
Cybersecurity INSIDERS
CLOUD SECURITY REPORT
(ISC)²

field notes

EDITED BY DEBORAH JOHNSON

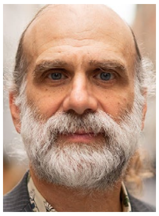
A ROUNDUP OF WHAT'S HAPPENING IN (ISC)² COMMUNITIES

Annual Conference Keynotes are a Who's Who of Security Luminaries

THIS MONTH'S virtual (ISC)² Security Congress will feature some familiar names as keynotes to launch each day of sessions. These renowned security professionals include a best-selling author, a researcher and a former Assistant Secretary at the Department of Homeland Security who is no stranger to the Security Congress main stage. There's still time to register for a pass if you haven't already.

Monday, November 16

Bruce Schneier



Dubbed a "security guru" by *The Economist*, Bruce Schneier is an internationally acclaimed security technologist and best-selling author of more than a dozen books—including his latest, *Click Here to Kill Everybody*, exploring the risks and implications of our new, hyper-connected era. He works at the intersection of security, technology and people, and has penned hundreds of articles, essays and academic papers on these topics. His blog, Schneier on Security, is followed by 250,000 readers.

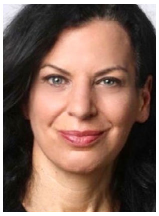
Tuesday, November 17

Graham Cluley

Graham Cluley is an award-winning independent security blogger, researcher, podcaster and public speaker. He has been a well-known figure in the computer security industry since the early 1990s and held senior roles at companies such as Sophos and McAfee before becoming one of the most popular British security bloggers. He was inducted into the InfoSecurity Europe Hall of Fame in 2011.

Wednesday, November 18

Juliette Kayyem



Juliette Kayyem has spent the last two decades in both state and federal government managing complex policy initiatives and organizing government responses to major crises. She currently lectures in international security at Harvard University's Kennedy School of Government, where she is faculty chair of the Homeland Security and Security and Global Health Projects. Previously, she served as President Barack Obama's Assistant Secretary at the Department of Homeland Security, where she played a pivotal role in responses to the BP Oil Spill and H1N1 pandemic. ■

Clar Rosso Joins (ISC)² as New CEO

Clar (pronounced "Claire") Rosso is (ISC)²'s new chief executive officer, taking over the helm from David Shearer, CISSP, on Oct. 1. As planned, Shearer will finish the year out as an advisor to the Board of Directors in order to ensure a smooth transition.

"It is a great privilege to join (ISC)² and lead this prestigious association," Rosso said in a prepared statement. "There is so much opportunity to continue growing the profession, striving to realize the association's vision of a safe and secure cyber world, and ensuring that cybersecurity is a rewarding and welcoming career to a diversity of people globally."

> "It is a great privilege to join (ISC)² and lead this prestigious association."

Rosso has more than two decades of experience helping professional associations and certifying bodies grow and strengthen member value. Prior to joining (ISC)², she worked as a senior executive for the American Institute of Certified Public Accountants and CIMA.

She earned a master's degree from San Francisco State University and a bachelor's degree from the University of California, Davis. ■

RETURN TO CONTENTS

MEMBER'S CORNER

Examining a Costa Rican PCI Data Breach

BY RODRIGO CALVO, CISSP, PCIP

TWO MONTHS INTO THE COVID-19 PANDEMIC, the Costa Rican public bank Banco de Costa Rica (BCR) learned it had a disaster on its hands. A cyber gang known as the Maze Team publicly claimed credit for leaking payment card data—the majority of it belonging to BCR.

BCR appeared to take a big hit. The Costa Rica Department of Commerce reported that as of January 2020, banks collectively had issued 5,557,606 payment cards. With a national population of 5 million, that's more than one card for every citizen. And according to *E&N Magazine*, in 2017, BCR ranked third in assets among financial institutions throughout Central America.

The Maze Team was known for using ransomware to fund its criminal operations prior to December 2019. Then members turned to "fear-as-a-service," where they threatened to release illegally obtained data unless they received a fixed amount of money, also known as exposure extortion. In late April, a website called Maze News posted several statements about payment card transaction leaks at BCR. The cybercrime organization had attacked the victim bank months prior without anyone noticing.

As (ISC)² members, we must act honorably, honestly, justly, responsibly and legally. As a result, the following analysis is based on my own research and processing of four files published by the Maze Team, as well as news articles and BCR social media statements. The analysis focuses on four areas:

- Communications
- Value of exposed data
- Technical assumptions
- Recommendations

WHAT WAS STOLEN?

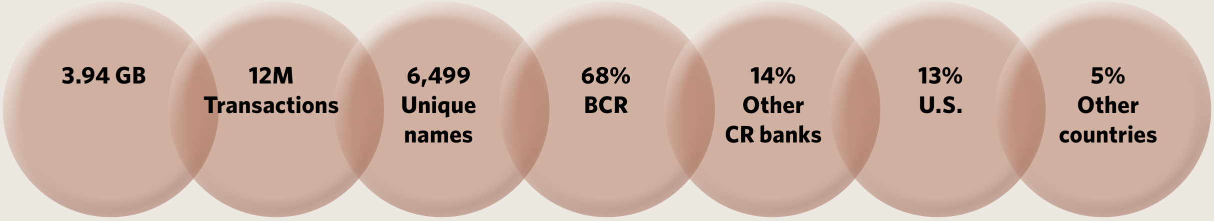
The stolen data primarily belonged to BCR, but it also contained a small percentage from other banks and countries. At risk of public exposure were payment card transactions, cardholders' names, primary account numbers (PCI PAN) and a virtual infrastructure report. *(See Figure 1, below.)*

COMMUNICATION ANALYSIS

Maze refers to its victims as "clients" and issues press

Figure 1

COMPOSITION OF DATA LEAKAGE AND SUMMARY OF THE EXFILTRATED FILES



database.csv

- Size: 123kb
- Payment card transactions
- 47 unique PAN
- March to April 2019

banco.xlsx

- Size: 212kb
- RV tools report
- Full VCenter report
- IPs, VMWare licenses and other information

en18.csv

- Size: 2.02 GB
- Payment card transactions
- 5,198 unique cardholder names
- January 2018

feb18.csv

- Size: 1.92 GB
- Payment card transactions
- 5,595 unique cardholder names
- February 2018

RETURN TO CONTENTS

releases to raise public awareness of stolen data. The tone of this news release suggested Maze was the good guy and BCR was in the wrong. Legitimate news media expected more clarity once BCR public relations released its own communications.

Among my other observations:

- Once the breach was made public, an independent company publicized information without authorization from BCR for customers to check the status of their accounts. Within just a few days, other third parties started to run similar initiatives, exacerbating the breach.
- Social media broadcast "panic episodes" around BCR security, given the magnitude of the breach and potential damage to credit card holders. However, due to more pressing COVID-19 coverage, the breach was a secondary concern.
- It took 24 days between Maze's initial warning for BCR to publicly confirm the data leakage.

VALUE OF EXPOSED DATA

Payment data stolen involved transactions between January and February 2018.

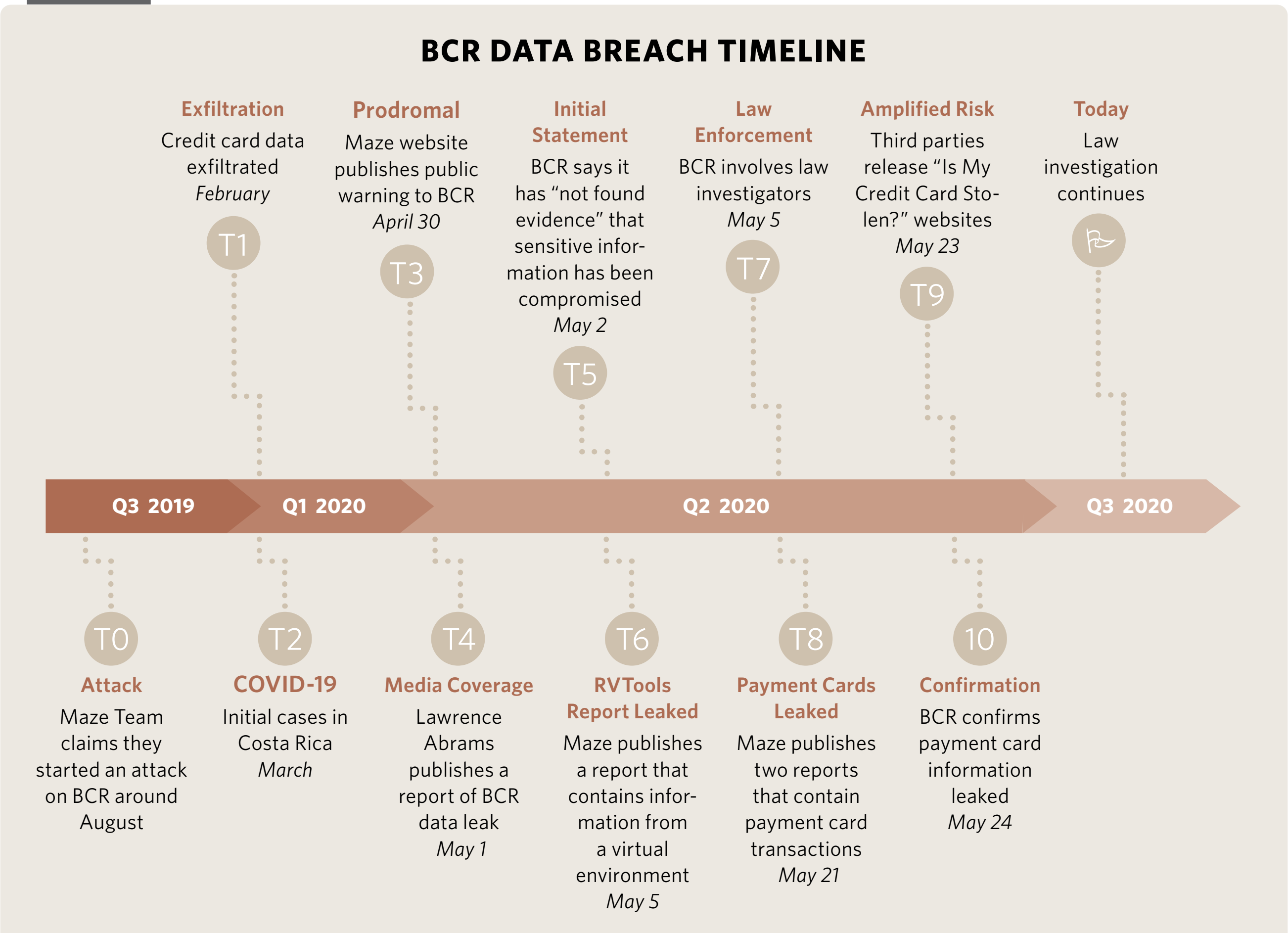
The potential dark market value was limited due to:

- Expired credit cards (the expiration average is three years)
- Credit cards' migration from traditional magnetic strip to an EMV chip or contactless technologies due to be complete by November 2020

What may surprise some members living in more heavily regulated areas is that in Costa Rica there is no direct fine from the General Superintendent of Financial Institutions for this kind of situation. BCR could easily manage a small number of active compromised credit cards, and for little cost. Replacing cards for each impacted card holder amounted to about US$10.

On May 24, 2020, BCR publicly offered to replace customers' credit or debit cards at no cost to minimize

Figure 2



BCR DATA BREACH TIMELINE

T0 **Attack** Maze Team claims they started an attack on BCR around August

T1 **Exfiltration** Credit card data exfiltrated *February*

T2 **COVID-19** Initial cases in Costa Rica *March*

T3 **Prodromal** Maze website publishes public warning to BCR *April 30*

T4 **Media Coverage** Lawrence Abrams publishes a report of BCR data leak *May 1*

T5 **Initial Statement** BCR says it has "not found evidence" that sensitive information has been compromised *May 2*

T6 **RVTools Report Leaked** Maze publishes a report that contains information from a virtual environment *May 5*

T7 **Law Enforcement** BCR involves law investigators *May 5*

T8 **Payment Cards Leaked** Maze publishes two reports that contain payment card transactions *May 21*

T9 **Amplified Risk** Third parties release "Is My Credit Card Stolen?" websites *May 23*

10 **Confirmation** BCR confirms payment card information leaked *May 24*

Today Law investigation continues

RETURN TO CONTENTS

damage to their accounts. Three months later, there is no public information regarding probes into the real losses for the bank's customers. *(See Figure 2, p. 10.)*

TECHNICAL ASSUMPTIONS

The naming convention of the exfiltrated payment card transaction files suggests that they were created locally in Costa Rica (banco.xlsx, en18.csv, feb18.csv are words in Spanish, translating to bank, January, February). If the cyber thieves were a group fully operating from outside, 90% of the acronyms would be expected to be in English.

A file with information from a virtual environment was obtained from running the tool known as RVTool showing:

- A VMWare environment
- IPs from 62 virtual machines
- OS versions
- VMWare licenses (from those, it can be installed to a new vCenter server)
- An identified IP range suggesting a DMZ deployment
- The exfiltrated VMWare infrastructure with a limited overview that cannot be used to confirm that it is used for an internal production network.

The RVtool requires to run the following parameters:

- IP address or FQDN of the vCenter server
- A username and password (at least with read-only rights)

If BCR keeps logs for at least nine months, potentially it could track which users triggered a complete report from VMWare. There appears to be two options for this particular exfiltration: network and endpoint. In doing so, the cardholder name column required processing and removal of duplicated values; by default, values were not visible.

Publicly available evidence suggests the existence of multiple payment brands, but BCR appeared to have agreements with just two brands, so it is possible a third-party payment processing company was susceptible to attack and was used as an initial entry point for the malicious hack.

Remnants of a solid state drive (SSD) destroyed in an SEM disintegrator. Final particle size is 2mm, as recommended by the NSA.

RETURN TO CONTENTS

Remember the three C's of trust—competence, character and caring, according to author and public relations expert Michael D. Matthews.

RECOMMENDATIONS

Regardless of an (ISC)^2 member's location or industry, here are some suggestions to prevent your organization from becoming the next BCR.

- Gain full visibility of your data, including customer and IT infrastructure information.
- Apply a data loss prevention (DLP) program based on a conscious data assessment process to determine the utilization and criticality of the information throughout the entire company.
- Make sure that your DLP technology covers all egress points (including a DMZ).
- Encrypt the hard drive on laptops.
- Block an endpoint's ability to copy to external resources information from customer and IT infrastructure.
- Follow up logged DLP incidents and handle properly.
- If you don't have a specialized team, evaluate managed DLP services from well-known providers.

Remember the three C's of trust—competence, character and caring, according to author and public relations expert Michael D. Matthews. The more that you deny and delay a response, the more your corporate image will be damaged. ■

RODRIGO CALVO, *CISSP, PCIP, is a senior security architect at Infolock. He can be reached at* rcalvo@infolock.com.

RETURN TO CONTENTS

Recognizing Outstanding Work Around the World

CONGRATULATIONS to the following security professionals being recognized as Global Achievement Award winners. (The awards were formerly known as the ISLAs.) 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 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 2020 honorees:

North America: **Jack Freund**, CISSP, CISSP-ISSMP, head of cyber risk methodology at Cyber Assessments, Inc., for his work with the NIST Applied Cybersecurity Division on behalf of the nonprofit FAIR Institute to map together the NIST CSF Risk Assessment and the Risk Management Strategy domains to the OpenGroup's FAIR risk taxonomy and risk analysis standards.

Asia-Pacific: **Troy Hunt**, founder, Have I Been Pwned?, for adding new APIs to his website, which allows internet users to check whether their personal data has been compromised. The site has nearly 3 million active email subscribers and contains records of almost 8 billion accounts.

EMEA: **Dr. Katalin Szenes**, CISSP, security and audit consultant, contributed to the establishment of the security specialization at Obuda University in Hungary, and educates IT professionals in that country on cybersecurity.

(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 2020 honorees:

North America: **Lt. Kim Do**, CISSP, information systems and communications officer for the U.S. Navy, who collaborated with Naval Surface Forces Pacific and Navy Information Warfare Pacific on a groundbreaking initiative for network scanning aboard surface ships that resulted in measurable improvements to her ship's vulnerability management program, which senior officers believe could be scaled to the entire fleet.

Asia-Pacific: **Dongyoung Roh**, senior researcher at the Affiliated Institute of Electronics and Telecommunications Research Institute, for development and standardization of cryptographic algorithms, a key technology for data security in the Fourth Industrial Revolution.

(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 2020 honoree:

Katia Dean, system engineer, AnaVation LLC and founder, Katia's

RETURN TO CONTENTS

WITH HUNDREDS of nominations across the entire program, our Award Committees have been impressed with the outstanding leadership, volunteerism, diversity and sharing of knowledge that this group has presented. We are proud of all of the nominees' work and look forward to growing this program throughout the years to recognize the best of the best.

Cylife, from North America. Dean created a website to help people understand the field of cybersecurity and provide educational content, while also connecting them with job opportunities in the profession.

(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 2020 honorees:

North America: **Darcy Saint-Amant**, CISSP, Colonel, U.S. Army, who helped to create a collaborative, U.S. Department of Defense (DoD)-wide community of interest and drafted a DoD Zero Trust Cybersecurity Strategy while building consensus to shift from a network-centric to a data-centric paradigm.

EMEA: **Yuval Segev**, director, audit and methodology, Israel National Cyber Directorate, who implemented a national IT system that enables organizations in the Israeli economic market to anonymously review the state of their information security and controls.

(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 2020 were hand-selected by the (ISC)^2 Board of Directors.

The (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.

2020 Recipient: **Yves Le Roux**, CISSP, from France. Le Roux is a security and privacy expert who has spent five decades in information and network security, standardization, privacy, compliance and risk.

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.

2020 Recipient: **Bonnie Butlin**, co-founder and executive director of the Security Partners' Forum (SPF), who resides in Canada. Under the SPF banner, Butlin created the Women in Security and Resilience Alliance (WISECRA), which engages a growing network of women in security and resilience associations/groups globally, and also serves as an Expert Network Member in Cybersecurity with the World Economic Forum.

The James R. Wade Service Award

is awarded by the (ISC)^2 Board of Directors to acknowledge the involvement of those volunteers who merit special distinction for their sustained and valuable service to (ISC)^2.

This year's honoree is **Hymavathi Pandyaram**, an identity management specialist with Nulli – Identity Management in Canada and an active member of the (ISC)^2 Alberta Chapter in the Edmonton community, who shares her knowledge of cybersecurity and makes an extensive effort to educate seniors, children and their parents, as well as small firms, about safe internet practices.

The (ISC)^2 Diversity Award

honors an individual who represents the core values of (ISC)^2 through

RETURN TO CONTENTS

significant contributions in driving a more diverse workforce in the cybersecurity community.

2020 Recipient: **Kristin Paget**, who currently resides in the U.S. Paget is a transgender woman who has continually promoted and represented diversity through her positions as "Hacker Princess" in the security departments of several leading technology companies, including Apple, Tesla, Lyft and, currently, Intel.

The (ISC)² CEO Award

The (ISC)² CEO Award recognizes members who have made a significant impact on the cybersecurity community through dedicated and exceptional volunteer efforts. Nominations are made solely by (ISC)² Board members and executive staff. As selected by outgoing CEO David Shearer, the 2020 recipients are:

Yves Le Roux, CISSP, security and privacy expert, for his deep dedication to helping grow (ISC)² across the EMEA region.

James Packer, CISSP, CCSP, head of cybersecurity, EF Education First, for his volunteerism and support of the cybersecurity industry, including as president of the (ISC)² London Chapter and as the current chair of the (ISC)² Chapter Advisory Council.

The (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 2020 recipients in each region:

Patrick Thompson, president of (ISC)² Northern Virginia Chapter

North America: **Northern Virginia Chapter** – The chapter leveraged its geographical region throughout 2019 to build strong relationships with organizations, universities and programs to educate the local community on cybersecurity, including partnering with the Center for Cyber Safety and Education to promote online safety to over 100 local children through the Garfield's Cyber Safety Adventures program at local schools.

R. Vittal Raj, CISSP, president of (ISC)² Chennai, India Chapter

Asia-Pacific: **Chennai, India Chapter** – As one of (ISC)²'s longest-standing chapters, it held several joint programming events in 2019 with other security professional organizations to create visibility amongst targeted interest groups, with the goal of encouraging others to take a proactive role in inspiring a more safe and secure cyber world through education, certification and networking.

(ISC)² Nigeria Chapter members

EMEA: **Nigeria Chapter** – The group not only hosted regular educational meetings, it also celebrated Cyber Security Awareness Month (Be Cyber Conscious) by presenting weekly webinars and hosting a national conference just three months after its official formation, which consisted of speaker presentations and panel discussions.

(ISC)² Peru Chapter members

LATAM: **Peru Chapter** – With 76% of its members without certification, the chapter has the unique opportunity to engage security professionals and showcase the importance of gaining their certification and hosts an average of 11 meetings per year.

CENTER FOR CYBER SAFETY AND EDUCATION AWARDS

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

This award is named after Julie Peeler Franz, who was the first director of the (ISC)² Foundation, now known as the Center for Cyber Safety and Education. Julie was an extremely effective spokeswoman whose

RETURN TO CONTENTS

passion was to build an educational program that would teach parents, seniors and, especially, children how to be safe and secure online. Within a conversation about the center's educational programs, she would remind everyone: "It's for the children."

Recipient: **Greg Thompson**, CISSP, Vice President and Chief Information Security Officer at Manulife Financial. Thompson has extensive experience in industries ranging from telecommunications to financial services and participates in industry forums. He currently chairs the Board of Trustees for the Center for Cyber Safety and Education and is the former vice chair of the (ISC)² Board of Directors, as well as a current board member the Canadian Cyber Threat Exchange.

Center for Cyber Safety and Education – 2020 Partner of the Year Award

aws

Recipient:
Amazon Web Services (AWS)
AWS began working with the Center for Cyber Safety and Education in 2019, sponsoring and participating in the first Cyber Safety Day in Orlando. Since then, the AWS team has helped the Center expand its award-winning programs beyond school campuses and into homes and virtual classrooms around the world. As a world leader in cloud services, AWS is committed to the cyber safety of children, parents and senior citizens and serves as a model for individuals and businesses who want to make it a safer cyber world. ■

(ISC)² Salutes the 2020 Cybersecurity Scholarship Recipients

(ISC)²® CENTER FOR CYBER SAFETY AND EDUCATION™

(ISC)² JOINS THE CENTER FOR CYBER SAFETY AND EDUCATION in congratulating the outstanding men and women who earned cybersecurity scholarships in 2020. With the generous support of sponsors including (ISC)², SAIC, Raytheon, KnowBe4 and others, the Center is proud to assist these hardworking and dedicated students as they prepare to help meet the critical demand for skilled cybersecurity professionals.

More than $200,000 in tuition/fee scholarships and (ISC)² certification education scholarships were awarded in 2020. The 2021 scholarship program will accept applications from Nov. 16 to Feb. 22, 2021. For more information go to www.IAmCyberSafe.org/scholarships.

WOMEN SCHOLARSHIP RECIPIENTS

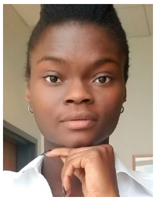
Romy Minko
Australia - University of Oxford

Annabelle Klosterman
U.S. - Dakota State University

Charity Pulliam
U.S. - Johns Hopkins University

Freya Archuleta
U.S. - Virginia Polytechnic Institute and State University

Favour Emeakama
Nigeria - Concordia University in Canada



"It is wonderful to be a recipient of this scholarship again this year. I am delighted to be a part of this movement of empowerment. Thank you for this opportunity to finish my education."

Naurin Farooq Khan
Pakistan – Riphah International University

Kittson Hamill
U.S. - University of Alabama

Olivia Galluci
U.S. - Rochester Institute of Technology

KnowBe4 Women in Cybersecurity Scholarship

Rachel Paul
U.S. – George Mason University

"Being awarded this cybersecurity scholarship by the Center for Cyber Safety and Education is monumental for me. This generous scholarship has provided me with the opportunity to continue my studies in cybersecurity, which I am so ecstatic to pursue as a career. Furthering my education is crucial to me when it comes to making a difference in the infosec world."

RETURN TO CONTENTS

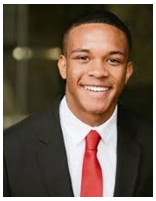
Raytheon Women's CCDC Scholarship

Caroline Linkus
U.S. – University of Virginia

"I am so grateful to have received the 2020 Raytheon CCDC Women's Cybersecurity Scholarship. This scholarship will give me the opportunity to continue to pursue my cybersecurity education at the University of Virginia. I am hopeful that I will also be able to help ignite an interest and a passion for cybersecurity in other women who may not have considered it before."

UNDERGRADUATE SCHOLARSHIP RECIPIENTS

Brandon Staple
U.S. - University of Colorado



"It is with the highest gratitude and honor that I write to extend my overwhelming appreciation to you and your great organization for this prestigious scholarship. This scholarship means a great deal because it has given me the unique opportunity to follow my dream of becoming a cybersecurity scientist."

Megan Connolly-Young
United Kingdom – Queen's University Belfast

Sara Takhim
U.S. - Northeastern University

Chase Heim
U.S. - University of Wisconsin-Stout

Terez Daniel
U.S. - Georgia Southern University

Vy Nghe
U.S. - University of Denver

Zion Basque
U.S. - Arizona State University

Raquel Reyes
U.S. - University of Southern California

Jonathon Negron
U.S. - Johns Hopkins University Whiting School of Engineering

Jasmine Cairns
U.S. – Stevens Institute of Technology

Austyn Gerzevske
U.S. - Illinois Institute of Technology

Sadie Levy
U.S. - Northeastern University

Samina Mondal
U.S. - Marymount University

Steven Seiden
U.S. - Louisiana State University

Logan O'Neal
U.S. - University of Tennessee

Aaron Esau
U.S. - Oregon State University

Robert Province
U.S. - University of Colorado, Colorado Springs

Bill Demirkapi
Germany - Rochester Institute of Technology

Fardeen Bhimani
U.S. - United States Air Force Academy

Sloane Miller
U.S. - North Carolina Agricultural and Technical State University

Kyla Guru
U.S. - Stanford University

Austin Grupposo
U.S. - Champlain College

GRADUATE SCHOLARSHIP RECIPIENTS

Ali Hasan Adnan Khajan
India – Carnegie Mellon University

"Thank you so much for all your contributions towards my development and I am inspired to help out others when I become capable enough of doing so in the manner the (ISC)^2 has aided countless individuals over the years."

Vy Nguyen
Vietnam – University of Pennsylvania

Michael Steckler
U.S. – University of California, Berkeley

Anusha Penumacha
India - Carnegie Mellon University

Abiodun Esther Omolara
Malaysia - Universiti Sains Malaysia

Scarlett Levine
U.S. - John Jay College of Criminal Justice

Muhammad Aamir
Pakistan - Shaheed Zulfikar Ali Bhutto Institute of Science & Technology (SZABIST)

Jonah Burgess
Northern Ireland - Queen's University Belfast

Collins Bunde
Kenya - Strathmore University

Katherine Hutton
U.S. - George Washington University

Christine Anari
Kenya - University of Derby

Marylyn Harris
U.S. - Nova Southeastern University

Jean Michel Armand
Rwanda - Dakota State University

Stuart Millar
United Kingdom - Queen's University Belfast

Ranjita Pai Kasturi
India - Georgia Institute of Technology

Jessica Gottsleben
U.S. - Salve Regina University

Kathleen Bodi
U.S. - University of Phoenix

Djerhkea Epps Dukes
U.S. - Norwich University Northfield

Ijeoma Olawale
Nigeria - University of Colorado, Colorado Springs

Mingxuan Yao
China - Georgia Institute of Technology

Will Fair
U.S. - Marymount University ■

RETURN TO CONTENTS

InfoSecurity Professional Earns International Recognition

EMERGING TECHNOLOGY

What's the RUSH?

BLOCKCHAIN

Is your company considering adopting the technology this year? Then let's be sure you understand what it is, what it isn't and what it means for security and privacy.

BY TUAN PHAN, CISSP

ETHICS

DO TELL

Fuzzy ethical guidelines can lead to a breakdown in protecting data

BY CATHERINE KOZAK AND BARRY DOWELL, CISSP

For the fourth year in a row, *InfoSecurity Professional* earned editorial recognition in technical writing from the Trade Association Business Publications International. The January/February cover story by Tuan Phan, CISSP, on blockchain earned a bronze in the highly competitive category. Another feature, on information security ethics, co-written by Cate Kozak and Barry Dowell, CISSP, placed among the top 25 features in the competition.

Congratulations to the authors and everyone on the editorial and design teams for their outstanding work. ■

READ. QUIZ. EARN.

Earn Two CPEs for Reading This Issue

Please note that (ISC)^2 submits CPEs for (ISC)^2's *InfoSecurity Professional* magazine on your behalf within five business days. This will automatically assign you two Group A CPEs.

Note: To access this members-only platform and quiz, you'll need a Blue Sky account.

If you don't have an account, go to the Blue Sky home page via the link and click on "Create User Profile" in the upper right-hand corner.

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&PCAT=7777&CAT=10853

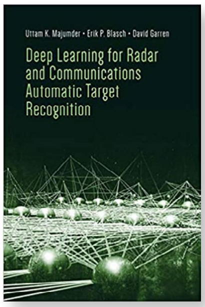
RECOMMENDED READING

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

Deep Learning for Radar and Communications Automatic Target Recognition

BY UTTAM K. MAJUMDER, ERIK P. BLASCH AND DAVID A. GARREN

(Artech House, July 2020)



Uttam K. Majumder • Erik P. Blasch • David Garren

Deep Learning for Radar and Communications Automatic Target Recognition

IN THESE DAYS OF THE INTERNET OF THINGS (IoT), security professionals are concerned about the vulnerabilities of devices that are connected using radio or smart chips. Also of concern is the use of machine learning (ML) and artificial intelligence (AI) for data exploitation, such as determining radio frequency signals and collecting data and images. A predecessor of this technology was used by the Defense Department to target moving and stationary objects. Deep learning enables ingesting large quantities of data and generating models and assumptions based on targets, environments, variables and other sensors.

Authors Majumder, Blasch and Garren present a broad overview of the concepts and approaches that are relevant to today's radar and communication systems along with its taxonomy, as well as specific information on ML algorithms. The application of AI or ML to large datasets is crucial to the development of autonomous cars and IoT medical devices such as pacemakers, along with radar imaging for air traffic, including the detection of objects and trajectories. The security implications of such technology are significant. The authors provide examples, such as an attacker using AI or MI to avoid detection, recognition or identification.

The use of AI, ML and deep learning is covered in sufficient detail that a novice will enjoy learning about these technologies.

The authors demonstrate how the algorithms of ML and deep learning permit the programs to "train themselves" based on rules to perform tasks over vast amounts of data. They also present some of the latest research topics on neuromorphic computing and energy-efficient computing for AI applications.

The use of AI, ML and deep learning is covered in sufficient detail that a novice will enjoy learning about these technologies. The authors briefly skirt the topic of white-box and black-box testing. I would like the authors to describe in more detail how enterprises can use AI and ML to defend the perimeter from insider threats using this technology. They might want to have sessions with firms developing applications using various threat models, such as MITRE ATT&CK, which are being built on AI, ML and deep learning.

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.

RETURN TO CONTENTS

Using a Crisis Wisely

Upskilling in times of uncertainty and change is a prudent career decision

BY TONY VIZZA, CISSP, CCSP

THE SAYING "everything happens for a reason" is often invoked as a message of support during times of hardship or adversity. While it may be difficult to apply to a crisis on the scale and impact of the COVID-19 pandemic, the resiliency that we as individuals develop during such difficult times can make us stronger and better prepared for whatever comes next.

A crisis comes with danger, but it also comes with opportunities. While the tourism, travel and retail sectors have been devastated by the global economic crisis, tech companies such as Apple, Amazon, Microsoft and Alphabet (parent of Google) are now all "tera-cap" companies—worth more than US$1 trillion each, with Apple worth more than US$2 trillion. That's not all. The digital transformation imposed on people and organizations worldwide has, almost overnight, precipitated the rise of such companies as Zoom, which have become the de facto standard in video calls—so much so that in a few (rather long) months, the phrase "to Zoom" has entered the vernacular the same way "to Google" has.

Multi-billion-dollar companies have the almost limitless set of resources to ideate and design think their way out of even global crises. Yet, if you distill the critical success factors, all that these companies have done is make the most of new opportunities at hand, pivot their operations to optimize the current environment and accept that they have to operate differently. As Charles Darwin famously said, "It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to change." If this axiom rings true for the largest and most successful companies in the world today, the same must be true in our own daily and professional lives.

Tony Vizza, CISSP, CCSP, is the Director of Cybersecurity Advocacy for (ISC)²'s Asia-Pacific region and is based in Sydney. He can be reached at tvizza@isc2.org.

Recognizing this, how can we as cybersecurity professionals apply the concept of adaptability and change to our own careers and ensure that we remain relevant in our knowledge, coveted for our experience and sought after for our abilities? Like Zoom, there are other boom industries that have flourished because of COVID-19. The cybersecurity skills gap that existed prior to the pandemic has arguably become even more critical given the rapid shift to remote work. We have also seen boom areas emerge outside of cybersecurity in areas like cloud services and healthcare IT.

What can we as professionals do to make ourselves even more relevant in a job market that needs new expertise? How can we make an even bigger impact on the organizations that employ us while at the same time improving our earnings and growth? The answer, of course, is to upskill in key areas.

There is a reason the CCSP is the fastest growing certification at (ISC)², with existing CISSP holders making use of the single annual maintenance fee to extend their already deep understanding of cybersecurity by also certifying in cloud security. Similarly, workers in the IT space who see the opportunity in cybersecurity are choosing to become SSCP-certified. Meanwhile, IT staff around the world who work for healthcare organizations are seeing the value of the HCISPP certification to help them better perform their duties.

I have found that the current COVID-19 crisis is an optimal time to gauge where future opportunities arise and to make the most of upskilling. I have chosen to take advantage of it. I encourage you to do likewise. ■

Photograph: Getty Images

RETURN TO CONTENTS

ARM YOUR TEAM
to Secure the Enterprise

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

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

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

Prepare for Tomorrow's Threats Today!

Get the FREE eBook

Evolution vs. Extinction

What cybersecurity professionals could learn from nature to build a more resilient career

BY CATHERINE KOZAK

MINUSCULE FRUIT FLIES have been doing their thing for 40 million years, somehow managing for millennia in southern Africa on a diet of marula fruit. After a fateful meetup about 10,000 years ago with multiple-fruit-loving humans, the insect promptly started evolving to the non-fussy generalist we know today.

"Their offspring then colonized the world," Marcus Stensmyr, senior lecturer at Lund University in Sweden, says in a 2018 news statement about his research. "It's actually quite awesome."

Although the humble fruit fly may not be awe-inspiring beyond the science laboratory, its very existence offers a valuable lesson on how to build a resilient cybersecurity career: Diversify. Seize opportunities. Adapt. Evolve. Have a back-up plan.

Faced with the multiple shocks of 2019-2020—the political divide, the pandemic, nations' reckonings with race and gender, the economic shutdown, not to mention a series of raging wildfires and vicious storms—it would behoove cybersecurity professionals to remember that we're all subject to the same internal and external environmental forces. Unless you're a crocodile, staying put and doing the same thing when under duress is rarely rewarded by nature.

Arguably, evolvability is the best way to be resilient because even broad or highly dependable niches will be threatened eventually."

—JASON BERTRAM, THEORETICAL BIOLOGY FELLOW AT THE ENVIRONMENTAL RESILIENCE INSTITUTE AT INDIANA UNIVERSITY

There's a reason for the fruit fly's endurance. For example, the *Drosophila melanogaster*, with a brain the size of a poppy seed, has evolved into a winter and summer version of itself. The tiny fruit flies even have complex courtship rituals that rival species one thousand times their size.

Jason Bertram, Theoretical Biology Fellow at the Environmental Resilience Institute at Indiana University, has spent considerable time constructing models that illustrate how complex biological systems interact with and respond to their environments—and change them.

Of course, he has studied generations of fruit flies, a species that has contributed immeasurably to understanding cellular mechanisms and genetic variation in evolution and which go through their entire lifecycle in a matter of weeks.

"For example, evolutionary biologists have set up fruit fly populations in a wind tunnel," he says in an email interview, "and they have evolved to fly more than 10 times faster than even the fastest fly we would measure in a natural population without new mutations contributing."

Bertram, who himself has gone through multiple evolutions with an undergraduate degree in mathematics from the University of Cape Town, a master's degree in physics at Australian National University (ANU) and a doctorate in biology from ANU, became fascinated with collective behavior while studying the physics of plasma, a population of charged particles.

Switching to ecology, his focus was broadened to looking at how organisms adapt to, and evolve as a result of, environmental change—how quickly and by what means? Would those adaptations, in turn, shift the surrounding ecosystem? In addition to his primary focus on adaptive evolution and rapid adaptation, Bertram is now studying how human-caused climate change differs from any previous environmental change Earth has experienced.

Despite his interest in collective behavior, Bertram was wary about making conclusions about the "balance" of life. But he did agree a career analogy could be made.

"The history of life on Earth is one of tremendous change, even when we zoom in on the recent lives of organisms that are alive today," he says, "Biologists often use the term 'niche' to describe an organism's place in an ecosystem." And taking a leap into the business world, he noted the coincidence of "niche" being used to describe how we make our living.

"Ecologists generally view resilience in terms of having a broad niche: i.e., you are flexible in how you make a living," he continued, "and can thus survive in a wide variety of different environments, ensuring that changes to one environment don't eliminate you."

Being "evolvable" is having the ability to change a niche when the environment changes, he says. An outcome known as "evolutionary suicide" can result, however, when selection is focused on short-term results to the detriment of long-term gain.

ENVIRONMENTAL IMPACTS

Evolution—the science of which is still evolving—is geared toward immediate outcomes, in that selection rewards attributes that favor survival and reproduction in those conditions, Bertram explains. But there is evidence that past evolution produces attributes that are essentially shelved until they become useful again, if and when a similar environment returns.

"Arguably, evolvability is the best way to be resilient," he says, "because even broad or highly dependable niches will be threatened eventually."

Stretching the metaphor, clearly the cybersecurity industry, though still evolving, has not yet gone beyond the Neanderthal stage. Cyber professionals know how to use tools and they're great at hunting, but the rules and culture are hardly set in stone, so to speak.

With much of the world now connected digitally, cyberattacks have become an increasing problem, costing global economies an estimated $400 billion annually, according to the CyBOK website.

Funded by the National Cyber Security Programme and led by the University of Bristol, CyBOK—which stands for cybersecurity Body of Knowledge—was launched in 2018 as an international effort to unify professional standards and training in fast-growing technology industries.

Mature scientific disciplines such as biology and chemistry, it states, have established bases of knowledge and clear steps to teaching the skills. "However, there is a long-recognized skills gap within the cybersecurity sector," the CyBOK site says, "an issue that experts agree is compounded by a fragmented and incoherent foundational knowledge for this relatively immature field."

To compound the challenges in cybersecurity, there is still a critical shortage of qualified cybersecurity professionals: about 4 million more trained cybersecurity professionals are needed today, according to various industry studies, including (ISC)^2's latest Cybersecurity Workforce Study.

On a broad level, one of the big problems facing the industry is the discrepancy in salaries for government and private sector jobs, says Alice Hill, Senior Fellow for the Council of Foreign Relations. As a result, federal government agencies often struggle to find and keep qualified staff.

"Now the government is maintaining a lot of systems, some of them deeply out of date … with some substantial vulnerabilities," she says. "Yes, we should have the very best helping protect against that, protecting our nation from attacks."

But as issues with managing health data and distribution of unemployment insurance payments during the pandemic have shown, problems with technology in government agencies is systemic, and budgets are only going to get worse for a while.

"I remember going to a Black Hat conference and meeting with a bunch of hackers, talking about the need for help for the federal government," Hill recalls, "and one of them told me, 'You can try to sell us on serving our country, but your salaries just don't match what we can make elsewhere, so you're going to have a hard time finding anyone.' And that turned out to be [true]—it was a very difficult task."

"Just in general, there's great pressure to specialize in one's career, and that can be very good until there's a major shift, and what you're specialized in may become obsolete."

—ALICE HILL, SENIOR FELLOW FOR THE COUNCIL OF FOREIGN RELATIONS

BOUNCING BACK

Hill, who in a previous life served as a special assistant to President Barack Obama and Senior Director for Resilience Policy on the National Security Council, as well as advisor on policy related to creation of the U.S. Department of Homeland Security's cybersecurity workforce, says that she is now focused more on climate change than cyber issues. But, she sees important similarities. Both are vast, interconnected systems that are directly linked to national security.

And there has yet to be sufficient political will to create policy measures to comprehensively address risks from climate change—sea level rise, species extinction, intensified storms, increased drought and wildfires—and the cyber vulnerability of infrastructure, including energy, weather satellites and communication systems and economic systems, to public and private data breaches and attacks.

"With both cyber and climate change, we have huge risks that are growing exponentially," Hill says. "And it's difficult for humans to stay ahead of them. So, what we're seeing is that we're playing catch-up. And that increases the role of vulnerability.

"I think the goals are the same: that we be able to prepare for and recover from, bounce back from, bad events. But similarly, we are unprepared at this stage, I think it would be fair to say. And I believe that both of these threats require a more systematic approach, deeper planning for how we will have a system that allows us to be resilient. We're just in the beginning for both of these threats, I think."

RETURN TO CONTENTS

Even if one company is vigilant in protecting itself from malware, for instance, that won't protect whoever is connected to their systems.

"A failure in one system can spread to another," Hill said, "and that's very similar with climate change. But it's hard to protect yourself entirely. Particularly with cyber, there are bad actors who are trying to actively exploit vulnerabilities."

There should be standards for resilience in both cyber and climate, and expectations that people will meet them, Hill says. Use incentives and employ penalties "to drive better compliance and better practice."

WINTER IS COMING

Again, resilience in navigating a career in a rapidly evolving field can be inspired by survivors in nature. Prepare for winter, and don't depend on one thing to survive.

"Just in general, there's great pressure to specialize in one's career," Hill said. "And that can be very good until there's a major shift, and what you're specialized in may become obsolete."

Her advice for a resilient career is to keep building skills. Look at opportunities that come your way.

"Think about: 'Does this teach me something new? Does it allow me to do things that I haven't been able to do before? Will it stretch me? Does it hone existing skills?' And when you get more yes's than no's, it's a more promising thing to do."

Often, Hill has seen people who, because they're good at their jobs, believe that is good enough. "But I think with the scope of the careers I've observed, circumstances continue to change. And it is people who are most nimble who are the ones that have continued to develop their skills. … You can use (them) to develop your network. So you know people doing different kinds of things. And then you can make switches in your career more easily."

But survival comes down to the environment you are living or working in, and whether you adapt, fly off or starve. Companies, after all, are a kind of ecosystem, except leadership creates the conditions instead of nature.

"The biggest threat is disengaged employees," says Johanna Lyman, Principal Consultant and Practice Leader for Culture and Inclusion at Kadabra SJLC.

Lyman says only about 30% of employees are "truly engaged" with their job, about half float through their days on autopilot, and about 20% are toxic and "poisoning the well for everybody else."

That all adds up to about $500 billion a year in lost revenue for U.S. companies, she says. But if there's one thing a company, and especially its IT department, does not want, it's employees who are sleepwalking or untrustworthy.

"If you've got disengaged employees, do you think they're going to be really careful about the code that they're writing?" Lyman asks. Or, in a toxic situation, the employee "could be actively working against security."

The solution comes from the top, she says. Leadership must foster inclusion and a sense of belonging in the company. Ask employees their opinions. Unite everyone around a mission beyond the bottom line or enriching stockholders.

"If you have a purpose beyond just making money, and if you are actually embodying that purpose, you've got your core values," she says. "Everybody knows what that looks like in action. Everybody knows what the purpose is. And they can see the company working toward it on a regular basis."

Or alternatively, a troubled company or cyber career may make no changes or adaptations. It doesn't evolve.

Instead, it dies off. ■

"If you've got disengaged employees, do you think they're going to be really careful about the code that they're writing?"

—JOHANNA LYMAN, PRINCIPAL CONSULTANT AND PRACTICE LEADER FOR CULTURE AND INCLUSION, KADABRA SJLC

CATHERINE KOZAK *is a freelance writer specializing in environmental reporting who is a past contributor to* InfoSecurity Professional.

RETURN TO CONTENTS

(ISC)²

35+ Courses
110+ 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 over 35 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.

Rethinking Your Cybersecurity Spending

Is your budget based on the right relationship between expenditures and anticipated events?

BY RAJ KAUSHIK, CISSP

NO DOUBT this year will be remembered for the COVID-19 pandemic and public health and economic devastation it wrought.

If we go by historical trends, the novel coronavirus can be conquered if we spend adequate money and resources. Even the 1918 influenza pandemic that infected about 500 million people was defeated within two years. However, a century later, we also can take the current reversal relationship between COVID-19 spread and precautionary measures, including health spending, to look at our own industry, where we frequently encounter viruses and other malicious code whose impact is influenced by cybersecurity spending.

According to Gartner, worldwide spending on cybersecurity is forecasted to reach $133.7 billion in 2022. Cybersecurity Ventures predicts that cybercrime will cost $6 trillion annually by next year. Obviously, reversal relationship doesn't exist here.

On the contrary, cybersecurity spending and cybercrime can be visualized as the two strands of a DNA molecule that entangle into one another and grow in the same direction—what we characterize as a helical relationship.

RETURN TO CONTENTS

In its Global Risk Report 2018, the World Economic Forum listed cyber threat as one of the most critical risks threatening the world economy. For our economic prosperity and quality survival, it is imperative to break away from the helical model between cyber spending versus cybercrime and establish a reversal relationship between the two. This goal is not simple to achieve, particularly because security is envisioned as an umbrella over the organization comprised of links among people, processes and technology. Not to mention most cybersecurity research continues to report that humans remain the weakest link.

GROWING BAD BEHAVIORS

Compromised and negligent insiders create enough opportunities for malicious hackers by disabling security controls, misusing or misconfiguring systems and networks and email, or falling for a social engineering attack. (*See Figure 1, below.*)

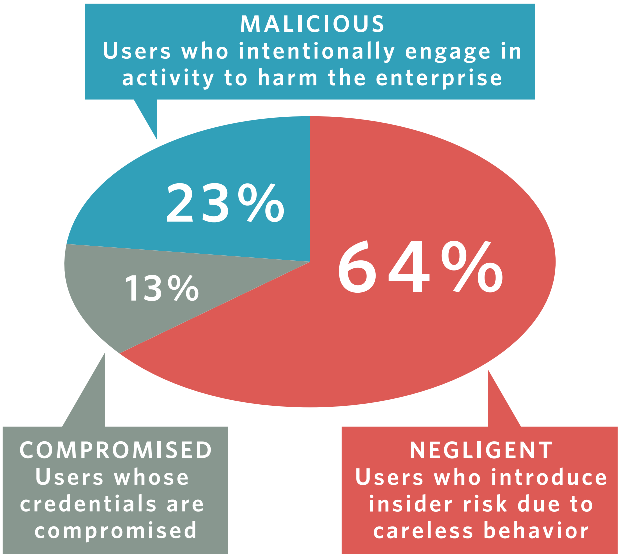
Analysts at the international financial institution Dtex found that users were able to repeatedly visit high-risk websites after disabling security controls. In 74% of assessments, the use of a USB or cloud storage drive was involved.

Instances where insider behavior introduces new system vulnerabilities are prevalent and well documented. While some users may be raising the level of risk in their organization to prove their technocracy, most users circumvent security procedures to deliver under tight deadlines.

I was recently hired as a consultant on an agile team for a major bank. When done strictly by their security policy book, new hires take around a week to get all the necessary permissions, including VPN access, to start their development work. However, human resources and other departmental policies are geared to ensure new hires are productive as soon as they step into the workplace. Leadership, instead of taking care of the overall health of the organization, tends to focus on costs, revenue and ROI—not cyber safety measures. Driven by their ambitions of achieving spectacular quarterly results, they maintain constant downward pressure on their workforce.

Figure 1

INSIDER THREATS



Source: Dtex

> In the morning session, I took the mandatory security awareness test—a test that drives home the message "Never Share Your Password." In the afternoon session, I was given a terminal opened by a teammate. By the next day, I was trustable enough to get access to my teammate's password.

Eventually, the team leads feel the heat. They try to transfer the pressure sideways, and sometime upwards, to the security department. Believe me, lateral pressures hardly yield desired results. The cybersecurity team typically uses the same time-worn email template to reply, outlining why the required permission cannot be expedited.

Security folks often remain as inflexible as a lamp post. Security policies are routinely designed in silos. The team leads that do the work are not looped in during the cybersecurity policy brainstorming and design process. In this instance, my team lead believed there was no option other than to trust me and bypass the prescribed security checks during my onboarding.

In the morning session, I took the mandatory security awareness test—a test that drives home the message "Never Share Your Password." In the afternoon session, I was given a terminal opened by a teammate. By the next day, I was trustable enough to get access to my teammate's password. This is common; 34% of 1,507 U.S. respondents admitted to sharing passwords or accounts with coworkers, according to an online poll. Almost a quarter admitted to reusing the same password on multiple work accounts—this despite a Verizon Data Breach Investigations Report showing 81%

RETURN TO CONTENTS

of hacking-related breaches leveraged stolen and/or weak passwords.

If the IT security department is really not aware of such practices, then it is the proof that these professionals work in isolation. Based on a 2019 poll of more than 500 IT professionals in the United Kingdom, RedSeal revealed that a lack of CEO awareness and engagement in cybersecurity could be placing their organizations at unnecessary risk of attack.

It is imperative for CEOs to ask the right questions proactively, fund projects and support cybersecurity teams. Cyber policies must be contemporary, functional and aligned with other organizational policies. It is common to find such policies stagnant and incongruous with the work culture and team dynamics.

TAKING A PAGE FROM PENAL SYSTEMS

In an organization, the Chief Security Officer (CSO) aims to create a citadel that is impossible to compromise by any intruders. In spite of all-out efforts, data breaches and hacks have increased exponentially in the last 10 years. *(See Figure 2, below.)* The contemporary security vision and strategies are simply not working. A radically different approach is needed.

We need to borrow a page from penal systems that categorized prisons as minimum, medium and maximum-security facilities. Knowing where a breach is more likely to occur based on the work and behaviors of users within a virtual area, we can allocate cyber resources appropriately. This makes more sense than creating a high-security prison for all offenders, including juveniles.

In the typical IT security setup, all employees are required or recommended to undergo security awareness training. But if large numbers of employees still share passwords or bypass security controls, then we know resources are put into a so-called black hole. Organizations have to create a high-security ring around their production systems, a mid-security ring around the test and validation systems, and a low security ring around development systems. *(See Figure 3, p. 29.)*

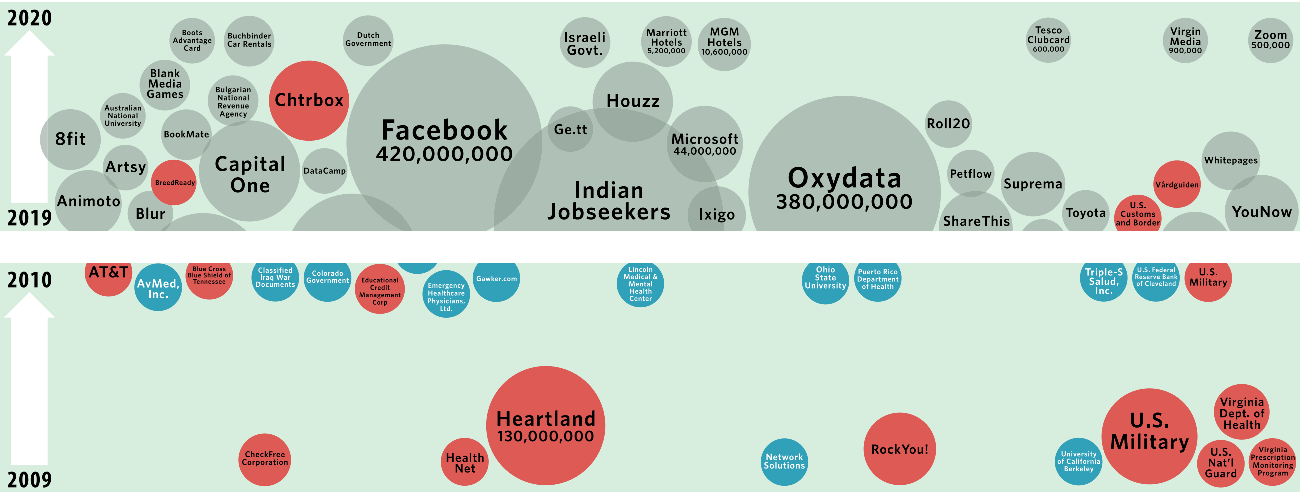
The categorization has several benefits. Topline security tools can be bought and installed around less than 25% of configurations items—which need fool-proof security—in the organization. The mid-security ring mirrors its high-security counterpart. If a sophisticated attack is able to penetrate the mid-security ring, the vulnerability pattern can be studied and any holes can be plugged in the high-security ring in real time.

According to the 2019 Veracode State of Software Security Report (10th Volume), 83% of the 85,000 applications scanned over 12 months contained at least one vulnerability upon the first scan. Two in three applications failed to pass tests based on OWASP Top 10 and SANS 25 compliance standards. It is imperative that no application be transitioned to the high-security ring unless it has passed the OWASP Top 10 vulnerabilities.

Most CSOs would argue that they already have the categorized IT security in place. Production systems are kept behind multiple firewalls. Documents are bucketed into categories ranging from confidential to public. Access controls are in place.

Figure 2

DATA BREACHES AND HACKS COMPARISON



RETURN TO CONTENTS

Figure 3

ISOLATION-BASED SAVVY SECURITY FRAMEWORK

	High Security	Mid Security	Low Security
Development Tools	Runtime Tools Approved Only	Runtime Tools Approved Only	Development Tools Reputed Open Source
USB & BYOD	Prohibited	Auditable Usage	Auditable Usage
Data	Customer Data	Simulated/Masked Data	Simulated Data
Vulnerability Scanners	24/7 Monitored	Randomly Monitored	Awareness
Security Controls	Highest	Highest	Embedded in Design
Application Security	OWASP Top 10 SANS 25	OWASP Top 10 SANS 25	Embedded in Design
Control Bypass Tolerance	Zero	Zero for Malicious Users	Reprimand
Eligibility (Configuration Items)	Production Systems (5-10%)	Validation Systems (20-30%)	Development Systems (60-75%)
Budget Allocation	60-80%	10-20%	10-20%
Training	Rigorous	Awareness	Awareness

Scenarios

SCENARIO 1	**'George' inserts a USB drive in a high-security configuration item.**
Security Tool	Detects the suspicious activity and an alert is raised.
CSO	The CSO receives the alert and calls HR and physical security personnel.
Actions	'George' is escorted out of the organization immediately.
SCENARIO 2	**A suspicious script attempts to run an unapproved cryptographic tool on a MS configuration item.**
Security Tool	Detects the suspicious activity and an alert is raised.
Security Team	The attack source and pattern are researched; a zero-day vulnerability is identified.
Actions	The high-security ring is updated via emergency release; preventive actions are taken with regards to all eligible configuration items.
Benefits	A ransom attack is avoided because unapproved cryptographic tools were not provisioned.
SCENARIO 3	**The CSO receives monthly report of suspicious activities from the low-security ring.**
CSO	The CSO notes three incidents where employees copied data to pen drives or from cloud drives.
CSO	The CSO audits all three incidents. In two cases, proper entries in the logbook were found. One incident was unauthorized.
Actions	The CSO asked Jon from the security team to work with the individual to learn about the need. After investigation, the file in question was provided from the trusted internal drive.
Benefits	The security controls are transparent and an enabler of productivity.

Yes, all items of the security audit sheet might be in place. But if you look down at your system from 36,000 feet, what do you see? If you see a train comprised of several compartments, then your security model is flawed. From up there, the view should instead resemble a cluster of floating ships.

Data breaches and hacking into the mid- and low-security rings must not dent any organization's operation or reputation in any way. Total isolation of rings is the key. If a low-security employee's password is compromised, hackers must not be able to leverage that to get high-security access.

In London's Buckingham Palace, only highly trained soldiers that have fought with great distinction can qualify for the guard's role. Similarly, anyone who has access to the high-security ring must go through rigorous security training. They should be savvy enough to identify and avoid social engineering and honey traps.

Worldwide, COVID-19 hospitals are divided into zones depending on the severity of health issues. For instance, "green zone" patients don't require ventilators. It is only by concentrating on what is really important and where that a reversal relationship can be attained between cybersecurity spending and cybercrime incidents.

We're all being asked to do more with less at some point in our careers. Maybe now. Maybe next year. The approach described above will help secure organizations from cybercrime in a more thoughtful approach that applies more resources where needed—and without preventing employees from doing the jobs they are paid to perform. ■

Trained as a physicist and with a Ph.D. in Science Museum Studies, RAJ KAUSHIK, CISSP, ITIL, PMP, entered the field of IT in 2000. For the past 20 years, he has been involved in design, development and post-delivery management of enterprise applications. Raj has written numerous research and technical papers and popular science articles.

(ISC)²

Join (ISC)^2 at

Think. Cybersecurity for Government 2020

Virtual Event, 1st December, United Kingdom

The most focused cybersecurity government conference on the calendar

Cybersecurity and the government have always been intrinsically linked. The newly launched Think. Cybersecurity for Government conference program is designed to build bridges across the government-vendor ecosystem through a series of impactful presentations and debates.

Join (ISC)^2's Chris Green for his panel session: **"Are Managed Security Services an Answer for Government?"**

CHRIS GREEN
Head of PR and
Communications EMEA
(ISC)^2

Register for the event:

https://www.thinkcybersecurityforgovernment.com/register/

THINK.
CYBERSECURITY
FOR GOVERNMENT
2020

FREE for public sector attendees
Private sector attendees who are (ISC)^2 members receive **£80 discount**.
Email Matt Stanley at **matt.stanley@thinkdigitalpartners.com**
and quote **ISC2-ThinkCybersec**

'HOLY FIDGET SPINNER!'

BY PERRY CARPENTER

EPISODE 4 (FINAL IN A SERIES): CULTURE CONNECTION

"CULTURE EATS STRATEGY FOR BREAKFAST"
- Peter Drucker
Did you forget something?
Yeah. We all did.

ILLUSTRATION BY TAYLOR CALLERY

PREVIOUSLY IN THIS SERIES:

It's been a month since Acme had a serious wake-up call—a data breach. During the initial investigation, IT Security Manager Mike and his team discovered that the cause tracked back to a phishing email that slipped through their mail filters ... a phishing email that their CEO, Jerry, just happened to click on. Since that day, Acme Corporation's CISO, Jim, along with Mike and team members Katie and Krish have been on a quest to determine how the breach happened and what lessons they can learn from the event.

Did they already have a security awareness program in place? Of course. But after careful research and viewing their program with an open mind, the team identified critical gaps in their approach:

1. Just because people are aware doesn't mean they care.
2. If you try to work against human nature, you will fail.
3. What your people DO is way more important than what they KNOW.

In our last episode, Katie and Krish met with the head of Acme Corporation's marketing department. Together they sketched out a multichannel awareness campaign using a combination of communication strategies at different times to keep their critical security messages top of mind, catch their audiences' attention and increase overall retention. They also leveraged behavior design principles in multiple areas—including that pesky problem area of phishing where they decided to conduct frequent simulated phishing training to help employees build motor memory and strength through constant training.

ONE MONTH LATER
MONDAY 3:23 P.M.
ACME CORPORATE HEADQUARTERS

Katie's finger hovered tentatively over the left button of her mouse. She leaned forward, studying her laptop screen. Cautious. She exhaled, lowering her finger to the mouse button ... *click.*

"All right. We're live!" Katie said. "This is the first security awareness program of the rest of our careers."

Krish jumped in. "Wow. That sounds exciting and ominous at the same time."

Mike, Jim, Krish and Katie stood huddled around an oval

RETURN TO CONTENTS

conference table. They'd spent the last few weeks putting everything into place. They developed a plan that incorporated their recent learnings in communication science, marketing and behavior design. And they managed to convince Jerry, their CEO and accidental clicker, to sign off on everything and agree to champion the program.

As the team filed out of the conference room, Mike was thinking through the events of the past month—from Jerry's infamous click that resulted in Acme's data breach, to Katie's click moments ago that kicked off their new security awareness program. The intervening weeks were all a strange blur punctuated by sharply detailed memories of their experiences. Jim was the last out of the room, turning off the light.

Just as the room went dark, Katie exclaimed, "Holy fidget spinner!" This was seriously strong language for Katie.

"Um ... are you OK?" Jim asked as he turned the light back on. "Did you forget something?"

"Yeah. We all did." Katie said as she pointed at what someone in Acme Corp. must have felt was a fantastic inspirational poster.

"I don't get it," Mike said. "We've got awareness posters scheduled as part of our campaign."

"Yeah, we do." Katie replied, "But that's not what I'm getting at. I'm talking about what the poster says." Katie continued to point as the group clustered behind her, taking in her line of sight. Each of them read the quote and took a minute to process the words. It said:

> *"Culture eats strategy for breakfast."*
>
> *—Peter Drucker*

About 30 seconds of silence passed. Then each member of the team walked back to the conference table and sat down.

"Soooo ... let's talk culture," Jim said, taking out a notepad and pen.

WELCOME to the fourth and final installment in our series all about building transformational security awareness programs. Jim, Mike, Katie and Krish accomplished a lot in the past month. They managed to re-envision their entire security awareness program in ways that will better resonate with their audience and work with human nature. They did a great job in planning their awareness communication and some behavioral interventions. But—as you just read—they stumbled across one final facet that they need to address: culture.

What Katie and the team realized was that, even with great communication and behavior management, they will always feel like they are swimming against the current. Their efforts will achieve good results but will not be self-sustaining unless the larger organizational culture values security and makes security part of its DNA.

Here's the harsh truth: awareness and behavior don't happen in a vacuum. They are impacted by everything happening in and around people's lives. Culture can be either your biggest ally or your biggest foe. All the great work you do with messaging and behavior can be degraded or undone if the overall culture of your organization isn't reinforcing the security values you are promoting or, even worse, if the organizational culture runs contrary to those values.

One of my favorite quotes related to organizational culture comes from management consultant John R. Childress in his book *CULTURE RULES! The 10 Core Principles of Corporate Culture and How to Use Them to Create Greater Business Success*. "You get the culture you ignore," he writes. That's about right. At all times you are building strength or allowing atrophy. You can't afford to ignore your security culture.

Now here's the challenge. You've got to find ways for your security team (which is likely dwarfed by the size of your larger organization) to influence the entire organization—and to do so in an effective and sustainable manner. This goes far beyond what you can hope to accomplish by simply rolling out a traditional information-based security awareness campaign and hoping for the best. This requires everything that we've covered in the other installments of this series combined with a few other bits of magic. Unfortunately, we don't have the space in this installment to get into detail—but I *can* give you two tips for getting started: (1) take stock of where you are and (2) make your security values go viral.

TAKING STOCK

Taking stock of where you are requires observation and measurement. The first part of influencing your security culture is assessing and understanding the culture as it currently exists. This can be accomplished via cultural surveys, focus groups, direct observation, behavioral metrics, face-to-face interviews or any other means available to you.

Ideally, you'll be able to collect multiple types of data—for instance combining survey results with observational data from your SIEM or DLP tools. But the main thing that you are trying to do is remove your own subjectivity and allow the data to speak. One survey tool that I'm fond of was developed by security culture researcher Kai Roer. His methodology breaks culture down into seven dimensions: attitudes, behavior, cognition, communication, compliance, norms and responsibilities. *(See Figure 1, p. 33.)*

RETURN TO CONTENTS

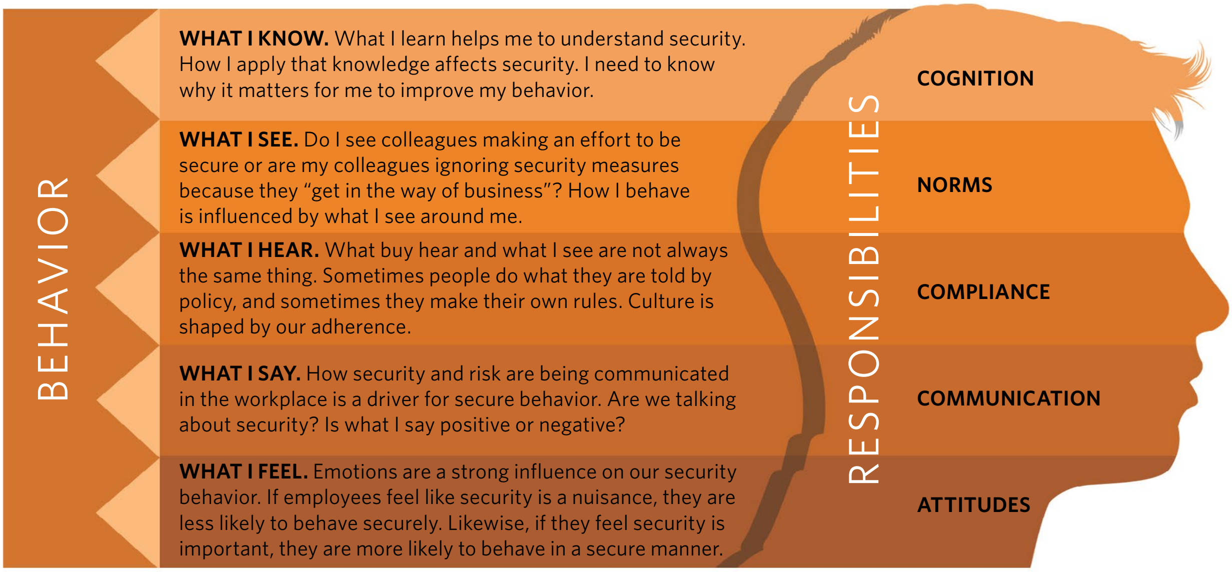
YOUR HOMEWORK

1. Consider contacting your own organization's Human Resources department. Ask HR about any culture-related campaigns that have been effective and discuss what qualities made them effective.
2. The first step of influencing your security culture is assessing and understanding the culture as it currently exists. This can be accomplished via cultural surveys, focus groups, direct observation, behavioral metrics, face-to-face interviews, or any other format at your disposal. Take stock of the measurement methods you have and start measuring!
3. Consider how to structure your culture carrier program. Design structures, social reinforcements, reward systems and rituals. Doing so will create a culture and support environment that is distributed, recognizes and addresses the unique differences between groups, implements social feedback, and is naturally encouraging and engaging.
4. Review previous installments of this series to ensure that your program encompasses aspects of awareness communication, behavior design and culture management.
5. Send LinkedIn connection requests to me and at least 10 other security awareness professionals so that you can always be contributing to and learning from others in your network. ■

—P. Carpenter

Figure 1

KAI ROER'S SURVEY METHODOLOGY HELPS DEFINE AN ORGANIZATION'S SECURITY CULTURE



WHAT I KNOW. What I learn helps me to understand security. How I apply that knowledge affects security. I need to know why it matters for me to improve my behavior.

WHAT I SEE. Do I see colleagues making an effort to be secure or are my colleagues ignoring security measures because they "get in the way of business"? How I behave is influenced by what I see around me.

WHAT I HEAR. What buy hear and what I see are not always the same thing. Sometimes people do what they are told by policy, and sometimes they make their own rules. Culture is shaped by our adherence.

WHAT I SAY. How security and risk are being communicated in the workplace is a driver for secure behavior. Are we talking about security? Is what I say positive or negative?

WHAT I FEEL. Emotions are a strong influence on our security behavior. If employees feel like security is a nuisance, they are less likely to behave securely. Likewise, if they feel security is important, they are more likely to behave in a secure manner.

By crystalizing your understanding of security culture, you can begin to identify gaps between where you are and where you'd like to be. That's the beauty of definition and measurement.

GO VIRAL

The second secret of managing security culture is finding ways to make your culture go viral. That virility is the key to distributing and reinforcing the security-related values and behaviors you're hoping to build into your culture.

That brings us to the concept of *culture carriers*. Within an organizational context, a culture carrier, according to designer Mike Buss, is "someone who has intimate knowledge of the company values and can have an intelligent discussion about why their company does what it does. They are ambassadors for their company and passionately work to promote the company values in their day-to-day dealings with clients and coworkers."

Now, think how the idea of culture carriers (sometimes also referred to as "security champions") might work within a security context. Imagine having groups of people across regions, departments and at all levels of your organization who have intimate knowledge of your security values and who model positive security behaviors. These culture carriers are able to discuss why your security values and behaviors are relevant and important. Imagine the power and influence that they would bring as they work to promote

RETURN TO CONTENTS

your values in their day-to-day work—as they interact with other people; as they initiate, comment on and support projects; as they mentor new hires; and as they help other employees around them.

This group of culture carriers becomes a force multiplier for your awareness program and your organization's security-related knowledge, values and behaviors. ■

PERRY CARPENTER *is the chief evangelist and strategy officer at KnowBe4, Inc. and author of* Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors *(Wiley Publishing, 2019), upon which this series is based.*

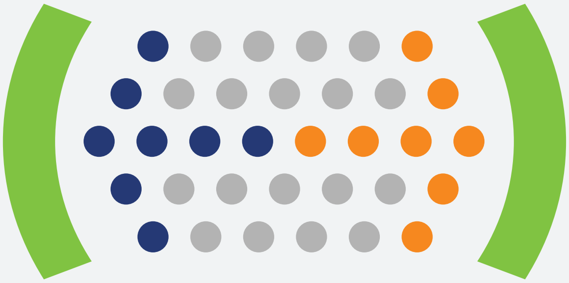
HAVE A QUESTION FOR PERRY?

You can reach him on LinkedIn at /in/PerryCarpenter, Twitter: @perrycarpenter, or email: perryc@knowbe4.com. He's also inviting our readers to join his *Transformational Security Awareness* group on LinkedIn (https://www.linkedin.com/groups/12207804/) or by simply typing "Transformational Security Awareness" into the LinkedIn search.

Word from the Author

Writing this series has been an honor. I hope that you've enjoyed reading it as much as I've enjoyed writing it. Please stay in touch. I'm always up for a chat about anything related to security awareness, security behavior design, or really anything related to the human side of security.

—*Perry Carpenter*



RETURN TO CONTENTS

Teaching Cyber Safety in a Virtual World

by Pat Craven

I THINK IT HAS BECOME OBVIOUS to all of us that how we learn and gain insight and knowledge has changed. I am sure that one day, we will gather for conferences and trainings again, but even then, it will be different.

All Center for Cyber Safety and Education cyber safety education programs were originally designed for group settings. For years, our members would set up their laptops and projectors at a school, community center or library and deliver a PowerPoint program to children, parents or senior citizens on how to be safe and secure online. In just the last five years, that effort has exploded by 1,300%! With our cyber safety materials now available in 20 languages, we expect our outreach efforts and impact to skyrocket even further in the future.

It has been exciting to see our volunteers realize they can deliver cyber safety training virtually, and that it may even allow them to reach greater numbers than they would in person. We have been getting notes from people around the world telling us how they presented one of our programs to hundreds of families via Zoom, WebEx and even Facebook Live. Seeing the shift our community was making, we hosted a training session to help volunteers get involved virtually. Hundreds of people attended the hour-long webinar. The replay is available at https://iamcybersafe.org/s/volunteers.

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

GARFIELD GOES DIGITAL

Our multi-award-winning Garfield's Cyber Safety Adventures program was created to be delivered in the classroom as a group learning experience. But like everything else, that came to an abrupt stop in March. As schools still work to sort out their "new normal," our proven method of teaching younger children how to be safe online was in jeopardy.

Garfield at Home launched in July as a fun and interactive way for children to learn about privacy, cyberbullying, stranger danger and safe posting from their home computer, laptop or tablet. Children around the world now have access to this exclusive program.

Photograph: Getty Images

But that program would not be the right fit for a classroom or group setting. The Educator Kit, which has been so successful in delivering the cartoon and conducting group conversations, proved a much bigger challenge. But we did it!

The Garfield Virtual program enables anyone to provide engaging digital citizenship training to schools or organizations meeting online. Using our digital eWorkbooks and your favorite video platform like Zoom, Skype, WebEx, etc., Garfield and his friends can help you teach children how to be safe and secure online in a fun instructor-led program. We provide all the online materials and training you will need to lead your group on this important educational adventure.

To learn more about any of these programs, visit our website www.IAmCyberSafe.org or reach out to us at center@isc2.org. Children are spending more unsupervised time online than ever before, and parents need our help more than ever to keep them safe and secure. Please join us in making it a safer cyber world for everyone. ■

RETURN TO CONTENTS

(ISC)² Community

SHARING INSIGHTS FROM BUZZWORTHY THREADS

Join the (ISC)² Community

Ensuring Policy Review, the Value of a Doctorate, Affordable Risk Assessment Software

The (ISC)² Community has more than 27,000 cybersecurity professionals connecting, sharing knowledge and offering solutions in the online forum. Note that the questions and responses may have been edited for clarity and brevity.

QUESTION:

I am looking for a way to hold the departments accountable and ensure they review the policies that we have. I was thinking about using Adobe Sign but don't want to go cloud. An application like those that make you scroll to the end, then click "agree" would be nice if it kept track of the people who signed.

—Posted by tim2

SELECTED REPLIES:

We use our payroll/HR software to disseminate that information. [Users] log in and are notified they have a message, view the document and when they click "OK," it acknowledges the fact that the document has been viewed and saves a log per user.

—Posted by tmekelburg1

You could look at a tool like MetaCompliance; however, reading a long policy isn't usually top of people's agenda in many organizations, so unless it's a complete rewrite, it may make sense to just announce the delta.

—Posted by Steve-Wilme

Find this complete thread here.

QUESTION:

I am a 40+ security professional wondering whether it is worth pursuing a doctor of philosophy in information security. I graduated with a master's degree in information security a couple of years ago. Since then, I cannot seem to find a job that matches with my qualifications. I know it is a very costly venture, but is it worth the dare just for job satisfaction?

—Posted by BMwine

SELECTED REPLIES:

After completing my master's in information security and assurance, I considered going on as well. What came to be my deciding factor was searching for jobs that required it, and I found very few. Even now I find that most jobs only ask for a bachelor's degree, and a master's is a plus. The only place I feel a further degree would have been of value would be in an academic setting, and that is not a direction I would have wanted to go.

—Posted by JKWiniger

Why do you want the degree? Unless your current employer has an incentive for you to move up to that degree, there is close to no job benefit in getting the degree. You might get your resume looked at with a Ph.D. on it, but you will not get a job because of it; they will still look at your skills and accomplishments in the field for the hiring decision.

—Posted by CraginS

You say the jobs in the market do not match your qualifications. Does this mean that you can't find a job that pays you what you think you should be paid? You can't find the job in a location you want? Are you looking for a very specific job that does not have a large number of postings (e.g., forensic specialist)? If you can't find a job with your current skill level/education/certifications, etc., getting a Ph.D. won't help.

—Posted by CISOScott

Find this complete thread here.

QUESTION:

I'm at a small 200+ private company, developing policies, procedures, etc. Is there a good risk assessment tool I could gain access to and use internally? Would like to start internally prior to spending $$$ with a third party.

—Posted by Lwhite

SELECTED REPLIES:

There are some open source tools which can be helpful. Most probably you could also get away with an Excel spreedsheet (just search Google for templates as there are tones of them).

https://github.com/Risk-Assessment-Framework/RiskAssessmentFramework

—Posted by Wiktor

The CIS RAM (https://learn.cisecurity.org/cis-ram) helped me get through risk assessment hurdles in the past. I used this tool to get an organization ISO 27001-certified, and at my old organization it was useful in fulfilling the requirements of our SOC 2 audit.

—Posted by BillyAnglin

I use Airtable for this purpose. It is a super-vitamin Excel software that provides more dynamic views, tables and reports. I use it in my company and so far, so good.

—Posted by DiegoRojas

Find this complete thread here.

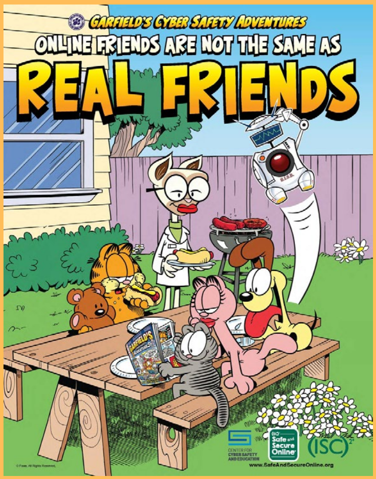
RETURN TO CONTENTS

FOR VIRTUAL CLASSROOMS

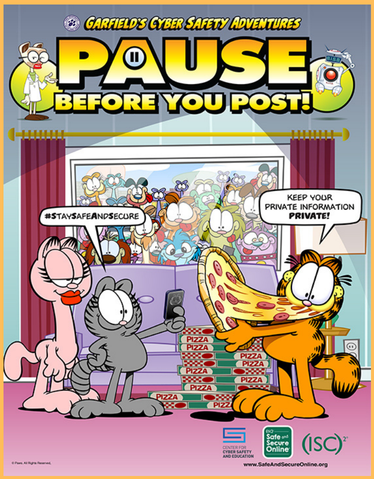
THREE VOLUNTEER-LED LESSONS AVAILABLE:

GARFIELD'S CYBER SAFETY ADVENTURES
BE KIND ONLINE!
USE CARE WHEN YOU SHARE!
NO MEAN COMMENTS!
NO MEAN PICTURES!
NO TAGGING WITHOUT PERMISSION!
www.SafeAndSecureOnline.org

Cyberbullying


GARFIELD'S CYBER SAFETY ADVENTURES
ONLINE FRIENDS ARE NOT THE SAME AS
REAL FRIENDS
www.SafeAndSecureOnline.org

Privacy


GARFIELD'S CYBER SAFETY ADVENTURES
PAUSE
BEFORE YOU POST!
#STAYSAFEANDSECURE
KEEP YOUR PRIVATE INFORMATION PRIVATE!
PIZZA
www.SafeAndSecureOnline.org

Social Media Safety

EACH LESSON INCLUDES:

- Volunteer eWorkbook with lesson plan
- Student eWorkbook
- 30-day access to 'Find & Click' Storybook
- Letter to Parents
- Educational Group activities

FEATURES:

- Ages 6-11
- 30-45 minute lesson
- Teaching level: easy!
- Interactive group activities
- Works with any video conference platform
- Use for classrooms, community outreach and events!

GET YOUR 2021 QUOTE:

CENTER@ISC2.ORG

(727) 339-6508

CENTER FOR
CYBER SAFETY
AND EDUCATION

IAmCyberSafe.org