HOW THE BOARD ACTS IN MEMBERS' INTERESTS

InfoSecurity PROFESSIONAL

A Publication for the (ISC)$^{2®}$ Membership

JULY/AUGUST 2019

Gamification

How to build a security-aware culture through play

'CODE' BREAKERS

When people don't play by the same rules

LEGAL ENTRY

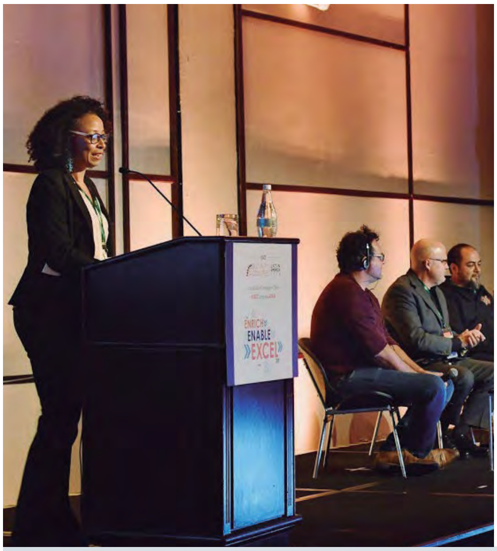
Why your incident response team needs a lawyer—now

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

(ISC)²

SECURE SUMMIT / LATAM

ENRICH ENABLE EXCEL



ENGAGE WITH LATIN AMERICA'S BEST

The (ISC)² Secure Summit LATAM 2019 will take place on September 25-26 at Camino Real Polanco Hotel, Mexico City.

Meet the best information security and cybersecurity professionals in Latin America and learn about the most relevant topics, innovations and solutions to the latest cybersecurity threats. Share your expertise with peers and develop skills that will advance your career.

(ISC)² members can earn up to 16 CPEs

REGISTER NOW latamsummits.isc2.org

September 25-26, 2019 | Mexico City | #ISC2LatamSummit

contents

VOLUME 12 • ISSUE 4

PAGE 19

features

MANAGEMENT

ETHICS

STRATEGIC PLANNING

Cover image: JEAN-FRANCOIS PODEVIN Illustration above: ROBERT NEUBECKER

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. ©2019 (ISC)^2 Incorporated. All rights reserved.

(ISC)²

REGISTER
NOW AND ***SAVE!***

2019 SECURITY CONGRESS

OCT. 28-30 | Walt Disney World Swan and Dolphin Resort | Orlando, Florida

Keynotes Announced

Earn up to 46 CPEs.

Captain "Sully" Sullenberger

Captain "Sully" Sullenberger is best known for serving as Captain during what has been called the "Miracle on the Hudson." He is a safety expert, international lecturer, keynote speaker and a New York Times best-selling author.

William H. McRaven

Admiral William H. McRaven is a retired U.S. Navy Four-Star admiral, best-selling author and former Chancellor of the University of Texas System.

Catherine Price

Catherine Price is a science journalist, speaker, author, teacher and consultant. She is the founder of Screen/Life Balance and author of several books, including her most recent, "How to Break Up with Your Phone."

Erik Wahl

Erik Wahl is a graffiti artist, creativity scientist, best-selling author and philanthropist. His breakthrough thinking has earned praise from influencers in both art and business. His artwork has raised millions of dollars for charity and can be seen hanging in executive offices around the world.

Early Bird Pricing through August 15

Register Today

SAVE $50 Off All Access Pass
with code: **SECPROF19**

congress.isc2.org #ISC2Congress

(ISC)²
Members
Save
$300

Welcome to the Big Leagues

I KEEP READING that high-level cybersecurity leaders face a mountain of job stress, and they aren't always handling their anxiety well. A widely circulated report earlier this year noted that about one in seven CISOs turned to drugs or alcohol to cope with job pressures.

I would have expected that number to be higher.

That same survey of 408 CISOs from U.S. and U.K. companies showed some 60% admitted finding malware that had resided undetected for an unknown period of time (another 9% couldn't claim their IT infrastructure was currently malware-free). Around the same percentage say they were denied the appropriate budgets, technology or talent needed to prevent attacks going forward. This despite the demands from their executives and boards that they keep the company out of headlines for data breaches and out of courtrooms due to class-action lawsuits.

The vast majority—almost nine in 10—typically worked beyond 40-hour weeks and many couldn't truly disconnect during limited downtime. This likely included the 23% who admit work negatively impacted personal relationships. A recipe for burnout, you say? That may explain why the tenure for 55% of survey respondents was less than three years (30% had served less than two years).

The average company size at which the surveyed cybersecurity executives worked was just under 9,000 employees. I'm not sure stress levels differ for those with similar positions at smaller companies. Threats and actual attacks don't tend to discriminate, and resource constraints aren't exclusive to certain-sized organizations.

This magazine issue tackles three ways to help alleviate some of the daily tension everyone's experiencing, whether entry-level or executive. Our cover story provides a way for users to take cybersecurity more seriously—through gamification. Another article keys in on ethics, and why we all should follow a code. Finally, with our third feature, I ask: When's the last time you brought in the lawyers *before* responding to an incident?

Yeah, that's what I thought. ■

Anne Saita, editor-in-chief, lives and works on the U.S. West Coast. 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

SENIOR CORPORATE COMMUNICATIONS SPECIALIST
Kaity Eagle
727-683-0146
keagle@isc2.org

MANAGER, MEDIA SERVICES
Michelle Schweitz
727-201-5770
mschweitz@isc2.org

EVENT PLANNER
Tammy Muhtadi
727-493-4481
tmuhtadi@isc2.org

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

EDITORIAL ADVISORY BOARD

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

TWIRLING TIGER MEDIA EDITORIAL TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

MANAGING EDITOR
Deborah Johnson

EDITOR
Paul South

PROOFREADER
Ken Krause

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

RETURN TO CONTENTS

Security Should Be in Everyone's Skill Set

Would someone in your company or team benefit from adding security to their skill set? Today, it is everyone's job to safeguard data from breach. While many IT professionals may not have imagined that data protection would be a critical part of an IT career, due to the value of corporate data and assets, and the increasing skills of cyber criminals, those with varying roles and responsibilities have learned they need to take ownership of security.

Encourage others to play their role and be a part of the change by sharing this eBook. Inside they'll find:

- Why Security Is Important to Practice in IT Roles
- How Security Knowledge and Skills Enhance IT Careers
- Tips for Getting Ahead with a Focus on Security

SHARE THIS EBOOK

www.isc2.org

The Hardest Job You'll Never Be Paid For

by Jennifer Minella, CISSP

I WAS JUST 16 YEARS OLD when I sat on my first advisory board to a government agency. Now well into my career, I manage a division of a company and serve as a technical strategic consultant to myriad organizations including some of the world's largest and most notable brands. While it pays the bills, my real joy comes from working with smaller organizations and volunteering with nonprofits, where I can see firsthand the hard work and passion manifesting in meaningful ways. Ah, to relish in the sweet fruits of our labors.

And so it has been with my time serving on the (ISC)² Board of Directors. As I wrap up my final year of service, I find myself humbled by the position of chairperson, where the job description is a daily orchestration of the flurry of activity constantly happening behind the scenes in the board of a fast-growing organization.

It's been said that "a good juggler can juggle more," and I'd like to share a peek inside the expert juggling that comes with a role on the board.

Jennifer Minella, CISSP, is vice president of engineering and consulting CISO with Carolina Advanced Digital, Inc. and chairperson of the (ISC)² Board of Directors. She can be reached at jminella@isc2.org.

WHAT THE (ISC)² BOARD REALLY DOES

From the outside, what the board does is not immediately visible to our more than 140,000 members worldwide. Serving on the board is an amazing experience, but it's not the glitz and glamour some may imagine.

What does the board do, and not do? First, we do not manage (ISC)²'s daily operations. There's a long history here of how an organization grows and how we got from a managing board to a governing board. As a such, we have legal responsibilities—duty of care, duty of loyalty and duty of obedience. What this means is that in addition to all the fun puzzles of "let's fix all the problems with (ISC)² and the world," we have obligations to run the organization according to law.

Those obligations translate to several committees with work and deliverables, including audit, professional conduct (or ethics) and business practices, along with managing the CEO's compensation, certifications and strategy, to name a few.

> **Each time we see dollar signs, we have to balance the fact that we're spending (at least in part) members' money with the reality that (ISC)² is thriving, growing, and owes those members a lot in return.**

The board has a heavy burden in making long-term strategic decisions and approving large budgets that fuel the organization's growth. Each time we see dollar signs, we have to balance the fact that we're spending (at least in part) members' money with the reality that (ISC)² is thriving, growing, and owes those members a lot in return. As a member, you bought into (ISC)², and now (ISC)² is buying into you.

Some of the recent big-ticket items the board approved and oversaw include a massive multi-year digital transformation that just recently concluded and the newly launched Professional Development Institute (PDI). The former project was a requisite for the latter, and also necessary to be able to deliver on the promise of member value. As you probably know at this point, PDI is our new platform of free (and robust, high-quality) training. Yes, (ISC)² had technical debt and member debt; we all know it and we're working daily to pay it back.

RETURN TO CONTENTS

The board's duties demand that we poke, question and rethink relentlessly.

Our job doesn't stop at approving projects. The board's duties demand that we poke, question and rethink relentlessly. We have a duty to constantly examine our current position and our path forward, and that type of collaboration takes a special blend of people willing to participate in bringing to light tough questions through occasional friction and debate conducted with trust, mindfulness and passion.

If you're interested in serving on the Board of Directors, talk to a current board member or your local (ISC)² chapter. At a minimum, you can participate by voting in the upcoming election, which takes place between September 12 and 26. ■

RECIPE FOR A GOOD BOARD MEMBER

EACH YEAR as the board goes through the process of identifying candidates to put on the slate for member elections, we consider the questions of "What makes a good board member?" and "What skills or experience gaps do we need to fill this round?"

In my past six years on the board, these are four key characteristics I think contribute to a highly functional and always-maturing board:

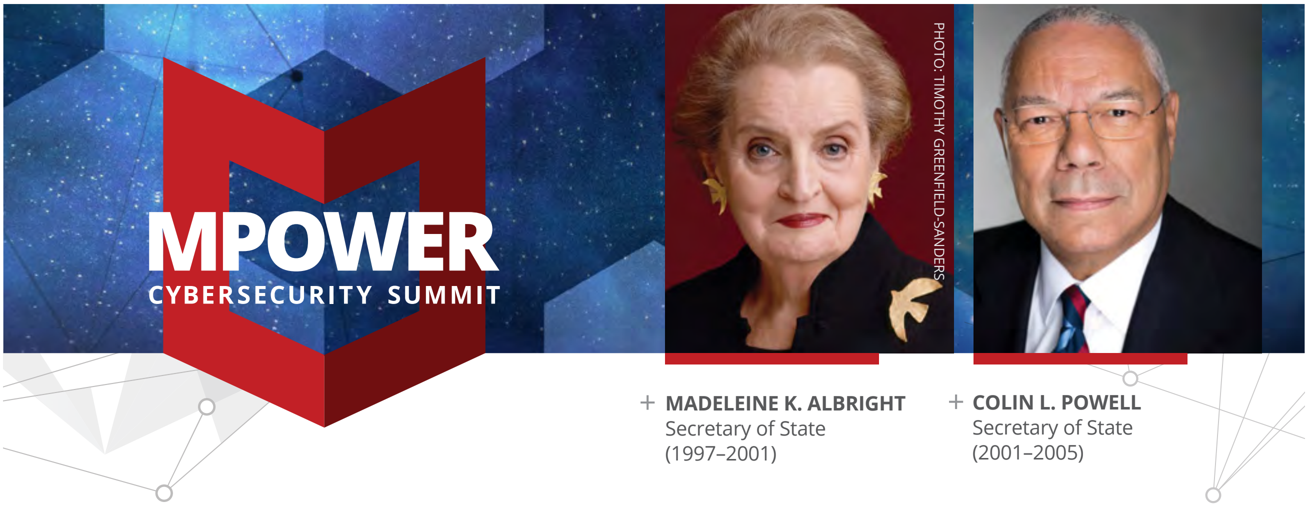
Passion: An unwavering addiction to wanting to better the industry

Mindfulness: Being attentive, thoughtful and willing to re-examine your own thoughts

Trust: Willingness to earn and give

Skill: Experience in both strategic and tactical execution

—Jennifer Minella



RETURN TO CONTENTS

field notes

EDITED BY DEBORAH JOHNSON

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

(ISC)² Hong Kong Marks Membership Milestone

Growth seen throughout APAC

(ISC)² offers a robust, online resource portal for information security professionals!
Learn more

Security Congress APAC 2018

About Us

(ISC)2 Hong Kong Chapter operates as a special interest group (SIG) of the Professional Information Security Association (PISA).

PISA is a Hong Kong based not-for-profit Information Security organization.

Benefits of Becoming an (ISC)² Hong Kong Chapter Member

- Gain a sense of fellowship with colleagues in your profession;
- Network and exchange knowledge with fellow (ISC)² credential holders and other information

  security professionals in Hong Kong;
- Participate in co-sponsored events with PISA and other industry associations;
- Earning Continuing Professional Education (CPE) by participating in professional activities;
- Assist (ISC)2 initiatives by speaking at industry events or writing articles for publication;
- Participate in local community outreach projects (public service) to

CONGRATULATIONS TO the Hong Kong Chapter for reaching a landmark member count of 2,000 information security professionals. This contributes to propelling the Asia-Pacific region toward the 20,000-member mark.

"Hong Kong is now the seventh economy in the Asia-Pacific region in which we have more than 2,000 members, joining Australia, India, Japan, Korea, China and Singapore in that distinction," says Clayton Jones, managing director, Asia-Pacific, (ISC)².

The 2018 Cybersecurity Workforce Study noted that 39% of cybersecurity staff in Asia-Pacific say a lack of skilled colleagues in their department is their top job concern, and a combined 53% indicate that this shortage puts their organizations at either moderate or extreme risk of experiencing a cyberattack. This extensive need in cybersecurity throughout Asia-Pacific can be attributed to several rapidly expanding economies as well as increased security legislation to protect consumers.

Jones adds, "There is a well-established need for more certified and skilled cybersecurity talent here and we're thrilled to represent so many of these professionals and help them along the path of continued development as they work to secure the critical data assets of both the government and the private sector." ■

> "Hong Kong is now the seventh economy in the Asia-Pacific region in which we have more than 2,000 members, joining Australia, India, Japan, Korea, China and Singapore in that distinction."
>
> *—Clayton Jones, managing director, Asia-Pacific, (ISC)²*

BOOMING CONNECTIVITY

100 BILLION

Connected devices by 2025 worldwide

Source: PwC Connected Solutions

THE CHURN

6.4 BILLION

Fake emails sent worldwide every day

Source: EY Global Information Security Survey 2018-2019

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 homepage 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=10824

RETURN TO CONTENTS

Get Ready for (ISC)² 2019 Security Congress

Save your seat (and get a price cut, too)

Join more than 4,000 cybersecurity professionals for three days of thought-provoking, challenging and eye-opening sessions, panels and presentations at the 2019 (ISC)² Security Congress, October 28-30 in Orlando, Fla.

More than 150 sessions will dive into the areas of cloud security and cybercrime, threats and incident response, career development, and much, much more. The programs and speakers will provide crucial and high-level information that is sure to expand your knowledge and enhance your professional growth. And (ISC)² members can earn CPE credits throughout the event.

The (ISC)² Security Congress will be held at the Walt Disney World Swan and Dolphin Resort in Orlando. In addition to outstanding convention and hotel facilities, attendees will have the opportunity to obtain discounts for many of the exciting attractions that the Disney theme parks are known for.

For complete information on registration, sessions and travel and accommodations, go to http://congress.isc2.org.

Too Much Data?

A new survey suggests that IT professionals may be weighed down by all the incoming information

Image: iStock

HOW MANY SOURCES for job-critical data do you have in order to complete assignments? If your response is “Too many,” you are not alone. A survey by Ivanti, a Utah-based software solutions company, reveals that 37% of 400 professionals surveyed said they have from 11 to 25 different sources of data. And 15% say they have too many to count.

The impact of the profusion of data sources can be seen in turnaround time: Only 10% of those responding said the incoming data is actionable within minutes and 51% report they have to work with the data for days or weeks—or more!—before it is actionable.

One of the causes of the congestion is the siloing of data for security purposes. “It’s clear from the results of this survey that IT professionals are in need of a more unified approach when working across organizational departments and resulting silos,” says Duane Newman, Ivanti’s vice president for product management.

> “It’s ... important to note that IT organizations need to find better ways to work with their data or it will continue to impact other critical IT priorities.”
>
> *—Duane Newman, vice president for product management, Ivanti*

The areas that suffer most from the data crunch, according to Ivanti’s survey, are:

- Automation – 46%
- User productivity and troubleshooting – 42%
- Customer experience – 41%

“It’s … important to note,” concludes Newman, “that IT organizations need to find better ways to work with their data or it will continue to impact other critical IT priorities.”

For more information and complete results of Ivanti’s survey, see https://www.ivanti.com/blog/survey-it-professionals-data-sources.

RETURN TO CONTENTS

Data Attacks Show No Sign of Slowing Down

Malicious hacking is down; social attacks are up

CYBERCRIME STILL PAYS, and well. The FBI's Internet Crime Complaint Center reports 2018 financial losses of $2.7 billion—nearly double the loss sustained in 2017. Just how those losses occur vary, but the Verizon 2019 Data Breach Investigations Report (DBIR) offers insight on common culprits. Among the most anticipated reports, DBIR findings are based on analyses of more than 41,000 cybersecurity incidents and more than 2,000 data breaches from 86 countries.

Among key findings:

- Two-thirds of the perpetrators of cybercrime are outside parties, almost always nation-states or their affiliates, which accounted for 96% of the breaches from outsiders in 2018.
- Social attacks, through spoofing, phishing and other methods that can deliver malware, remain one of the best entry points to a breach.
- C-level executives are 12 times more likely to be the target of social incidents.
- Also more susceptible: mobile device users. The on-demand accessibility of the devices makes them a target; their size limits navigating and necessitates toggling.

Then there's the distraction factor, which isn't exclusive to mobile users. That said, one reason mobile attacks are effective is because users tend to walk, talk, drive and do other activities while using their smartphones or tablets.

For the complete report, go to https://enterprise.verizon.com/resources/reports/dbir/. ■

VERIZON 2019 DATA BREACH INVESTIGATIONS REPORT

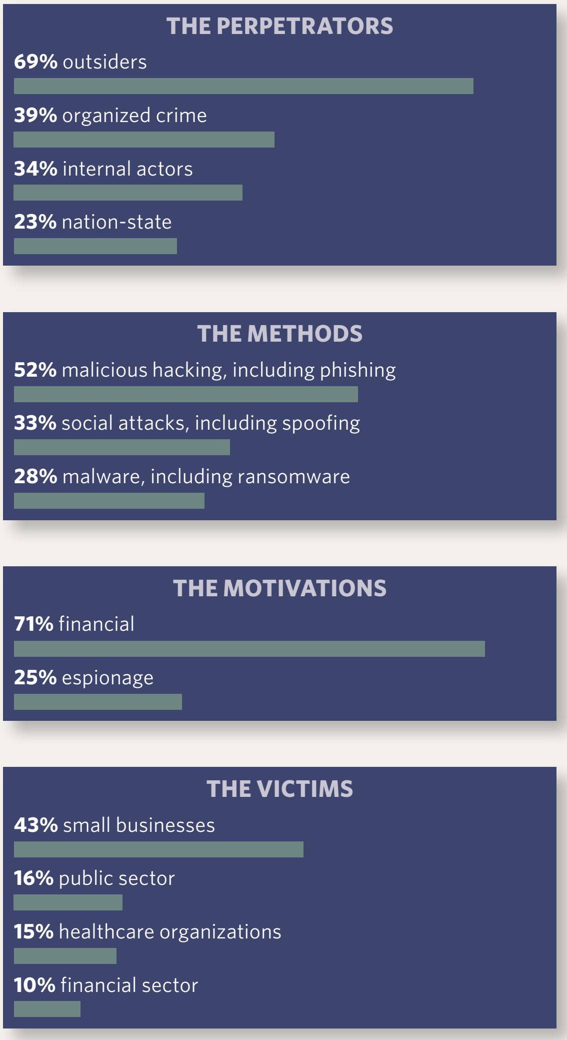


Image: iStock

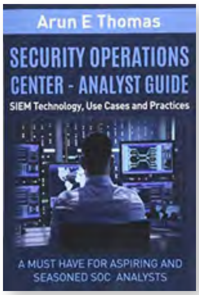
RETURN TO CONTENTS

RECOMMENDED READING

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

Security Operations Center – Analyst Guide: SIEM Technology, Use Cases and Practices

By Arun E Thomas
(CreateSpace Independent Publishing Platform, May 22, 2016)


Arun E Thomas
SECURITY OPERATIONS CENTER - ANALYST GUIDE
SIEM Technology, Use Cases and Practices
A MUST HAVE FOR ASPIRING AND SEASONED SOC ANALYSTS

INTENDED AS A CHECKLIST for a security operations center analyst, Arun Thomas's guide provides techniques to "defend the castle against the invaders." While not espousing specific software, *Security Operations Center – Analyst Guide* is technique-rich in approaches to leading an SOC and is especially helpful to the new manager. Though not a guide from a management point of view (i.e., staffing, resources, etc.), Thomas delineates the 10 functions of an SOC that focus on issues like incident response, vulnerability management, signature updates and more.

Thomas discusses the essentials, the importance of security information and event management (SIEM) policies, and provides a strong selection of use cases and metrics that an analyst can use to identify trends and can be employed as key risk indicators (KRIs). Interestingly, the author also presents an approach to improve the threat intelligence function by either using a managed security service provider (MSSP) or having a third-party threat intelligence platform.

> *Security Operations Center – Analyst Guide* is technique-rich in approaches to leading an SOC and is especially helpful to the new manager.

One challenge with Thomas's presentation is that he describes use cases by tool or security device instead of the security risk presented to the firm. And he does not describe key use cases for business-related applications. There are two schools of thought for use cases, either by device or by risk. Identify the threat and then set up the use case to monitor the threat. Can an SOC utilize both approaches? Of course. Also, the reader has to take it one step further and know to correlate events across security devices, too. This book is rich in information that can be mined to ensure best practices are being followed. Bravo! ■

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.

Top Cybersecurity Blogs of 2019

1. Daniel Miessler
   @DanielMiessler
2. Graham Cluley
   @gcluley
3. IT Security Guru
   @IT_SecGuru
4. Paul's Security Weekly
   @securityweekly
5. Liquidmatrix
   @liquidmatrix

Source: University of San Diego

OUTSIDE HELP

54.5%

Percent of cybersecurity decision makers running crowdsourced security programs

Source: ESG Research, Security Leadership Study: Trends in Application Security

Image: iStock

RETURN TO CONTENTS

(ISC)² COLUMBIA MIDLANDS (CHARTERING) CHAPTER

Becoming an (ISC)² Chapter

Presenting Safe and Secure Online gives new chapter the final push

Education Director Tony McNeil, presenting (ISC)²'s Safe and Secure Online to the third-grade class at Center for Achievement.

THE ROAD TO BECOMING an (ISC)² chapter has many milestones, among them, completing three activities based around the (ISC)² chapter's credo: Connect. Educate. Inspire. Secure.

As its final activity, the chartering chapter in Columbia Midlands (South Carolina) brought the Safe and Secure Online program to 70 primary school students (second through sixth grade) at Columbia's Center for Achievement.

For the presentation, the members chose to focus on privacy. "The material is all about keeping yourself private in online interactions, but is relevant to other interaction types for children as well," Kareem Briggs, the chapter's communication director, says in an email. "Also, we felt the kids would relate to the scenario about how to handle playing online with others and what types of information should and should not be shared because a large percentage of children this age are doing online gaming."

Using videos, comic books and stickers featuring the cartoon cat Garfield, each of the chapter's six volunteers presented to a class of about 15 students. The response from students and volunteers was overwhelmingly positive.

"I learned that I shouldn't give my password to people, even if they are my friends," one fifth-grader said. Another student added: "I really liked the cartoon. It was funny, and they gave us a book to take home to help."

Pictured from left: Marketta Wright (chapter secretary), Kayden Wright (third-grade student at Center for Achievement and class ambassador), Janel Jones, fifth-grade teacher and director of Camp Pathways at CFA.

The presentation underscored the chapter's goals, Marketta Wright, one of the chartering chapter volunteers, says. "Seeing the children's reaction and participation levels firsthand strengthened my belief and elevated my excitement in our chapter's mission of providing security awareness and education for the Midlands area."

The chartering chapter also gained valuable experience in working with students. "The most important part of volunteering with school-aged children is being 'relatable,'" Briggs says. "It's being able to tailor content you want to teach them into something that they can understand and that is intriguing enough to get and keep their attention. Safe and Secure Online made that easier for us." And the most rewarding part, says Briggs, was "the students' reactions. They were so excited!" ■

(ISC)² COLUMBIA MIDLANDS (CHARTERING) CHAPTER

Contact: Ralph Collum, President, (ISC)² Columbia Midlands (SC) Chartering Chapter

Email: ralph.collum@trainingconcepts.com

LinkedIn group: https://www.linkedin.com/groups/12177523/

RETURN TO CONTENTS

Q&A

Ralph Collum

President, (ISC)^2 Columbia Midlands (SC) Chartering Chapter

Why did you and the others decide to become an (ISC)^2 chapter?

I don't know if I can speak for everyone in the chapter, but I have always wanted to be able to give back to this great community of information security/technology. Having a chapter that is driven to promote social awareness and education in security and privacy is an honor and great privilege.

We plan on building a group of professionals that will be able to share their own experiences with the community and promote interest in information security/technology in the Midlands of South Carolina.

What is the background of some of the founding members?

We have six total members right now working at different capacities for our local chapter. I started as system administrator and trainer for a company in Columbia, S.C., working with customers to deploy, manage and troubleshoot systems and train on certifications such as MCSA and MCSE for Windows Server.

I took an interest—which turned into a passion—in information security after taking a few security courses. I now work with companies on risk management and vulnerability management, as well as penetration testing. I also do presentations and teach classes on cybersecurity. My goal is to secure companies by educating them on the methods used by attackers, identifying vulnerabilities and mitigating issues through appropriate levels of awareness and security.

Marketta Wright, the chapter secretary, also shared her background:

"For me, although I got my CISSP back in 2015, I didn't really start focusing on info/cybersecurity until the last couple of years. I'm an Army vet, having worked as a communications/infotech technician. I actively participate in a few other groups here in Columbia that are focused on coaching and mentoring students aspiring to have careers in computer science, information technology and cybersecurity. That's my passion."

What were the first two projects you had to complete as part of the chartering process?

Our first activity was a meetup focused on relationship-building, using "hacker trivia" where the participants answered a series of questions that were both pop culture- and technology-driven from varying topic areas.

The second activity was recruiting more people by inviting others into the chapter. We presented a "war game tabletop exercise," where members were provided the details of a security incident and had to explain how they would handle it. It was great, because you had a variety of people from different backgrounds being able to participate in an activity as a team of incident responders.

What advice would you give to members who are contemplating starting a chapter?

The most important advice I can think of for anyone wanting/planning to start a local chapter is to find people like you who have a passion for the community and want to make a difference. The strength of any chapter is in the members and leadership who support it. ■

SUSPICIOUS SITES

One in 10 URLs are malicious

Source: Symantec Internet Security Threat Report 2019

BREACH SOURCE

20%

of healthcare breaches in 2018 were caused by third-party vendors, in a survey of 600 organizations

Source: CynergisTek, Inc. Measuring Progress: Expanding the Horizon, April 2019

BUG TRACKING

$100,000

in rewards paid by the Netflix Bug Bounty program in its first year

Source: The Netflix Tech Blog, March 2019

RETURN TO CONTENTS

Resurrecting and Reinventing the Culture of Privacy

by Tony Vizza

A NUMBER OF YEARS AGO, I had a conversation with a senior cybersecurity professional about an upcoming census and the information security measures that were being deployed to protect the collected data. He proudly exclaimed to me that he was going to fly overseas the afternoon of census day and then fly home the following day in order to avoid filling out the census! Legally, he didn't have to complete the census at all if he was not in the country, and since he had no interest in sharing his personal information with the government, he made sure he acted legally in not providing census data.

For some, such a course of action may seem extreme. In the context of today's world, where many people happily *overshare* information on Facebook, Instagram or Twitter, some may think that flying overseas to avoid the census would be rather neurotic—particularly when they themselves happily post photos of boarding passes, the hotels they are staying at, and readily "tag" themselves at the restaurants they are dining at.

The culture of online sharing that exists today contrasts significantly with the concept of privacy that existed prior to the digital era. When I was a child, I remember asking an uncle who he had voted for in a general election. He chastised me for even asking, telling me that voting is a private matter and pointing out the measures set up to ensure a secret ballot. By comparison today, a quick scan of a Facebook newsfeed will very likely indicate to you who your family and friends are voting for during an election. There is no need to ask anymore!

Tony Vizza 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.

The art of privacy is dying at a rapid rate. For Gen X, millennials and Gen Z, an argument can be made that privacy is no longer a necessity, and, in fact, is the antithesis to how they want to live their lives. I often point out to organizational decision makers that if one of their younger staff members has no problems readily sharing extremely private personal information, why would they be concerned about their organization's information?

Recently, my family babysitter, who is in her early 20s, asked if it were possible for me to scan some documents she needed to send to her education provider and email them to her. Her email address was her full name followed by a number that, to my trained eye, appeared to be a date of birth. I asked her if it was and she said yes, it was her date of birth. I then suggested that she may want to change her email address to rectify this. Her response: "Why should I?"

> **We cannot expect information security to be successful until, as an industry, we collectively address how members of society value their privacy.**

The decline in the value of privacy presents a conundrum for information security professionals—particularly given that the concept of confidentiality is a pillar of information security strategies. How do we, as an industry, address this erosion of the value of privacy? How do we balance the "needs" of people to engage in social media and at the same time promote a message of online safety and the value of private information, to ensure confidentially measures both exist *and* are being maintained?

While it is true that many jurisdictions around the world are addressing privacy concerns in relation to information kept on their systems (with the most notable one being the EU and its GDPR mandate), these do not address privacy with respect to individuals and the personal information they willingly, or even contentedly volunteer, to be collected.

We cannot expect information security to be successful until, as an industry, we collectively address how members of society value their privacy. I am reminded of the words of author Katherine Neville who suggests that "privacy—like eating and breathing—is one of life's basic requirements." ■

RETURN TO CONTENTS

Play On

BY CRYSTAL BEDELL

How gamification can improve employee cybersecurity compliance

AS A FORMER CYBER ANALYST for the government, Masha Sedova has seen firsthand what a Russian state-sponsored attacker is capable of. So, when she was charged with building a security culture at Salesforce in 2012, she knew an employee newsletter and animated videos wouldn't prepare end users in the event of a targeted corporate attack.

"I thought, 'There's no way this will work. It's a waste of time,'" says Sedova, co-founder of Elevate Security in Berkeley, Calif. "In order for an organization to withstand an attack like that, people have to *want* to do security instead of *have* to. If it's just a check-the-box task, people will do the bare minimum and not any critical thinking. Unless I got people to buy into the idea that they could and needed to defend the network, I wasn't going to get any measurable security change."

ILLUSTRATION BY JEAN-FRANCOIS PODEVIN

George Gerchow also recognized early in his career the need to better engage end users with cybersecurity. "Policies, procedures and compliance are so dry. People sign policies without knowing what they're getting into. I thought there's gotta be something we can do to make this interesting," says the chief security officer at Sumo Logic, headquartered in Redwood City, Calif.

Like other security leaders, Sedova and Gerchow started experimenting with gamification to improve end user awareness. The results have been "remarkable," according to Gerchow.

"Over the course of this last year, we had a 10% reduction in end user risk. Most organizations, when they get compromised, it happens because an end user has a weak password, gets phished or downloads malware. The amount of education you need to do around these things is incredible. One percent to 2% is a win, but a 10% reduction is remarkable," Gerchow says.

Sedova has also seen quantifiable improvements in security awareness through gamification. During her tenure at Salesforce, she sent a phishing attack to two groups of people—those who had participated in her gamified training and those who had not. Alumni of her program were 50% less likely to click on a malicious link and 82% more likely to report the link.

WHAT IS GAMIFICATION?

So, what is gamification and why does it work?

"Gamification is taking game mechanics and applying them to business objectives. It focuses on autonomy, mastery, feedback, getting better at a particular task," Sedova explains. "Gamification helps with the motivation factor. It doesn't necessarily change the mindset. The thing I've realized is that people still might not care about security—that comes from a different place. It might not mean anything to me to be secure, but competition or winning or a sense of accomplishment might mean something to me."

Spencer Wilcox, the executive director of technology and security at PNM Resources in Albuquerque, N.M., puts it another way: "To me, gamification is the use of game-like structures—play, if you will—to incentivize people to act in the way you want them to."

A common example of gamification within cybersecurity is around phishing attacks. At Sumo Logic, for example, when users successfully identify and report a phishing attempt, they receive points that lead to different rewards. When users earn enough points, they can cash them in for a reward.

"That's worked out pretty well," Gerchow says. "The last thing you want is for people to hide when they do something wrong. You want transparency."

Annalea Ilg, chief information security officer at Involta in Cedar Rapids, Iowa, uses gamification to keep her SOC team apprised of the latest attack methods. Her goal is to reduce the team's mean-time-to-detect and mean-time-to-respond to attacks.

"Any way you can promote continual training in the security space is important," Ilg says. "At this point, the more creative ways we can find to keep security professionals up to date, the better. It's hard enough to find the talent, once you have it, you have to keep everyone educated because security is evolving and you have to keep evolving with it."

Ilg uses Project Ares, an online cybersecurity learning and assessment platform from Circadence. Team members "train" daily in Project Ares by attempting to stop a simulated attack as it moves through the kill chain. "The team goes in daily because there isn't a compromise every day. The more they can be familiar with the real-world scenario, the more ready they'll be. That's the real advantage. It's all about continuous readiness."

HOW TO IMPLEMENT GAMIFICATION

The first step to applying gamification to your cybersecurity training is to understand what behavior you want to drive. "Get really clear on what you want the outcome to be," Sedova says. "The behaviors should be the things you really want to change in your organization because you want to make your organization safer or reduce risk."

Once you've identified the behavior you want to improve, you need to establish a way to measure that behavior. "Ultimately, you want to recognize people who are doing great and give course-corrective feedback to those who aren't meeting the delta. In order to do that, you need data," Sedova says.

The next step is to determine how good behavior will be incentivized and bad behavior disincentivized. A common approach is to give or take away points accordingly. Karl Kapp, a professor of instructional technology at Bloomsburg University and author of *The Gamification of Learning and Instruction*, advises companies to be careful about what is emphasized in the points process.

"Rather than feedback around the game, give feedback messages around the behavior. That way when the employee is rewarded, it's aligned with the behavior you want to occur," Kapp advises. "Instead of telling a user they've earned 20 points, tell them they've successfully identified four phishing attempts, thereby saving the organization x dollars."

Users are often allowed to cash in their points for rewards. These, too, should be carefully considered. "The thing about rewards is to look at the culture and see what's

RETURN TO CONTENTS

valued in the culture and tap rewards into that," Kapp says.

For instance, if your company has a hectic, fast-paced environment and people burn out quickly, then extra time off might be a good incentive. Lunch with an executive might be highly valued if you're in a hierarchical environment where the average employee doesn't have access to upper management. In a retail environment where disposable income is an issue, then gift cards might be a good incentive.

Finally, don't underestimate the power of public recognition. "Rewards that are recognized company-wide visibly reinforce the behaviors you're driving. Employees know the company is paying attention and rewarding good behavior, and you're more likely to get more of it from other people," Sedova says.

> **"You need an executive suite sponsor and they should lead by example. If you're having classes on cybersecurity, that executive should attend."**
>
> *—Karl Kapp, professor of instructional technology, Bloomsburg University*

ENSURING SUCCESS; CHALLENGES TO AVOID

To be successful, gamification requires a team effort. Gerchow advises security leaders to get human resources staff involved early in the process. "Talk to people and get ideas from them," he says. Getting HR involved will not only reduce any concerns they may have about a competitive program, but it will also help security leaders sell the initiative to the rest of the company.

"HR is usually non-technical, so if you can get them to participate first, you're enabling a champion of the people. You're taking the people who look out for everyone within the organization, who have great communication skills and can help you sell to the organization," Gerchow says.

Experts also emphasize the importance of having executive support.

"You need an executive suite sponsor and they should lead by example. If you're having classes on cybersecurity, that executive should attend. A lot of times in organizations, executives launch the initiative but they're not part of it, and that sends the message that this is not very important," Kapp says.

It's also important to have direct-line supervisors on board, according to Kapp. They should be monitoring user behavior and providing verbal feedback whenever possible to reinforce the program. If positive feedback can be given within a group setting, that's even better.

Finally, Gerchow recommends starting small. "When I was at VMware, I got overly excited. I created a program that consumed too much effort and I could never get it going," he says. "Building momentum is key. Have quantifiable things you can measure—even if it's as simple as phishing. Start there, build, review it and then add on."

GAMIFICATION PLATFORMS

When it comes to technology for gamifying cybersecurity awareness training, companies have several options.

According to Kapp, there are two types of gamification platforms. There are learning platforms that ask questions, provide simulations and report on behavior. "All of that is divorced from the user's actual behavior."

Then there are performance-based gamification platforms. "These serve as an integration layer that can sit on top of your systems. That layer reports back into a dashboard or your LMS, where you can then monitor, track and report on user behavior," Kapp says.

Still another option is to build your own solution, as Gerchow's team at Sumo Logic did. Security developers built integrations between the company's public-facing Slack channel, "Ask the SOC," and Excel, where they can monitor and analyze the data from their various gamification efforts.

Much like the other components of gamification, experts agree that the platform that works best for one organization won't necessarily work as well for another. "It's not one-size-fits-all," Kapp says. "Trying to shoehorn into your organization gamification that worked for another organization won't work. Engineers are less likely to buy into a cartoony gamification platform versus HR folks or teachers, for example, while engineers love to solve problems. For them, you'll want to make it more problem focused than character focused."

Wilcox adds, "The more playful you make the environment, the more incentivizing and rewarding people will find the environment. You need to find the right balance of play and entertainment that the culture requires to build awareness, to reward good behavior and disincentivize poor behavior." ■

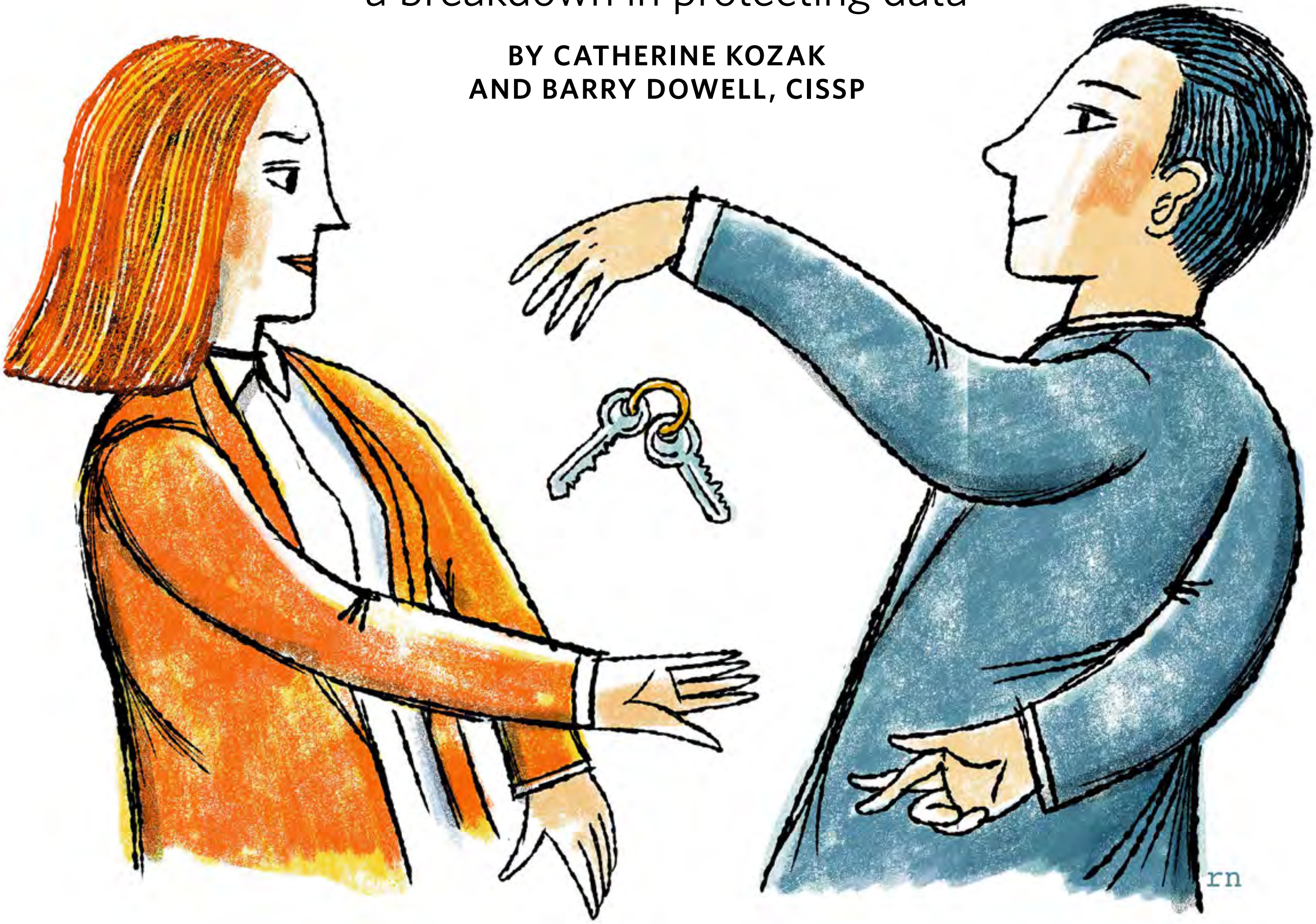
CRYSTAL BEDELL *is a freelance writer and past magazine contributor living and working in Spokane, Wash.*

RETURN TO CONTENTS

DO TELL

Fuzzy ethical guidelines can lead to a breakdown in protecting data

BY CATHERINE KOZAK
AND BARRY DOWELL, CISSP



IT WAS A ROUTINE CHANGING OF THE GUARD: a new contractor for IT services taking the reins. As expected, authorizations to access technical equipment and company systems were updated. And as is typical in such transitions, most lower-level staff, especially technicians, were retained at the customer worksite and managers and upper-level supervisors were relocated to other positions within the company. Some moved on to new roles elsewhere.

But unexpectedly, a morally questionable action transpired, setting up a potentially disastrous violation of standard ethical practices.

ILLUSTRATION BY ROBERT NEUBECKER

RETURN TO CONTENTS

FOLLOWING ORDERS—OR BREAKING THE RULES?

When the system administrator for the original prime contractor was instructed by management to change passwords for all devices the contractor had managed, the former employees were properly cut off from accessing and administering the devices, protecting the security and privacy for the new contractor and its customers.

The former administrator should have provided the updated passwords to the new contractors and system administrators as soon as possible. But in this case, the new contractor was given the wrong passwords.

More alarming, it was not immediately clear if system administrators who had changed the passwords declined to provide the new, correct ones at the behest of their employer—or because they were trying to create havoc for their former customer and co-workers. (The former was later confirmed by the former administrator, though "off the record.")

While doubtless an example of a grave, unethical act, if true, it may be less obvious how a cybersecurity professional should confront such a violation, especially if the employer lacks an ethics officer, or even an ethics policy.

ESTABLISHING ETHICS IN A RELATIVELY NEW INDUSTRY

Now part of nearly every facet of life worldwide, cybersecurity and subsequent ethics have become "a huge, huge challenge," says Sean Brooks with the Center for Long-term Cybersecurity at the University of California, Berkeley. "I think one of the things that we're really dealing with now is there is not a good sense of—not just in the cybersecurity industry, but in the broader tech industry—appreciation among the rank and file and also among corporate and private institutions about ethical obligations."

Even a well-respected member association such as (ISC)^2, established in 1989 during the early days of the digital revolution, cannot dictate industrywide ethical behavior. But from its inception, the organization's founders saw the need to create standards, certifications and ethical guidelines for the cybersecurity industry. "This is something, if you want to become a member of (ISC)^2 and to obtain our certifications, besides [having] necessary experience, besides passing the exam and having the recommendations of your colleagues, you have to obey the Code of Ethics," says Biljana Cerin, CISSP, (ISC)^2 Board Ethics Committee chair.

Developed by "seasoned experts" in the field, Cerin explains that the (ISC)^2 Code of Ethics is based on four canons, with the first one being the most important:

- Protect society, the common good, necessary public trust and confidence and the infrastructure;
- Act honorably, honestly, justly, responsibly and legally;
- Provide diligent and competent service to principals;
- Advance and protect the profession.

The reinforcement of ethics in the profession, found in educational programs, conferences and online, is a large part of why an (ISC)^2 certification is considered the gold standard in the industry, Cerin asserts. Prominently displayed on the organization's website is its Code of Ethics: "The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this Code is a condition of certification."

ESTABLISHING THE RULES

Ethical standards also require lawful behavior, a melding that can be difficult in a profession that operates worldwide. At its core, ethical behavior requires making principled judgment calls based on different circumstances, Cerin explains, whether or not allowed under law.

"We have more than 140,000 members and those members work in different legal environments," she says. "Maybe something that is legal in one country is not legal in another one. So, it always comes down to: 'What am I—a professional in the field having, for example, favored access to some information? Seeing things that maybe other people are not able to see? What can I do to make sure I act professionally?'"

Still, employees and contractors should have guidance on ethical codes and violations from the organizations themselves. "That's where I think all of us should start," Cerin states. "It's kind of amazing how many companies don't have internal regulations that actually explain to people … the security policy or acceptable use policy."

Too often, ethical dilemmas in the cybersecurity workspace leave people feeling confused or powerless.

For instance, in the opening scenario where the system administrators provided the wrong passwords, they claimed to be following an order from their contractor's management to change the passwords and not give the correct passwords to their customer. Assuming the administrator was telling the truth, the management was attempting to cause harm to the soon-to-be former customers, and their conduct would certainly be considered unethical.

The administrators were given what in the military would be termed "an unlawful order." In the best of circumstances, that order could have been ignored and the correct information passed on. Unfortunately, there are myriad rea-

RETURN TO CONTENTS

sons for what appears to be an obvious response. Perhaps there is fear of retribution or losing one's job. Perhaps the company lacks proper whistleblower protection, or there is no protocol in place to address violations. Perhaps the administrator simply feels obligated to obey his or her superior or is incentivized with promises for future work.

> "I think we need a lot more conversations within industry groups and within the classes that train the people who will become the professionals."
>
> *—Irina Raicu, director of the internet ethics program at the Markkula Center for Applied Ethics, Santa Clara University*

THE CHALLENGE OF ENFORCEMENT

By nature, ethics are "nuanced and contextual" and reflect the "inherent complexity of human life and human interaction," explains Irina Raicu, director of the internet ethics program at the Markkula Center for Applied Ethics at Santa Clara University.

"We make ethical decisions all the time about what is the right thing to do in our interactions with other people, and about what kind of people we want to be when we take certain actions," Raicu says. "Laws, at their best, are codified ethics. They are things that we, as a society, have reached some decision that this is the right thing to do or this is the wrong thing to do. And the fact that it's difficult, and we may not agree on them, does not mean we don't have to make those decisions.

"And we make them according to our values and trying to help as many people as possible and hurt as few people as possible. So that's where ethics comes in—when there's no law that tells you exactly what to do or what not to do."

It can be helpful, advises Raicu, to look through different perspectives in making decisions that are aligned with one's values. The Markkula Center teaches a framework for ethical decision making that looks at it through five lenses: rights, justice, utilitarianism, common good, and virtue ethics. For a long time, she says, expectations in the industry were focused solely on skills with technology and protection of data.

But now there's greater understanding that ethical considerations are just as important for cybersecurity professionals, who often balance complex security situations under intense stress. "Those are the kinds of things that can't be addressed at the moment of crisis, when they discover a breach or something," Raicu warns. "I think we need a lot more conversations within industry groups and within the classes that train the people who will become the professionals."

Massive data breaches and hacking of public and private devices have become common, leading to more scrutiny of the ethical behavior of cybersecurity professionals. As a result, says UC Berkeley's Brooks, the culture of the industry is evolving to incorporate more ethical education and standards.

"But a lot of it is, these are companies, large institutions that have been built by folks who, by the nature of the career path, have never been forced to engage at an intellectual level with some of these more—I hate to use this term—'soft' issues around ethics and social responsibility and things like that," he says. "It's just not something that engineering educational programs have emphasized in the past, [and] there's no regulations to force the issues on companies."

If anything, the rapid-fire transformation to a data-driven, interconnected world has dramatically demonstrated that, absent ethical conduct by cybersecurity professionals, there's real potential, advises Brooks, "for truly bad things to happen."

One example he cites was the recent revelation that former U.S. government cybersecurity personnel had participated in hacking into accounts belonging to journalists and human rights advocates for the United Arab Emirates, and that some data from U.S. citizens had been swept up in the process. It's the kind of situation that should serve as a warning, "that there's now a fully formed class of professionals in the cybersecurity space."

CREATING A MORE ETHICS-ORIENTED CULTURE

From the earliest days of the tech fields, the career path for information security has been in the private sector, defense and intelligence communities, Brooks says. "That creates an institutional bias in the entire field around what is and what isn't permissible behavior. So, there's this whole class of professionals out there—some have built skills on the defensive side, some have built skills on the offensive side, some of whom have personal ethical frameworks, some of whom don't. You don't have strong industry standards about what is acceptable practice, and part of that is it's a rapidly changing space."

Even when there are professional associations like (ISC)^2 to support and certify cybersecurity professionals, Brooks says that the standards offered by the dozen or so groups for the industry tend to be uncoordinated and often competitive. Certifications have merit, he adds, but without enforcement and unified industry standards or a review board, they fall short of being the cyber industry's version of American Medical Association licenses.

RETURN TO CONTENTS

Companies also have learned that best practices require multiple individuals who have appropriate access to systems and services to prevent the vulnerability of a single point of failure.

As the case of the systems administrator who mishandled password information illustrates, the possibility of a disgruntled employee or contractor can present an especially dangerous threat to company security. That's why it is common for terminated employees to immediately have their system access removed and be escorted from premises. Companies also have learned that best practices require multiple individuals who have appropriate access to systems and services to prevent the vulnerability of a single point of failure.

Ethical conduct is a critical workplace component in the cybersecurity industry, but it can still be overlooked, undervalued or unsupported. Still, that's no excuse to plead ignorance or not seek guidance, Brooks says.

"There are long-term issues around education, and ethics and professional standards, but I think for people who are in the field now, some of it is just really swallowing your pride and knowing how to ask for help from people who are outside your field. Because that's going to be critical to making you better at your job." ■

CATHERINE KOZAK *is a freelance writer and past magazine contributor who lives and works on the Outer Banks of North Carolina.*

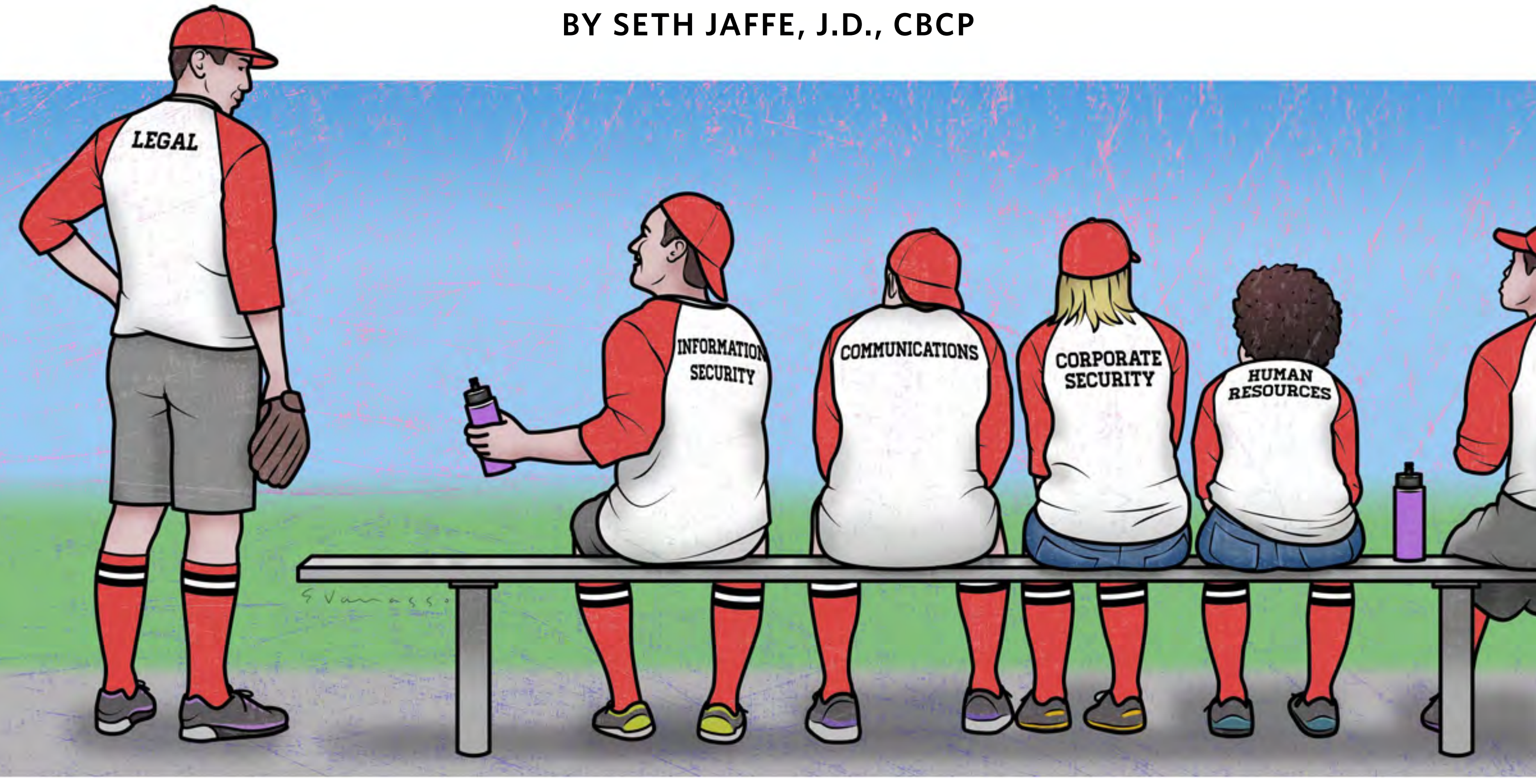
BARRY DOWELL, *CISSP, is an information systems security official working as a contractor for a U.S. government agency. He has worked for that agency for more than 16 years, the majority of which were as a systems engineer and information systems security official.*

RETURN TO CONTENTS

IMPROVE YOUR INCIDENT RESPONSE

Ways to leverage your legal team and others prior to a cyber event

BY SETH JAFFE, J.D., CBCP



MOST INCIDENT RESPONSE PLANS arise within the information security or information technology departments, but in-house counsel certainly has a dog in the fight. When cyber events rise to the enterprise level, it's all-hands-on-deck to respond efficiently and effectively, and counsel is on the front line.

All too often, though, the legal department is left out of an incident response until late in the game, oftentimes leading to inflated damages from subsequent data breach litigation. That doesn't need to happen, so let's explore opportunities for cybersecurity and legal to work together.

ILLUSTRATION BY ENRICO VARRASSO

RETURN TO CONTENTS

ESTABLISH A CYBERSECURITY COMMITTEE

In the face of lackluster cybersecurity policies, members of a company's board of directors may find themselves personally liable for a data breach.[1] As a result, numerous authorities recommend including on the board a member with cybersecurity knowledge.

That's not always feasible, so a second option is to create a cybersecurity committee tasked with briefing the board at regular intervals. A cybersecurity committee should include, among others, representatives from information security and legal, both of whom are instrumental in assisting the board with enforcing policies sufficient to satisfy the directors' duties of care and loyalty.

EXPECTATIONS FOR ATTORNEY-CLIENT PRIVILEGE

Information security personnel, in their desire to bring a cyber incident under control, all too often jump the gun by engaging forensic vendors without involving a legal team member. The communications and reports from that engagement can come back to haunt the company in post-breach litigation.

Known as "attorney-client privilege," communications to and from legal representation for the purpose of obtaining legal advice are, for the most part, protected from disclosure. Early involvement of legal provides the opportunity to bring third-party vendors under the privilege, which in turn allows for better communication during a stressful and time-crunched period.

The privilege plays out within a company itself as well, allowing the incident response team members to freely discuss what may have been the cause of the incident without fear that said communications will become evidence of culpability in a subsequent jury trial.

Even without the privilege, the legal team member should brief the incident response team early about communication best practices. As an example, team members should avoid conjecture, instead focusing on the facts and limiting communication only to what is required.

In addition, team members should limit communications to those with a need to know, and they should make clear that those communications are confidential and, if applicable, attorney-client privileged.

NEGOTIATING CYBERSECURITY INSURANCE

Enterprise-wide cybersecurity events generally come with dollar signs attached, the cost of which can be difficult to stomach.

Many companies choose to take out cybersecurity policies to offset that cost, but like any insurance, there are exceptions and exclusions. In recent cases now working through the courts, insurance carriers have denied claims on numerous bases. Failure to comply with minimum required procedures and risk controls, for example, has been the cause of a denial.

In one example, restauranteur P.F. Chang's found its claim denied because the carrier argued that the restaurant was not injured by the cyber breach, but rather its customers were injured. Sony got a taste of the "incorrect party" denial as well when its carrier refused to pay a violation of privacy claim because, as Zurich Insurance argued, it was the hackers who published the material, not Sony. And lately, carriers are denying claims citing the "act of war" exclusion, arguing that attacks facilitated by nation-state actors are outside the cyber insurance policy.

For data breaches originating with a third-party vendor, claims are often dictated by contractual obligations written years before in applicable master services agreements.

What's clear, in light of the aforementioned claim denials, is that legal and information security should work together during procurement and negotiation of cyber insurance policies—not only to minimize exceptions and exclusions, but also to understand them as applied to ongoing policies and procedures.

And the legal implications of cost shifting do not stop at insurance claims. For data breaches originating with a third-party vendor, claims are often dictated by contractual obligations written years before in applicable master services agreements. Here again, legal must work with information security to settle on cybersecurity provisions correctly tailored for each vendor in view of the types of data processed by the third party.

FULFILLING NOTIFICATION OBLIGATIONS

At present, all 50 U.S. states have data breach notification laws on the books, obligating a company to disclose certain facts of the breach to either the affected data subjects, a state authority like the attorney general, or both. Notification obligations, however, differ by jurisdiction.

RETURN TO CONTENTS

It is the job of the legal team member, and outside counsel, to assess whether a cyber incident has risen to the level of a breach, thereby triggering obligations within the law. Notification obligations, however, do not live solely in state data breach laws, but also are found at the national level, internationally, through associations and contractually.

In carrying out required notifications, the legal team members assume a number of roles. They work with the communications department to craft the language of the notification letter, ensuring it meets state requirements. Where data breach notification vendors are needed, legal engages and manages them to ensure compliance with law. And early participation in the incident response process better prepares legal to field inquiries from regulators.

DATA BREACH LITIGATION

Class action suits stemming from data breaches are on the rise. As a result, companies victimized by cyberattacks find themselves having to relive the breach in a courtroom.

Certain measures can be put in place prior to a cyber event that will situate a company on more favorable footing when plaintiff attorneys come knocking. Standing to bring suit, for example, is a major issue in data breach litigation and can offer a strong defense in protection of a victimized company. Plaintiffs must show an injury in fact, a causal connection between the claimed injury and the defendant's acts, and that the alleged injury would be redressed by a favorable decision in the lawsuit.

> **Working together, information security and legal can put in place policies and procedures that lessen the chance for the plaintiffs to get past the second prong—causality.**

Working together, information security and legal can put in place policies and procedures that lessen the chance for the plaintiffs to get past the second prong—causality.

Attorneys often play the long game; during an incident, legal members of the incident response team will be preparing for litigation by quarterbacking litigation hold notices, overseeing electronic discovery, memorializing facts that may prove useful at trial, and organizing the theory of the case.

UPDATING THE INCIDENT RESPONSE PLAN

Many cybersecurity laws already mandate regular updates to a data security program;[2] regardless, it is just good practice.

Updates should occur in numerous instances, including upon major changes in infrastructure, as a result of organizational change, due to new programs that affect the privacy of data subjects, and at least annually in view of changing laws and regulations.

For obvious reasons, the legal team member, in conjunction with information security, should lead this initiative. Failure to do so may well paint a target on the back of the company, leading to regulatory oversight, fines, public relations nightmares and litigation.

DATA SECURITY IS A TEAM EFFORT

In a few short years cybersecurity has moved from relative obscurity to the forefront of compliance and risk mitigation. Consequently, data security is a team effort involving nearly every department related to compliance. Yet many information security departments are still going it alone.

Now is the time to establish ongoing relationships with other participants of the incident response team, whether they be the communications department, corporate security, human resources or especially legal.

In-house and outside counsel can be an invaluable partner to information security teams in lowering risk and protecting the company from damages associated with cyber incidents. Information security professionals would do well to take their own advice—don't wait until you're in the midst of a breach to make your move. Bridge the gap in your institution today. ■

SETH JAFFE, *J.D., CBCP, is vice president of incident response and general counsel for LEO Cyber Security.*

FOOTNOTES:

[1] The directors of Home Depot, Wyndham Hotels and Target faced shareholder derivative suits following their respective data breach events.

[2] As an example, the Alabama Data Breach Notification Act ("adjustment of security measures to account for changes in circumstances"); FTC Red Flags Rule ("Ensure the Program is updated periodically"); HIPAA Security Rule ("update as needed"); Massachusetts CMR 17.03 ("Reviewing the scope of the security measures at least annually"); NY-DFS Section 500 ("assessed and updated as necessary by the CISO").

RETURN TO CONTENTS

What Are *You* Doing for Cybersecurity Awareness Month?

by Pat Craven

AS CYBERSECURITY AND CYBER SAFETY continue to become a growing global conversation, there are an increasing number of themed days and events to help promote the industry and highlight the need to educate people on how to be safe online. One of the biggest promotions of the year is Cybersecurity Awareness Month in October.

October is a busy time of year for your Center for Cyber Safety and Education. We plan all year for Cybersecurity Awareness Month, and I wanted to share with you some ideas for ways that you individually, your (ISC)² chapter, or your company can help us achieve our collective mission of building a safer cyber world.

Is your town ready for a Garfield-sized event in October? If so, now is the time to start planning. For us, one of the biggest things we will celebrate is a Cyber Safety Day. Our main effort this year will be in Orlando on Wednesday, October 30, during (ISC)² Security Congress, but there will also be other cities that we hope to expand to as well.

Last year, we piloted the effort in New Orleans and reached more than 2,300 children in 17 schools. This year, our goal is to reach some 10,000 children with the *Garfield's Cyber Safety Adventures* program in one day! To pull off these types of events takes a coordinated effort and requires a team of people and financial support from local businesses. If your chapter or company is interested in taking on such a project in your town, reach out to us at center@isc2.org for help and guidance.

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

But you do have more options available to help your community, aside from our Garfield program. You can have the same kind of impact coordinating free presentations for parents, families and seniors at local schools, libraries or community centers. The idea is to decide upon a date and a common goal. Something that will rally people in your group, company and the community. These types of events can often be of interest to the local media, so don't hesitate to invite them to see how your group is working to help families be safe and secure online. All the resources you need are available for free and downloadable in multiple languages at www.IAmCyberSafe.org.

Illustration: MHJ/iStock

October is also a great month to promote cyber safety and security through blogs, social media and local media (newspaper, radio and TV). Reach out to bloggers and podcasters to find out if they are looking for a cyber expert on this very hot topic. Keep in mind that most podcasts and stories are recorded well in advance of their release, so don't wait too long to contact them, or you may miss out. If you're not comfortable doing interviews, then simply retweet or post on your favorite platform.

We have a variety of safety messages going out all year long, so make sure you follow us on Facebook, Twitter, Instagram and LinkedIn. Don't forget to opt-in to receive information from the Center in your membership profile.

Your Center for Cyber Safety and Education is always looking for ways to partner with professionals and companies to make it a safer cyber world for everyone. Please don't hesitate to ask for help or ideas on what you can do to give back and help others be safe and secure online. ■

RETURN TO CONTENTS

(ISC)²® community ▮▮▮ SHARING INSIGHTS FROM BUZZWORTHY THREADS

Join the (ISC)² Community ›

Highlights from Recent Discussions on the (ISC)² Online Forum

The (ISC)² Community has more than 20,000 cybersecurity professionals connecting, sharing knowledge and offering solutions in the online forum. *InfoSecurity Professional*, in partnership with the Community's administrators, presents a few of the more buzzworthy threads. Note that the questions and responses may have been edited for clarity and brevity.

QUESTION:

Please help me clear [up] ambiguity regarding VPNs. I have a VPN installed on my personal device. I would like to connect to http://www.iluom.com, which is hosted by a web service and is not an HTTPS website. When I connect to the website, I use my VPN service. My data is encrypted since I'm using their application; [it] goes in encrypted form to the ISP, then to the VPN server. The VPN server is the third party that connects to the web on my behalf. Now, from this point the VPN server should take it forward, but there is no secure session or TLS handshake between the VPN server and www.iluom.com. It's an open communication to the website. So in this scenario, how does the VPN help me to secure the info?

—Submitted by iluom

SELECTED REPLIES:

Your VPN will only protect your traffic up to the VPN server. If you want end-to-end encryption, then you need to change your website to use HTTPS or only connect to websites using HTTPS. Most websites on the WWW now also/only offer HTTPS. To be absolutely sure no one is snooping on your traffic, check that each website's certificate is all in order when you connect.

—Submitted by AlecTrevelyan

Let me try to simplify it: There's a VPN user (A), a VPN server (B) and a destination server (C). When the user communicates with C, the traffic path will be A – B – C. The VPN tunnel itself only gets established between A and B, so ALL traffic between these points will be secured. There won't be any tunneling between B and C—so unless the destination server uses HTTPS, traffic between these points won't be secured.

—Submitted by Shannon

First off, just because VPN stands for "virtual private network" doesn't necessarily mean that it keeps you anonymous in any way. The "private" part refers to management (your ability to manage a network link over a public network), not necessarily encryption. There are many VPN technologies. Some have encryption (or encryption capabilities, and you have to turn them on to use them) and many, many don't.

—Submitted by rslade

Find this complete thread here.

QUESTION:

The BC [business continuity] guys and gals often complain that the security folks don't invite them to the party. Security folks complain about how BCP [business continuity planning] tries to be the directors in the crisis matrix. Nobody (particularly stakeholders and shareholders) wins when the bickering and dickering sours the matrix. Does anyone have experience or ideas they might share as to how we can "all just get along?"

—Submitted by j_M007

SELECTED REPLIES:

Have to agree that the bickering can actually be very damaging to the organization, sometimes more so than an event. Having lived through several events, I did the following:

1. Set up quarterly meetings to discuss issues and concepts between the groups (sometimes this had to be monthly)
2. Ensured that security folks were invited to DR exercises (in my case they owned authentication and authorization, the firewalls and the proxy servers)
3. Asked both teams to review all documentation
4. Developed an organization chart for DR exercises showing all reporting lines
5. Asked the CIO of the organization to notate who was the lead and approve 1 thru 4.

Really cut down on the bickering about who owned what. Maybe I was lucky but this worked for me.

—Submitted by dcontesti

In my experience, I've always found that developing a good relationship between the two "teams" before any incident applies bears most fruit. As long as roles and responsibilities are clearly defined, then there is little to bicker about. Most importantly, it's crucial to take away the perceived "importance hierarchy" when nasty issues arise. Better to have a common goal, a consensus if you will, that allows objection provided it's constructive and sensible. After all, we are all working toward the same rough objectives.

—Submitted by HTCPCP-TEA

Find this complete thread here.

RETURN TO CONTENTS