MOVING THE NEEDLE ON DELIVERING MEMBER VALUE

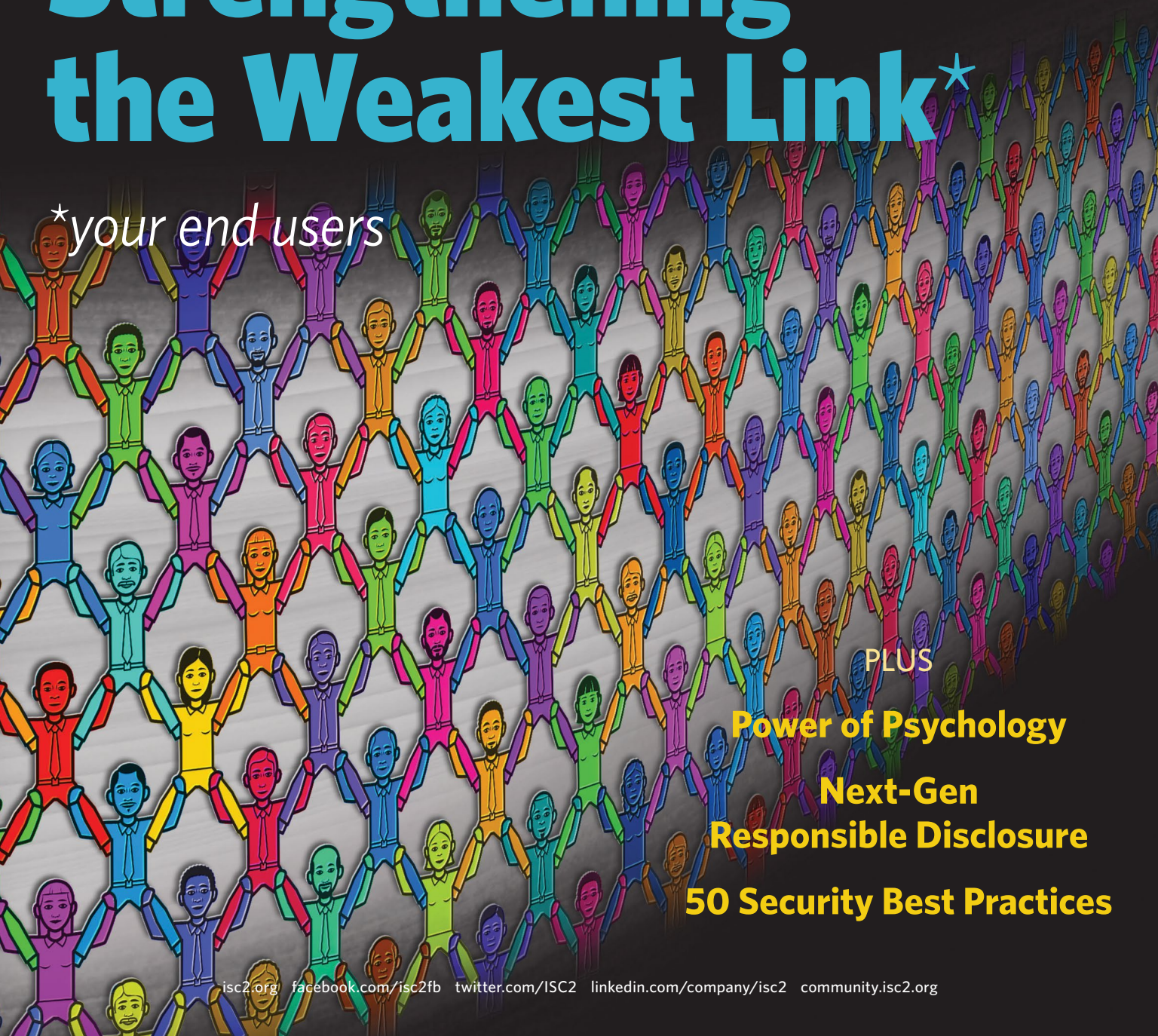
InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

MARCH/APRIL 2020

Strengthening the Weakest Link*

**your end users*



PLUS

Power of Psychology

Next-Gen Responsible Disclosure

50 Security Best Practices

CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

Commit to CCSP CERTIFICATION in 2020

Here's Everything You Need to Succeed – Without Excuses

You know that preparing for an (ISC)² certification is a BIG commitment. You also know that the CCSP will help you stay on top of growing cloud security demands and build critical skills. If not for your busy schedule you probably would have gone for it by now.

We get that life is hectic. But don't let another 365 days slip by! Make 2020 your year for CCSP certification.

Get started today with our no-excuses guide to success.

(ISC)² Exam Action Plan ▶

contents

VOLUME 13 • ISSUE 2

PAGE 17

features

Cover illustration: ENRICO VARRASSO Illustration above: DAN SIPPLE

departments

InfoSecurity Professional is produced by Twirling Tiger® Media, 7 Jeffrey Road, Franklin, MA 02038. Contact by email: asaita@isc2.org.

Ah, Users

AS YOU READ THROUGH this issue of *InfoSecurity Professional*, I want you to think long and hard about who and how you serve. Your function on a strategic level is to keep a business from being disrupted or damaged by various violations and increasingly sophisticated cyberattacks. Just how you do that is broad in scope and highly individualistic. But every cybersecurity professional in every organization has the same mandate: Do your job so everyone else can continue to do his or her own job.

That means your users likely will never take security as seriously as you do. Even after their flimsy credentials are compromised. Or they forget to check with the real CFO before emailing financial data to a fake one. All of the fear, uncertainty and doubt you throw at them won't stick, at least for long.

Legislators and regulators may now require your top-line executives to do right by their customers, but those government assists come with heavy fists. Some of you resent anyone, let alone lawmakers, telling you how to do your job. Some of you balk at the additional burdens achieving compliance now requires. Some of you know you should fully read up on new regulations, standards and threats. You also should keep up with messages in your inbox. But you've got more important work to do, like currently keeping an eye on Bob in accounting accessing a database he shouldn't and preventing someone using stolen vendor credentials from gaining remote (and, gulp, root) access.

Anne Saita, editor-in-chief, lives and works on the U.S. West Coast. She can be reached at asaita@isc2.org.

I get it. We all get it. That's because we're all busy trying to do our best at what we best do. That, unfortunately, leaves little time to listen to lectures and thoroughly read security policies, maybe even to give ample attention to security awareness training. Your users may want to know how to help you, but their priority is to build that software, market that product, provide that service, acquire that new customer and forge that profitable partnership. Because if they don't, the company will be gone. And so, my friends, will you. ■

ADVERTISER INDEX

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

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 Eagle
727-683-0146
keagle@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

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

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

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

Moving the Needle on Delivering Member Value

by Wesley Simpson

LAST YEAR BROUGHT many changes to our association. But one thing never changes: our commitment to deliver highly valuable programs and content to our members and associates. As we move deeper into 2020, we'll continue to create more CPE-earning opportunities, advocate for our profession and maximize member benefits. The following are just a few ways we intend to do that going forward.

More from PDI

In 2019, we launched the Professional Development Institute (PDI) as a brand new platform for learning opportunities and continuing professional development. Having just celebrated its first anniversary, the PDI now offers more than 30 courses across a broad range of topics (and formats), including Moving to the Cloud, Security in the IoT Ecosystem, Communicating with the C-Suite and Integrating Security into DevOps. We'll be introducing several more courses throughout the year, and I encourage you to take advantage of these free courses that non-members must purchase.

(ISC)² Security Congress moves to November

In 2019 we hosted our largest (ISC)² Security Congress to date, with 2,500 attendees and more than 250 speakers. This year's annual Security Congress will be held a bit later in the year, from November 16-18, at the Hyatt Regency Hotel in Orlando. If you haven't been to a Security Congress, make this the year that you attend so you can experience relevant educational sessions, networking opportunities and world-class keynotes.

Wesley Simpson is the COO of (ISC)². He can be reached at wsimpson@isc2.org.

Webinar library will continue to be stocked

Last year (ISC)² delivered more than 160 webcasts across the globe, and our EMEA Channel was recognized as an All-Star Partner by BrightTALK. There's a vast library of some 800 webcasts available to view on demand. These educational webinars are a way for you as (ISC)² members to stay current in your fields and discover new ideas and approaches while earning CPEs. We also introduced closed captioning in 2019 for webcasts in English and will be rolling out the service for other languages later this year.

Industry research to advocate for cybersecurity growth

Our latest Cybersecurity Workforce Study found the cybersecurity skills shortage growing to more than 4 million needed professionals, and for the first time, it also estimated the existing workforce at 2.8 million. Other 2019 research reports included our Women in Cybersecurity Study, Securing the Partner Ecosystem and Cybersecurity Assessments in Mergers & Acquisitions. We're working on several upcoming studies to uncover new insights on the industry and those who work within it.

Keeping our community cyber safe through new student programs for all children

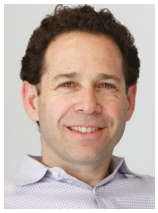
The Center for Cyber Safety and Education, the charitable arm of (ISC)², is expanding the Safe and Secure Online program to a new audience: high school students. *Vita Unplugged*, currently being piloted, teaches teens about healthy screen time and life balance. The Safe and Secure materials for parents, senior citizens and middle school students is available in more than 24 languages. The award-winning children's program, *Garfield's Cyber Safety Adventures*, has been translated into Spanish and is in its creative stages to begin establishing the program in Latin America. ■

(ISC)² Welcomes New Board Members

THREE VETERAN CYBERSECURITY EXECUTIVES have been elected to the (ISC)² Board of Directors, volunteering their extensive and varied experiences to the mission of the organization. New to the Board this year:

Aloysius Cheang, CISSP, is based in Singapore. He is a director and executive vice president/APAC for the Centre for Strategic Cyberspace + International Studies, a think tank based in the United Kingdom. Additionally, he is a director with AC3Labs in Singapore and co-founder of Taiwan-based IoT and blockchain security startups iSync-Group Inc. and Doqubiz Inc. As an international security expert, Aloysius has contributed to ISO and ITU-T and has been interviewed multiple times by the BBC, *The Times of London*, *The Wall Street Journal*, *Xinhua News*, SCMP.com and other international news outlets.

Yiannis Pavlosoglou, CISSP, is based in the United Kingdom. He is the CISO for the U.K. region of financial services firm UBS. He has experience in practiced operational resilience, NIST, CERT RMM, ethical hacking, coding and process excellence. His governance experience includes providing quarterly updates to U.K. boards and regulators.



David Melnick, CIPP/E/US, CISA, CISSP, is vice president of web isolation at Proofpoint and the previous founder and CEO of security firm WebLife. In his 25 years of experience in technology and security, David has worked extensively with both U.S. and global companies on their technology and cybersecurity needs, implementing security technology and addressing privacy regulatory requirements including global and U.S. federal and various state privacy requirements. David has authored several books including *PDA Security: Incorporating Handhelds into the Enterprise*.

The three join re-elected members **Arthur R. Friedman**, CISSP, and **Zachary Tudor**, CISSP. Both are from the United States.

"We are excited that these outstanding professionals have agreed to lend their time and talents to our association," said (ISC)² CEO David Shearer, CISSP. "Their unique experiences and professional insights will help us address our goal of advancing the cybersecurity profession and inspiring a safe and secure cyber world."

The 13-member board is composed of (ISC)² members—all volunteers—who provide strategy, governance and oversight for the organization, grant certifications to qualifying candidates and enforce adherence to the (ISC)² Code of Ethics.

Payment Card Information Needs More Protections

The 2019 Verizon Payment Security Report surveyed 302 global organizations to assess the level of fulfillment in meeting Payment Card Industry Data Security Standards (PCI DSS). The findings suggest companies have a long way to go to achieving full compliance.

LOW COMPLIANCE

36.7%

of companies surveyed achieved full compliance with Payment Card Information (PCI) requirements

ON THE SECTOR SPECTRUM

Industry with the Lowest Compliance: **Hospitality**	**26.3%**
Industry with the Highest Compliance: **Finance**	**39%**

CISSPs In and Outside the Office

ONE OF THE FIRST things Kelly Dial, CISSP, had to learn after joining the cybersecurity team at HP in Boise, Idaho, was to call fellow CISSP and the current HP Head of Cybersecurity Assurance, Gary Miller, by his first name. That wouldn't seem unusual, except that outside of work, Kelly has another name for the U.S. Air Force veteran and former Boise State University network manager: Dad.

Kelly Dial and her dad, Gary Miller, are both CISSPs at HP in Boise, Idaho.

"It's natural now to call him Gary at work, but I did have to be cautious in the beginning," Dial says when asked about the pros and cons of working with your father. "It's been a great experience working alongside my dad."

Her father, who's worked at HP for 26 years, agrees that there are benefits to working with family members in similar career fields as it enables the opportunity to have ad-hoc, in-depth discussions about technology breakthroughs and career growth through ongoing education, such as (ISC)²'s certifications and graduate-level studies.

"There are no cons for me," Miller says, "just a lot of pride when I hear people speak so highly about my daughter without knowing the connection, as she's married and has a different last name."

Among the biggest pros for Dial is the mentorship provided by her father as she continues to expand her cybersecurity resume. In addition to achieving her CISSP, Kelly's also a CEH and CHFI and currently serves as a senior cybersecurity analyst.

Miller evangelizes that regardless of age, ongoing education is the key to being a top security practitioner or leader and continues to earn certifications, including CISM, CRISC and CIS LI LA. Unlike his daughter, who found the CISSP exam easier than expected after four months of intensive studying, Miller thought the exam was difficult due to the [then] six-hour exam on paper. "I'd never taken a test that took that long."

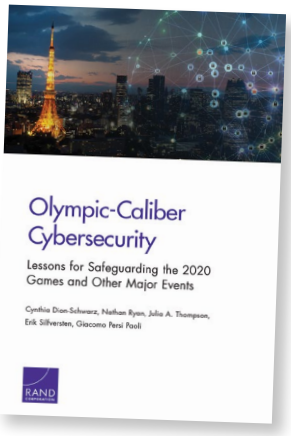
Both passed on their first attempt.

Father and daughter also earned master's degrees while at HP: Gary has an MBA from the University of Washington, while Kelly recently earned an M.S. in Cybersecurity and Information Assurance from Western Governors University.

"I found my niche," Dial says. "I find cybersecurity fascinating and through earning my master's degree and various certifications, I've been able to enhance my skills and focus. The CISSP was a huge motivator and empowered me to continue learning and advancing in the cybersecurity field." ■

—Anne Saita

Let the Games Begin



Olympic cybersecurity teams are bracing for some heart-stopping moves during this summer's Olympic Games in Tokyo. None have to do with athletic performances. A Rand Corp. report titled *Olympic-Caliber Cybersecurity* outlines the top threats and who is most likely to attempt an attack.

Top 4 Cyber Threats to the Games

1. Targeted attacks aimed at high-profile Olympic assets
2. Distributed denial of service (DDoS) attacks against Tokyo 2020 infrastructure
3. Ransomware attacks against a variety of devices held by participants, visitors and services
4. Cyber propaganda or misinformation against individuals, sponsors and nations

6 Most Likely Cyber Attackers at the Games

1. Foreign intelligence services
2. Cyber terrorists
3. Cyber criminals/organized crime
4. Hacktivists
5. Insider threats
6. Ticket scalpers

MEMBER SPOTLIGHT

Wilson España Carrasco of Chile: Putting Family First (for Everyone on a Security Team)

Wilson España Carrasco, 49, is a Chilean computer engineer recently featured in the first Spanish language webinar for (ISC)². We wanted to learn more about the husband of 17 years and father of three daughters, ages 9 to 15.

What was your career before becoming a CISSP? What do you do at your current job?

Before obtaining my professional certification, I worked as a security project engineer for a company operating in several Latin American countries. I participated in projects led by the professional services unit, in which I could apply all my technical knowledge in information security management and consulting. Currently I am a CISO, mostly working in structuring and implementing effective risk management strategies in all dimensions—operations, technology, cybersecurity, business continuity, etc.

What were your dreams when you started in cybersecurity?

I was around 35 years old when I formally entered the field; however, my journey began long before I decided to enter the field and obtain my CISSP certification. Before that, I was too technical, applying criteria that were limited to my scope of professional responsibility, without a cross-sectional and holistic vision.

I guess I didn't have big dreams for my professional life at that time; I more focused on starting a family with my wife, establishing roots and values and not falling into the craziness of daily life, not being successful at any price and not detaching from our family.

"I believe that generational differences today are a tremendous challenge for professionals who fear exercising leadership. It's an approach that enables understanding the generations, and how they differ in their approaches to their work."

—Wilson España Carrasco

Today I dream about sharing my knowledge and experience with real important things that are crucial to a safe and secure world. One of them is to promote the teaching of cybersecurity in schools and for people in general. I would love to see cybersecurity adopted as public education policy in all Chilean schools—and in the rest of the world too, specifically Safe and Secure Online's Garfield program.

How do you manage four different generations of team members, specifically ensuring everyone gets time off as needed without creating holes in coverage or unfairness?

I believe that generational differences today are a tremendous challenge for professionals who fear exercising leadership. It's an approach that enables understanding the generations, and how they differ in their approaches to their work. We understand each other much better when we share a common purpose and we throw ourselves into achieving it.

Regarding balancing everyone's needs, I always try to apply a basic principle that has accompanied me my entire career: family comes first, no matter how successful you are, no matter how hard you try to achieve that dream position. If by getting [it] all that you sacrifice your family, then you do not understand anything about why we do what we do.

I remember a situation that happened a long time ago in which a member of my team was very busy trying to deliver a report that happened to be on the same day as his daughter's school activity. When I offered to take care of the report, so he could be with his family, he asked me: "Why are you doing this? This is my responsibility, and you are my boss." Then I answered: "If your job and the commitment of your colleagues, including your boss,

do not allow you to have the opportunity to attend your kids' school activities, then this is not the place where you should be." Then two other colleagues helped me finish the report on time. In my humble opinion, respecting that principle consequently creates commitment among the team. Everyone will work in order to cover our professional responsibilities.

When you pursued your CISSP, how did you balance time studying with working and maintaining a solid social life? What advice would you give to others in pursuit of certifications based on your own experience?

In my case, I set up study sessions three times a week with a colleague very early in the morning, before starting work. The balance with my personal life in that sense was easier because when everyone was on his or her way to work or sleeping, we were preparing for the exam. My wife gave me great support during that period; she was crucial.

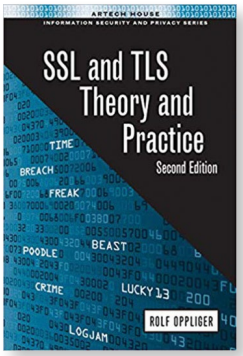
There is no secret formula to recommend to those that pursue a certification. I just insist that you attend to your priorities, be aware of what will be affected during this period and have enough support from the people around you. With that in mind, it is easy to structure a good plan, measure out your efforts and designate enough time to reach your goal. In addition, do not forget to do many practice tests and certainly sleep well the day before the exam. ■

RECOMMENDED READING

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

SSL and TLS: Theory and Practice, Second Edition

BY ROLF OPPLIGER
(Artech House, 2016)



SSL (secure sockets layer) and TLS (transport layer security) are part of most contemporary security systems that are used in most, if not all, web-based e-commerce applications. SSL protocol has evolved into three versions—SSL 1.0, SSL 2.0 and SSL 3.0—to become what is currently TLS. The need for SSL and TLS and the best practices—do's and don'ts of implementing SSL and TLS—are covered in this reference written by veteran cybersecurity expert Rolf Oppliger, founder of eSecurity Technologies and an active member of the technology community.

SSL and TLS: Theory and Practice starts with the building blocks to SSL/TLS, including the engineering and wiring. From there, Oppliger discusses the vulnerabilities and application protocols and presents several ways to build more security into an application. He demonstrates how increased security using data encapsulation with SSL and TLS offers the developer or security professional a way to limit the access within an application in order to perform a restricted set of operations.

The architecture and best practices of SSL/TLS are often neglected in other books. Oppliger includes best practices, covering TLS extensions, TLS version 1.3 and datagram TLS (DTLS). He offers techniques to protect against cryptanalytic attacks and mitigate risks. And he warns the reader that even though SSL/TLS is widely expected to protect most applications used on the internet, an additional layer of protection using a level of IP security (IPsec) and key exchange will go a long way to ensuring risk mitigation.

SSL and TLS: Theory and Practice is written from a practitioner's point of view. Oppliger's work provides crucial information to better understand the vulnerabilities related to SSL/TLS as well as an attacker's approach using cryptanalytic tools. ■

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.

READ.
QUIZ.
EARN.

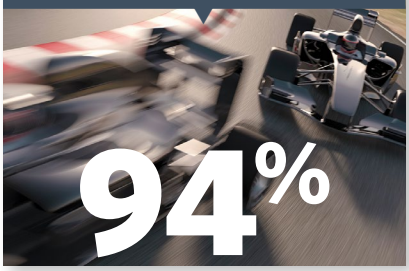
Earn Two CPEs for Reading This Issue

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&ACTION=SI&CatRedirect=10837%7C10837

ATTACKERS HAVE THE EDGE



Cybersecurity professionals say that cyber adversaries have the advantage over defenders

Source: Enterprise Strategy Group
https://www.esg-global.com/data-point-of-the-week

SIX TOP CLOUD SECURITY THREATS

1. Improperly configured containers
2. Compromised credentials
3. Weak identity and access management safeguards
4. Excessive use of privileged accounts
5. Misconfigured cloud storage
6. Lack of visibility

Source: *CRN Magazine*
http://bit.ly/3atGju3

"In 10 years, if you're not using some sort of AI-enhanced assistant, it will be like not being on the internet today."

—Kaza Razat, AI developer

Source: *PwC, Bot.Me: A Revolutionary Partnership*, a survey of 2,500 U.S. consumers.
https://www.pwc.com/CISAI

Mevans / Getty Images

Top 5 Webinars for 2019*

It was a great year to build skills and expand members' knowledge bases through webinars on different continents. Here are the most popular (ISC)² webcasts last year by region.

**Ranked by view rating*

NORTH AMERICA (NAR)

TITLE	LINK
Infoblox #2 – Threat Intelligence Update – Ransomware Tools Continue to Increase	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=373603
Infoblox #3: Stop Attacks Faster Using the MITRE ATT&CK Framework	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=377887
Infoblox #1 – Get Encrypted! Examining Emerging DNS Privacy Standard	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=370586
Gigamon #1: Network Data Capture for Incident Response	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=362131
Bitglass Part 3: Security in the Cloud – CASBs for IaaS Security	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=366387

EUROPE, MIDDLE EAST, AFRICA (EMEA)

TITLE	LINK
20 SIEM Use Cases in 40 Minutes: Which Ones Have You Mastered?	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=348085
Key Attributes of a Modern Phishing Awareness Program	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=374310
The State of Cyber: Global Trends, Predictions & the Lessons Learnt	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=372465
Fight the Good Fight Against the Bad Bots	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=359136
From Liability to Asset: The Role of DNS in Your Security Architecture and Ops	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=351657

ASIA PACIFIC (APAC)

TITLE	LANGUAGE	LINK
Zero Trust Best Practice and Financial DDoS Attack Trends	Korean	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=374446
A New Approach to CIAM & Demystifying Deserialization	English	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=367834
The Implications of the Data Breach Incidents for the Chinese Corporations	Chinese	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=366503
Appropriate Countermeasures Against Malicious Bots	Japanese	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=356239
Key Attributes of a Modern Phishing Awareness Program	English	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=375548

The Human Element: Zen and the Art of Cybersecurity

by John McCumber

ON A RECENT BUSINESS TRIP TO TOKYO, I had the opportunity to fulfill a bucket list item: traveling on a bullet train. On a beautiful Sunday, I sped from Tokyo to Kyoto at 145 mph. There, I hired a car and driver to tour that charming city. We stopped at a Zen garden where I perched on a wooden platform and silently contemplated the scene. I learned that each stone had a name, and that each was placed precisely where it needed to be. My task was to remain quiet, breathe, look out over the stones and absorb what they had to teach me.

You may be wondering how a Zen garden relates to cybersecurity. The major Zen element of cybersecurity is understanding there is not some ideal state of security you can ultimately achieve for an organization. Cybersecurity is not a destination, but rather a journey that never ends. It's a process, not a product.

The other Zen revelation was how the garden was designed as a focus on the human element. Cybersecurity has three main elements: technology, policy/process and the human factors. The garden mirrors that construct. The stones, sand and plants represent technology. Their placement is dictated by the architect's insightful process—the policy/process. And the positive effect on the observer is ultimately the reason the garden exists—the human factors.

Many in our profession fail to fully comprehend the necessity of combining those three elements. One very large federal agency that will remain nameless has a bad habit of trying to solve nationwide cybersecurity problems with immense one-size-fits-none technical solutions that are designed, developed and deployed from Washington, D.C. When these so-called solutions finally get to the field (years late in many cases), they inevitably fail to live up to expectations. It's the equivalent of providing users with a Zen garden experience by mailing them a pallet of rocks that simply show up on the loading dock. Some assembly required.

The human element of our cybersecurity profession must always be preeminent and must have a far more lasting impact than simply the deployment of some new (for now) technology-based solution. As our Code of Ethics states, we have an obligation not only to our employers, but to the greater societal good.

Image: Martin Wahlborg / Getty Images

Human factors are present in all our solutions, and no matter your selected technology safeguard, there must be policy/procedures enforcing its use. The human factors are involved in its design, deployment and operation. And you must also consider the human elements required to not only enforce the policy but understand how it impacts your users.

The only safeguards that stand alone are the human factors. They can be used to influence peoples' behaviors, good and bad. My favorite example of a human factors safeguard are those signs from alarm/security companies that people plant in their flower beds to inform potential thieves the house is actively being monitored and (hopefully) deter the bad actor.

The human factor of security is often the most neglected. We should always ensure we are considering the human factors not only of those whose technology we support, but those who would exploit our assets. Consider the Zen garden: It is not about the stones and their architected placement. Human factors are the centerpiece of the garden and of the information security profession. ■

John McCumber is director of cybersecurity advocacy for North America at (ISC)². He can be reached at jmccumber@isc2.org.

(ISC)²

6 TRAINING MYTHS EXPOSED

Don't Fall for FICTION. Know the FACTS.

We're Looking Out for Your Training Investment

Eight out of 10 Fortune 100 companies rely on (ISC)²-certified professionals to prepare for and recover from cyberattacks. With so much on the line, who do you trust to train your cybersecurity team?

Before you put your faith in a cybersecurity certification training provider, learn the **TRUTH**.

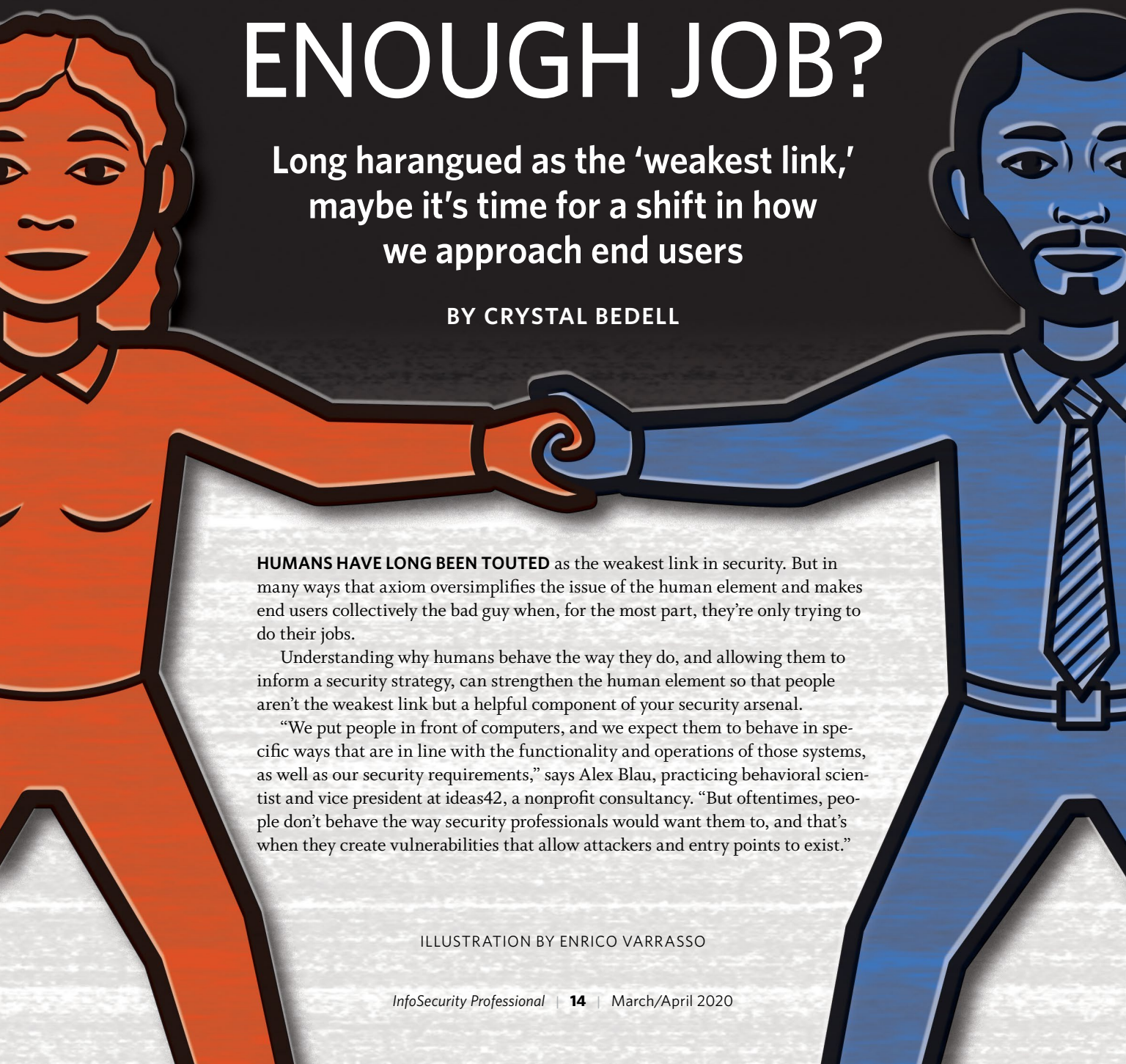
Get the Facts ▶

CISSP® ISSAP® ISSEP® ISSMP® SSCP® CCSP® CAP® CSSLP® HCISPP®

FIRST LINE OF DEFENSE: ARE HUMANS DOING A GOOD ENOUGH JOB?

Long harangued as the 'weakest link,' maybe it's time for a shift in how we approach end users

BY CRYSTAL BEDELL



HUMANS HAVE LONG BEEN TOUTED as the weakest link in security. But in many ways that axiom oversimplifies the issue of the human element and makes end users collectively the bad guy when, for the most part, they're only trying to do their jobs.

Understanding why humans behave the way they do, and allowing them to inform a security strategy, can strengthen the human element so that people aren't the weakest link but a helpful component of your security arsenal.

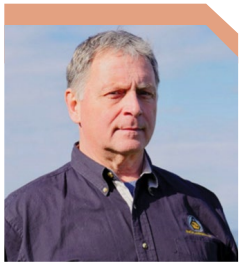
"We put people in front of computers, and we expect them to behave in specific ways that are in line with the functionality and operations of those systems, as well as our security requirements," says Alex Blau, practicing behavioral scientist and vice president at ideas42, a nonprofit consultancy. "But oftentimes, people don't behave the way security professionals would want them to, and that's when they create vulnerabilities that allow attackers and entry points to exist."

ILLUSTRATION BY ENRICO VARRASSO

UNDERSTANDING HUMAN NATURE

As any cybersecurity professional knows, you can't apply technical controls to human behavior. By their nature, people are creative, emotional and often unpredictable. Those characteristics apply equally to end users as well as cyber criminals who leverage human behavior to advance their attacks.

"There only needs to be one way to breach your network, and it may be a human that creates that opportunity by misconfiguring a security tool, by misusing a communications system, the network, or email, or inappropriately responding to social engineering," says Bob Hillery, chief operations officer and chief research officer for InGuardians, Inc., an information security consulting firm.



"The reason social engineering has always worked is because people want to help each other. That's not going to change."

—Bob Hillery, chief operations officer and chief research officer, InGuardians

"The reason social engineering has always worked is because people want to help each other. That's not going to change," Hillery says. "That's human nature, and we hire people because we want them to help each other and be innovative in how they find solutions to make things work."

Roselle Safran, president at Rosint Labs and entrepreneur in residence at Lytical Ventures, agrees. "Attackers evolve and up their game when what they're doing is being thwarted. To a large extent, what they're doing with social engineering just works as it is. They don't have to improve their capabilities," she says.

"Attackers evolve and up their game when what they're doing is being thwarted. To a large extent, what they're doing with social engineering just works as it is."

—Roselle Safran, president, Rosint Labs and entrepreneur in residence at Lytical Ventures

It's important for both end users and security professionals to understand that nothing is off-limits to cyber criminals. "The real cyber attackers don't care about rules. They don't care about being nice. They don't care about proper techniques," Hillery explains.

Consider, for example, a phishing email that instructs recipients to click on a link to learn about proper procedures if there's an active shooter in the building. In Hillery's experience, everyone clicks on the link, but companies don't want to use this type of content for a phishing exercise because it's the very thing they *should* click on if there's an active shooter. That wouldn't, however, stop an attacker from using it.

"Unfortunately, people are going to fall for those types of attacks," Safran says. "That's going to happen if you're relying on the end user to always get it right, and that's why I feel the burden of making sure that doesn't happen needs to fall on the security team to make sure that email doesn't reach them in the first place or, if it does, the user will be stopped when they click and prevented from being able to enter their credentials."

Safran continues: "That makes the task of the security team even more challenging, because they can't rely on the end user to be that last line of defense. But, in my opinion, it's unrealistic to think that an end user can be a line of defense that's going to be infallible."

Hillery agrees. "There's no way to stop all the risks of the human element. Any time the human can be a single point of failure for your overall security posture, you have a design problem. And you need to make sure it's not a single point of failure; there needs to be a second person check, a software check, something," he says.

That said, a solution cannot be implemented in a vacuum. "No matter how advanced the technology you're implementing, no matter how simple the processes, if people are not aware and if they are not committed individually to that security control … no matter what you do, it will fail," says J. Eduardo Campos, president and managing partner at business consulting firm Embedded-Knowledge, Inc.

CONTEXT, CONTEXT, CONTEXT

That's where security awareness training can help.

"User awareness training is helpful, but it needs to go beyond the minutia of what a phishing email looks like," Safran says. Otherwise, all too often, users assume that they personally aren't a target. "User awareness training needs to first start with providing an understanding of why attackers are interested in their organization and why users are targets. Once people understand the context of why cyberattacks are happening to their organization and potentially to them personally, then it's easier to go to the

"Human behavior is motivated by context, so rarely will you find that decision-making happens on a lone island."

—Alex Blau, practicing behavioral scientist and vice president, ideas42

"No matter how advanced the technology you're implementing, no matter how simple the processes, if people are not aware and if they are not committed individually to that security control … no matter what you do, it will fail."

—J. Eduardo Campos, president and managing partner, Embedded-Knowledge

next step of identifying when those attacks are coming in."

Security professionals can also benefit from having a better understanding of context.

"Human behavior is motivated by context, so rarely will you find that decision-making happens on a lone island. The context you put someone in will dictate the behavior they exhibit. The technical controls, policies, anything that's visible to them will be most important to how they actually operate. If you take that lens, it opens up a lot of opportunity," Blau explains.

Security awareness training might make users smarter, but "a deeper diagnosis about behavior and the context in the environment that's increasing or decreasing that behavior will be the lever you need to pay attention to," he says. "That's where a policy can be changed, or you literally need to write something down so that people will be more attentive to it."

Hillery also stresses the importance of context in terms of security policies. "Across my careers, one of the challenges has always been writing a policy that does what you want it to—and that users can actually follow. We often write policies so constrictively that they impede work, and many times people are breaking policy either because they don't understand the security implication, or they had to break it in order to actually get their work done.

"Policies must be functional," he continues. "The people who write the policies are often not the ones doing the work. The people doing the work need to have a say so that they understand what the policy says, and the policy writers need to understand what's doable."

In fact, security policies are only effective if they take into account the end user. "Engage your stakeholders. Talk to people. Listen to their needs. Listen to what moves them. And then, design a solution that speaks to their minds and hearts," Campos advises. "The solution is not yours as a security provider. If the program fails when you leave, it's because it's not theirs. It was yours. The first thing you do is come at the problem from the end user's perspective. Make whatever you're implementing—the security policy or data transfer policy—*their* solution. And then find champions, people who can advocate for you without you being in the room."

WHERE TECHIES TEND TO FAIL

Departmental champions are important, but they don't negate the need for support from "the top."

"It's critical that there is buy-in and support from leadership in order for the security program to be as effective as it can be. What happens at the top cascades down. If senior leadership is not paying attention to cybersecurity, that will be reflected in the organization's policies. If the organization's policies are not weaving in cybersecurity, then the security team has very little ability to enforce what needs to be enforced in order to have a secure posture," Safran says.

"That's where techies fail," Campos argues. "We get excited about the technology, and we forget about the risks. At the end of the day, someone in the food chain will make a decision to invest in cybersecurity or technology or training, and that decision is based on a risk assessment. [Whether] the risk assessment is well done or not, that's another thing. Someone has the power of approval to avoid, mitigate or ignore risk. [Cybersecurity professionals] need to work with users and senior leadership to put policies in place that will empower users to carry out their functions, deliver their goals and the company commitment, and at the same time protect the assets."

Bottom line: "Cybersecurity is a continuous effort. We're never going to be at the point where we can just say, 'All right, we have this handled. No more need to focus on cybersecurity,' because the attackers are constantly evolving, and we have to as well," Safran says. "The human element makes mistakes. … That's inevitable and that has to be factored into the equation." ■

CRYSTAL BEDELL *is a longtime magazine contributor who lives and works in Washington state.*

IT'S ALL IN YOUR HEAD

BY MICHAEL M. HANNA, CISSP

Leveraging the power of psychology to strengthen your cyber defense posture.

WHETHER YOU'RE A CISO, CIO, IT director/manager, team leader, or you are just beginning your journey as an IT security leader, your days never seem to end because your organization always faces the threat of an attack. Leading your team to protect the organization, users and customers from an array of threats is a daunting and demanding task. Failure to protect the organization's information systems and data may result in grave consequences. That's a tough job.

To succeed as a security professional, you must incorporate the skills of a cybersecurity engineer, computer scientist, business leader and psychologist on a daily basis. Trust me, you're using psychology every day, but you may not be fully realizing its potential.

ILLUSTRATION BY DAN SIPPLE

The wonder of the mind, human behavior and psychology are some of the most fascinating and unexplained concepts in the scientific community, yet they make up a critical component of an information security program, too. You must manage people, processes and technology to protect the organization; however, too often, the order of importance on a practical level tends to be technology, processes and people. That's a concern. Examining and understanding the human factor, as well as leveraging psychology, are as important, if not more so, than technology and processes.

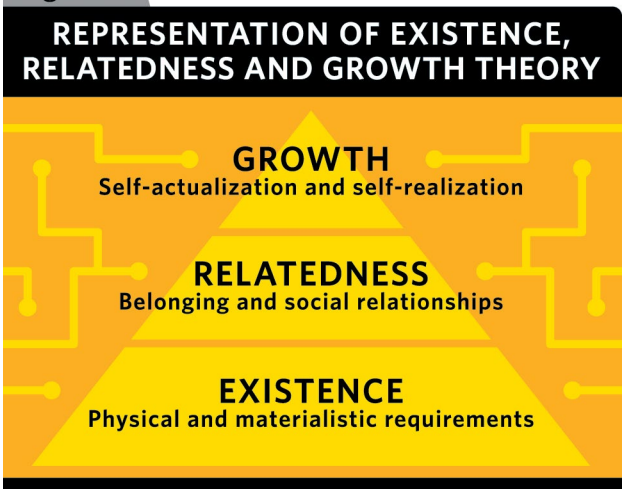
As information security professionals, we generally accept that human beings are the weakest component of an organization's information security program. The unintentional and intentional insider threat is significant, which is why for this article we will just examine psychology concepts from the domains of industrial and organizational, social and cyber psychology relevant to the unintentional insider because both groups are significantly different in their approaches.

You must manage people, processes and technology to protect the organization; however, too often, the order of importance on a practical level tends to be technology, processes and people. That's a concern.

I want you to think about all the reasons that employees throughout your organization have failed you. One reason could be because employees have uninformed and inaccurate perceptions of information. Another is because they quickly forget what they have been taught. For example, one study within the United Kingdom (https://bit.ly/2sBMZoy) found that 58% of employees did not possess the knowledge or skill set to protect an organization from malicious activity.

Another study that examined business training sessions (https://bit.ly/2rKdJD6) discovered that employees forgot 50% of a lesson within one hour, 70% was forgotten within 24 hours, and 90% was forgotten within a week. This decline in retention, referred to as the Ebbinghaus Forgetting Curve, is applicable to any material, meaning it applies to cybersecurity awareness training. We generally attempt to keep training to the most important and relevant topics, but if employees are forgetting 70% in just the first day, how are we expected to defend? Furthermore, research

Figure 1:



shows individual demographics, traits, risk-taking comfort, and decision-making styles, just to name a few, will influence employees' cybersecurity behaviors.

With the requirement to produce desired behaviors throughout the organization, from the C-suite to the most junior employee, cyber psychology may be the answer. Forget top 10 tips to promote positive cyber behavior; instead, let's focus on realizing its greater potential. Delving deeper into psychology is no different than being an individual who knows how to use a computer compared to a person who understands how a computer and the installed components operate. The deeper understanding affords you the opportunity to interpret theories to learn how to achieve a desired outcome.

The following psychological theories are overlaid with leadership and security practices. The bottom line is that leveraging the power of human psychology has great potential to bolster your initiatives, leadership development, and overall success.

Let me begin with a disclaimer. The building blocks that I am going to present just scratch the surface. Human psychology applied to information security goes much deeper, and this is an area that will require continuous study. But the introduction should provide a foundation upon which you can build a more robust information security program. Furthermore, psychology should not be thought to support fear, uncertainty and doubt, but rather support development.

EXISTENCE, RELATEDNESS AND GROWTH (ERG) THEORY

ERG theory (https://bit.ly/2u6k38L) is based of Maslow's Hierarchy of Needs, with a different grouping and some minor adjustments to the individual layers. ERG denotes

existence needs at the bottom, followed by relatedness needs, and then growth needs (*see Figure 1, p. 18*).

Existence is concerned with materials needed for survival and physical contact. From an employment standpoint, this relates to earning a paycheck, which impacts your ability to purchase goods. Relatedness is related to belonging, which translates to how you fit in within your organization, department and team. The growth layer accounts for self-realization to accomplish greater things.

ERG can be used in implementing sanctions for information security infractions and reward positive behavior. Many of us understand that a one-strike-and-out approach is just not going to happen within an organization. Rather, consequences and rewards can be implemented that impact specific layers of the model to leverage human motivation.

As an information security leader, you can improve your team's satisfaction through HMHT and positive psychology. The key point is that intrinsic motivators are much stronger than extrinsic.

A first offense can result in interrupting an employee's ability to further realize their potential by withholding non-required training or denying assignment to special projects for a period of time.

A second offense would focus on interrupting the second layer and play to their acceptance within the group. For example, if an employee inappropriately plugged a smartphone into a host, you could remove that host and another from the team to impact their productivity temporarily. You could also make the offending department known throughout the organization without naming names. Both approaches impact relatedness.

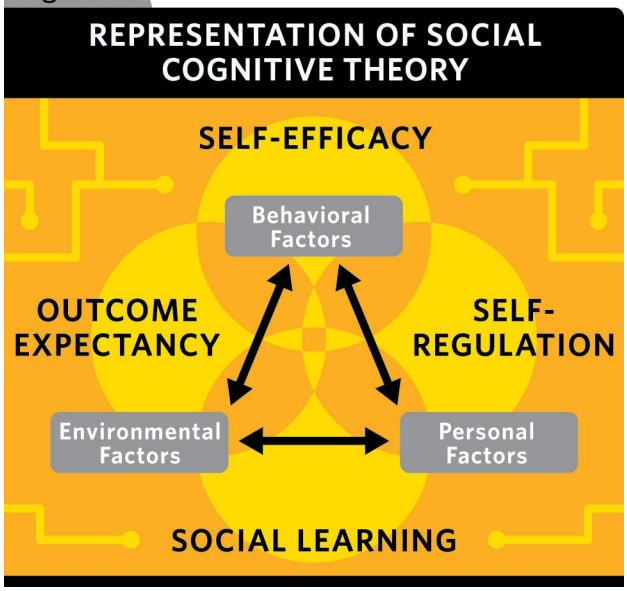
Finally, a third offense could result in termination or some other penalty. You must be careful in utilizing these approaches. Also, ERG can support incentive programs, and leadership buy-in is absolutely necessary.

DETERRENCE AND INCENTIVE THEORY

Like Newton's third law, for every action, there is an equal and opposite reaction. For inappropriate actions, a consequence proportional to the offense is needed, which fits within the scope of deterrence theory.

On the other hand, successes by teams and departments should also be rewarded, which falls into incentive theory. You may be able to overlay the principles of ERG theory to assign punishment and reward or leverage the findings of Herzberg's Motivation-Hygiene Theory.

Figure 2:



HERZBERG'S MOTIVATION-HYGIENE THEORY (HMHT)

Frederick Herzberg examined employee job satisfaction in the late 1950s to develop HMHT (https://bit.ly/2ZGS62X), but recent research has demonstrated its consistency and value. Hygiene factors are not additive in nature, but motivating factors are. Arguably the most important piece of HMHT is that motivating factors are all related to personal psychological growth, whereas hygiene factors involve avoiding physical and psychological pain (http://bit.ly/2G9I9lC).

Don't get this theory wrong, though: People can be motivated by earning more money (a hygiene factor), but it does not lead to increased satisfaction. As an information security leader, you can improve your team's satisfaction through HMHT and positive psychology. The key point is that intrinsic motivators are much stronger than extrinsic.

SOCIAL COGNITIVE THEORY

In my humble opinion, Social Cognitive Theory (SCT) is one of the most robust and powerful learning and behavior models developed. The theory was developed by Dr. Albert Bandura of Stanford University and assumes that human beings are agents that can make intentional decisions to produce a positive outcome. The agentic perspective

assumes that human beings practice intentionality, forethought, self-reactiveness and self-reflectiveness. SCT also provides a framework to promote individual learning.

Basically, SCT assumes that human beings are influenced by environmental, behavioral and personal factors, known as the triadic reciprocal determinism model. Furthermore, four concepts guide these major factors: self-efficacy; outcome expectation; self-regulation; and social learning (*see Figure 2, p. 19*).

Personal factors include characteristics specific to an individual such as their beliefs and attitudes. Behavioral factors describe constructs and skills that guide an individual's behavior, such as a person's ability to self-regulate and self-examine their behavior. Environmental factors consider the world around an individual, such as the organization's culture.

By understanding the makeup of your organization—including employee characteristics behavioral factors and organizational culture—improved security, education, training and awareness programs can be produced. Think about the personal factors of a marketing team versus your IT team. They both possess very different attitudes and beliefs with very different goals. As an information security leader, you must recognize this and approach both teams differently. SCT is an extremely powerful tool that can guide many initiatives. By incorporating other theories within SCT, you may be able to amplify positive results and minimize potential effects.

TYING IT ALL TOGETHER

We just scratched the surface of what cyber psychology could do to help your team and security program, but it provides an opportunity to reap significant benefits. To begin, try the following:

- Explore various theories each day. Start off with 15 minutes a day. Trust me, the power of compounding effects will be substantial in the long run.
- Test them out on smaller groups before scaling your approach.
- Acquire senior leadership buy-in to your approaches.

Most importantly, be a believer in the power of psychology in cybersecurity. The human mind is the most powerful tool we possess in our repertoire. ■

MICHAEL M. HANNA, *CISSP, is a member of the U.S. military. The views expressed here are solely those of the author, and do not necessarily reflect those of the Department of the Navy, Department of Defense or the United States government.*

SOCIAL COGNITIVE THEORY AT WORK

Here are some ways to leverage the principles of Social Cognitive Theory to motivate your users to follow cybersecurity best practices.

Self-efficacy
Individuals with higher levels of self-efficacy generally perform better; therefore, it may be necessary to conduct more frequent and increasingly difficult training sessions to achieve your desired outcome. A single annual training session does not meet the bill. You should look to overlay adult learning theory or experiential learning theory.

Environmental factors
If senior leaders within your organization do not emphasize the importance of security, then a different approach may be necessary to bring home the point during training sessions. It may be necessary to incorporate motivational theories such as ERG, deterrence or incentive.

Social learning
Individuals learn by watching other individuals. By focusing on training smaller groups of individuals to behave a specific way, your team may leverage their positive behaviors to promote better behavior of trouble groups. For example, hand select departments or individuals that you know will behave as you desire and are relatively influential. Their public and consistent behavior will begin to change the behavior of those around them. Imagine if the American actor Dwayne "The Rock" Johnson preached the importance of password managers. You can bet that a lot more people would take it seriously.

Outcome expectancy
This does not have to only be a fear tactic. Positive behaviors can be rewarded as well. The point is that negatives behaviors cannot be overlooked, and positive behavior should be rewarded. You should overlay a motivational theory here, such as incentive or deterrence theory.

—M. Hanna

SECURITY.TXT

Responsible disclosure for the next generation

BY FAVIAN ERIC RAYGOZA, CISSP

WITH AN INCREASING number of security researchers finding vulnerabilities in public systems, it's often very difficult to find a proper channel for responsibly disclosing these findings to the owners of the information systems.

A new Request for Comments (RFC) currently in draft (as of December 2019) will assist in standardizing and creating a viable process for researchers to report findings to information security teams (http://bit.ly/2TODOfK). Giants such as Facebook and Google have already gotten behind this RFC's implementation. Everyone else in the industry should, too.

WHAT IS SECURITY.TXT?

Security.txt is a proposed standard (IETF "draft-foudil-securitytxt-07") which allows websites to define security policies and specifically defines a standard to help organizations implement processes for security researchers to disclose vulnerabilities. Drafted by Ed Foudil, Security.txt is the equivalent of robots.txt, but for security issues. In a sense, its founder is taking robots.txt and extending it into a framework.

IMAGE BY JOHN KUCZALA

RETURN TO CONTENTS

"When security risks in web services are discovered by independent security researchers who understand the severity of the risk, they often lack the channels to properly disclose them. As a result, security issues may be left unreported. The very purpose of this method is to give a direct line to technical security teams, for security researchers who want to diligently disclose vulnerabilities that they might find," according to a 2018 draft abstract (http://bit.ly/2RH3cBC). It is a concise, to-the-point solution to assist with the need of reporting security issues, building on existing conventions such as robots.txt.

This initiative has been gaining steam—and rapidly—since its proposal. Companies such as Google, LinkedIn, HackerOne, Facebook and Bugcrowd have adopted Security.txt. You can easily see this at the root of their websites, by visiting https://[company-website]/.well-known/security.txt.

MAKING SECURITY.TXT WORK FOR YOU

So how do we implement this? How can we explain this mechanism, to champion it at our own organizations? Security.txt is a simple text file, like a robot.txt file, located in the root directory of a website. Not only does this file provide you with the proper contact information but it also provides one with a secure way to transfer the information.

The meat of the technical details is simple to follow. The file we would create is named "security.txt," and this file should be placed under the /.well-known/ path ("/.well-known/security.txt") of a domain name or IP address for web properties.

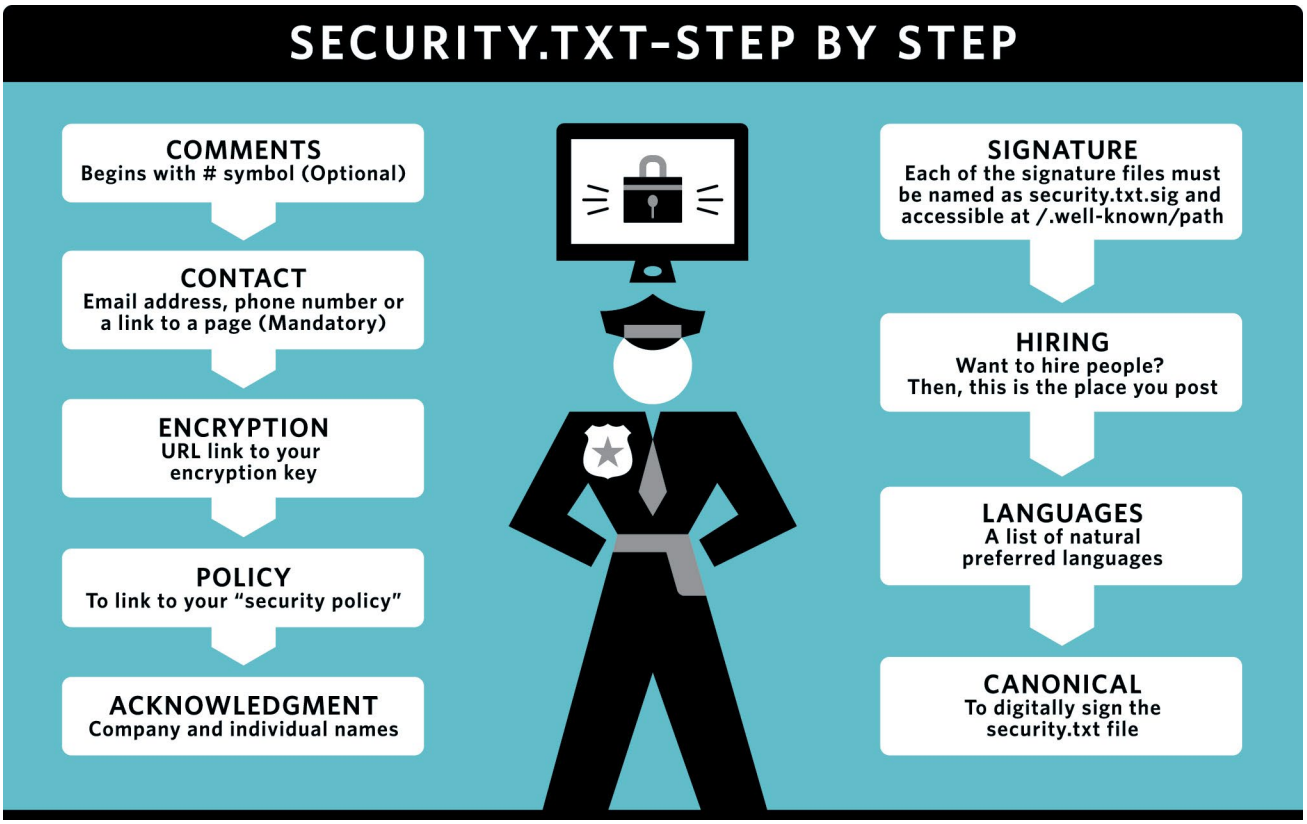
Not only does this file provide you with the proper contact information but it also provides one with a secure way to transfer the information.

As explained by web application developer Michal Spacek in his an Aug. 9, 2018 blog post on Security.text (http://bit.ly/37jAMUQ): It would be a best practice to build a redirection target on the same domain; you wouldn't redirect from https://www.example.com/security.txt to https://www.example.net/.wellknown/security.txt and not even to a subdomain, such as https://foo.www.example.com/.well-known/security.txt. Instead, you'd go only to https://www.example.com/.well-known/security.txt. This facilitates an easier-to-find security.txt document for researchers.

And in a rare instance, if you can't place the security.txt file in the /.well-known/ path, or setup a redirect, you can place the file in the top-level path as a fallback option.

Rishi Narang on his blog Cyber Sins (http://bit.ly/2RiMXeR) explains how to host this file internally. This is immensely beneficial for large organizations. For companies the size of a Fortune 500, you might find different security teams are responsible for overseeing different assets. On internal hosts or file systems (http://bit.ly/37jAMUQ) you can place the security.txt directly in the root directory. As Narang, a security consultant, explains in the same blog post, the file must be served over HTTPS, and HTTPS must be used in all the URLs inside the file, including but not limited to the following directives:

- Text file contains multiple directives with different values. The "directive" is the first part of a field all the way up to the colon ("Contact:") and follows the syntax defined for "field-name" in section 3.6.8 of [RFC5322].
- Directives *must* be case-insensitive (as per section 2.3 of [RFC5234]). The "value" comes after the directive ("https://example.com/security") and follows the syntax defined for "unstructured" in section 3.2.5 of [RFC5322].
- A "field" *must* always consist of a directive and a value ("Contact: https://example.com/security").
- A security.txt file can have an unlimited number of fields. You must have a separate line for every field.
- One must not chain multiple values for a single directive unless it is explicitly defined by that particular field. Unless otherwise indicated in a definition of a particular field, any directive may appear multiple times.
- Comments: The file can have information in the comment section that is optional. The comments shall begin with the # symbol.
- Each separate field needs a new line to define and represent.
- Contact: This field can be an email address, phone number or a link to a page where a security researcher can contact you. This field is mandatory and must be available in the file. It should adhere to RFC3986[3] for the syntax of email, phone and URI (must be served over HTTPS). Possible examples are:
  - Contact: mailto:security@example.com
  - Contact: tel:+1-201-555-0123
  - Contact: https://example.com/security-contact.html
- Encryption: This directive should link to your



Infographic: Robert Pizzo

encryption key if you expect the researcher to encrypt the communication. It must not be the key, but a URL to the key-file.

- Signature: If you want to show the file integrity, you can use this directive to link to the signature of the file. Each of the signature files must be named as security.txt.sig and accessible at /.well-known/path.
- Policy: You can use this directive to link to your "security policy."
- Acknowledgement: This directive can be used to acknowledge the previous researchers and findings. It should contain company and individual names.
- Hiring: Want to hire people? Then, this is the place you post.
- Languages: A list of natural languages (language tags) that are preferred when submitting security reports.
- Canonical: The most common URL for accessing your security.txt file. It is important to include this if you are digitally signing the security.txt file, so that researchers can know for sure that you didn't just steal someone else's file with the same content.

The infographic above is a good illustration for the visual learner.

THE ETHICS OF RESPONSIBLE DISCLOSURE

Let's talk about a code of conduct, as this does involve responsible disclosure among third parties. If you're reading this article, you are most likely a member of (ISC)^2. We are bound by a Code of Ethics, which we all agreed to abide by when we joined (ISC)^2. When we are dealing with others outside of our organization, it's important to be respectful, friendly, patient and kind.

Let's also be cautious with how we word things to always remain professional. When we disagree with those reporting issues to us, try to understand why. And most importantly, be realistic with setting expectations. If a security researcher reports a finding, you typically want to work your hardest to have it rectified within the industry standard of 90 days.

We, the information security community, have collectively witnessed immense innovation in our field that has expanded our capabilities to operate successfully in the cybersecurity space. As we see advances in our field, it is a reminder to not forget the basics. Subjects as simple as responsible disclosure have been quiet thus far.

I think we can all agree that we are appreciative of the Security.txt founders for giving us a mechanism that could pull responsible disclosure technologies into the modern world, and even propel it forward into the next generation of elegant solutions. ■

FAVIAN ERIC RAYGOZA, *CISSP, is director of information security for an Austin, Texas-based healthcare provider.*

save for use as a handy reference

BANK ON IT

50 RESEARCH-BASED BEST PRACTICES FOR THE FINANCIAL SECTOR (AND EVERY OTHER INDUSTRY, TOO)

BY SHAUN AGHILI, DBA, CISSP-ISSMP, CCSP, CISA, AND BOBBY SWAR, PH.D

IN MAY 2018, two major banks in Canada—Bank of Montreal and Canadian Imperial Bank of Commerce—received email threats from malicious hackers claiming to have gained access to customers' sensitive information. The attackers demanded $1 million in cryptocurrency from each bank or they would publicly release customers' information. The successful attacks on these banks led to 90,000 customers' account information being compromised and an undisclosed amount of money lost as the result of the security breaches.

In recent years, the global banking sector has been the main target of severe cyberattacks. This, of course, is largely due to the enormous assets and sensitive information managed by this sector—and most others globally (*see Figure 1, p. 25*).

At the Information Systems Security and Assurance Management department of Concordia University of Edmonton in Canada, we recently completed a study of 25 large-scale North American banking security breaches over the past decade. Following a root cause analysis for each security breach, we conducted a literature review of some major information security-related frameworks and standards—including NIST 800-53 (R5), ISO 27001:2013, ISO 27032:2012, COBIT 2019, the Office of the Superintendent of Financial Institutions' (OSFI Canada) cybersecurity assessment-guide, and the Cloud Security Alliance's Cloud Control Matrix v.3.0.1—in order to compile a list of more than 50 cybersecurity best practices that could have mitigated these 25 banking cybersecurity breaches.

The following is a condensed version of these research-based best practices. Please note that this compilation is by no means comprehensive, but it could serve as a useful checklist and/or discussion points for information systems auditors and cybersecurity professionals in the banking industry and many (if not most) other sectors, including retail, service and manufacturing.

FIGURE 1: ESTIMATE OF GLOBAL FINANCIAL LOSSES ATTRIBUTABLE TO CYBERATTACKS

Region	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (GDP%)
North America	20.2	140 to 175	0.69% to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79% to 0.89%
East Asia and the Pacific	22.5	120 to 200	0.53% to 0.89%
South Asia	2.9	7 to 15	0.24% to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28% to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07% to 0.20%
MENA	3.1	2 to 5	0.06% to 0.16%
World	75.8	445 to 608	0.59% to 0.80%

Source: J. Lewis, "Economic Impact of Cybercrime—No Slowing Down," 2018 (https://bit.ly/35jh0Xu)

GOVERNANCE

1. The mission, vision, core values, business strategies and objectives of the enterprise should be well defined, prioritized and documented.

2. Both management and its board of directors should ensure that the enterprise maintains full adherence to all legal and regulatory requirements in order to avoid sanctions and to help reduce incidents of large-scale security breaches.

3. Management and the board of directors must ensure that the IT and audit functions within the enterprise receive the needed resources in order to effectively and proactively protect the enterprise from security breaches. As such, information systems' security-related capacity management plan, which details the required resources to meet current and future cybersecurity needs, should be presented to the management and to the board of directors for review and discussion with the information security team and the audit department.

POLICY MANAGEMENT

4. The enterprise information security policies should be defined, approved and implemented by management and communicated clearly to all stakeholders in such a way that all employees and stakeholders fully understand their roles and responsibilities to keep the enterprise secure.

5. Management should implement periodic reviews of information security policies to ensure they remain relevant.

TRAINING AND EDUCATION

6. Management should ensure that all employees and business partners are properly trained to carry out their assigned duties and responsibilities related to cybersecurity policies, procedures, and other related agreements through the implementation of a robust and continual information security training program.

7. Customers should also be sensitized to prudent cybersecurity practices through an effective and consistent information security awareness program.

RISK MANAGEMENT CONSIDERATIONS

8. Management should invest an appropriate amount to implement a comprehensive and relevant information system security-related framework.

9. Management should also be committed to ensuring that the implemented framework and risk management procedures continue to achieve their intended outcomes and objectives.

10. Approved risk management processes should be properly documented and communicated to all stakeholders.

ACCESS CONTROL (PHYSICAL AND LOGICAL)

11. A defense-in-depth approach in terms of the physical security of assets should be adopted that includes effective use of controls such as CCTV cameras, motion detectors, security personnel, locks, trap doors, fences, bollards, and smoke/fire detection mechanisms, just to name a few.

12. Access to physical assets should be adequately restricted, and all access to such assets should be documented and reviewed on a regular basis.

13. Appropriate remote access configurations and connections procedures should be established, implemented, documented, and monitored continuously.

14. All remote maintenance efforts on systems should be approved and logged in order to prevent unauthorized access.

15. An appropriate access control architecture,

based on the enterprise's information access and security needs, should be implemented and continuously monitored.

16. An appropriate password policy detailing mandates for password complexity, expiration, account lockout, password reset procedures, minimum and maximum password age, as well as the use of password random generators, one-time passwords and strong authentication (such as the use of biometrics) for critical systems, needs to be drafted, implemented, and reviewed at regular intervals.

17. Access control should also be based on the principle of least privilege. Auditors should also ensure that previous access privileges for employees do not result in an access control scope creep.

18. Access control logs must be properly set up and reviewed on a consistent basis.

DISASTER RECOVERY (D/R) CONSIDERATIONS

19. Detailed and appropriate disaster recovery and business continuity policies, procedures and processes should be developed, properly communicated, and reviewed on a regular basis (e.g., yearly) based on lessons learned, test results, and/or environmental changes.

20. D/R plans should be regularly tested and updated on an annual basis.

21. D/R-related documents, such as call trees, should be updated on a regular basis.

22. Critical systems need to be clearly identified and should be given top priority in terms of expedient approach to get them back up and running as quickly as possible.

HR CONSIDERATIONS

23. The human resources department is the first line of defense for information systems security's weakest link, namely employees. As such, the HR hiring and performance evaluation procedures, such as thorough background checks, should be established and followed consistently.

24. The HR department should also ensure that the enterprise's non-disclosure requirements and information security policies are read and understood by all employees.

AUDIT CONSIDERATIONS

25. Management should ensure that the internal/information systems audit activity is properly structured and implemented. These include the creation of an audit charter and appropriate reporting mechanisms to management and the board of directors.

26. Audit policies and procedures should be documented and reviewed on a regular basis based on lessons learned from data security breaches and previous audit results and experiences.

27. Audit activities should be risk-based and continual in nature throughout the enterprise in order to ensure that appropriate controls, based on a defense-in-depth approach, are implemented and that such controls continue to remain effective as the business environment continues to change and evolve.

28. The audit activities should also entail regular scanning of the enterprise's web-site(s), applications, and third-party plugins. Regular penetration testing in high-risk enterprises, such as banks, should be considered as a proactive approach to prevent future data breaches. Such penetration tests should only be conducted by highly qualified penetration testing teams, not by the enterprises' audit team unless its members are qualified to conduct penetration testing activities.

29. Disaster recovery plans should be continually reviewed, along with periodic testing results, to ensure that the enterprise maintains the capabilities to resume full operations as quickly as possible when needed.

30. Secure input data validation processes to prevent common attacks, such as SQL injection and parameter tampering on websites, should be tested regularly.

CONTINUOUS MONITORING

31. Continuous monitoring should be effectively incorporated as an effective and integral part of the control process in order to help both auditors and information security specialists within the enterprise to detect security-related anomalies.

32. Audit trails and exception reports should be reviewed consistently by not only the audit team, but also by experienced information systems personnel as appropriate.

33. Audit logs and exception reports should be secured in order to prevent unauthorized access to them.

SYSTEM AND DATA LIFECYCLE MANAGEMENT

34. Management should ensure that an accurate

and comprehensive inventory of information system-related assets (hardware, software, applications, data, intellectual properties, etc.) is created and kept up to date.

35. All inventoried assets should be classified based on risk and criticality.

36. Appropriate procedures for handling and managing all assets throughout their lifecycles are identified, documented, properly communicated and consistently enforced.

37. Change management policies, procedures and processes should be developed, implemented and strictly enforced.

38. All changes/modifications/major updates to servers, software and applications should be reviewed and approved by an appropriate committee prior to implementation with proper contingency plans in place, in case an intended change does not proceed as planned.

REMOVABLE MEDIA AND BYOD DEVICES

39. A comprehensive removable disks and BYOD devices policy and procedures should be established, documented, and strictly enforced through a continual monitoring approach.

40. In high-risk departments, employees should require appropriate written approvals to use removable media or BYOD devices based on their job functions.

41. Sensitive information on removable media or BYOD devices should be encrypted, and whenever possible such devices should also be equipped with a remote data deletion mechanism.

NETWORK SECURITY

42. An appropriate and framework-based information systems' security architectural approach should be devised and implemented. This includes system and network segmentation, physically and logically.

43. Network performance and protocols baselines must be well defined and reviewed regularly in order for the cybersecurity team and/or intrusion detection systems to detect system anomalies quickly and effectively.

44. An effective and appropriate network defense-in-depth using appropriate technologies approach should be devised and implemented. These include the effective use of anti-malware software, firewalls, and intrusion detection or prevention systems as appropriate.

45. All sensitive data should be encrypted while at rest, in transit, or at end points.

46. An effective cryptographic key management approach must be established and followed.

47. All systems should be properly hardened by disabling unneeded services, closing unused ports, and updating default passwords.

48. Effective mechanisms should be in place to ensure that all systems are updated effectively and expediently with the latest patches and security updates.

49. Procedures and processes involved in the configuration of servers, websites, routers, firewalls, networks and switches should be documented and reviewed by the cybersecurity and/or the audit team to help prevent errors that could lead to unauthorized access.

50. An important and sometimes neglected area is the related network security risks associated with third-party information systems and cybersecurity practices. As such, all third-party information systems should also be subjected to appropriate security standards, requirements and controls assessed at the beginning of a business relationship and ensuing regular audits. ■

SHAUN AGHILI, *DBA, CISSP-ISSMP, CCSP, CISA,* and BOBBY SWAR, *Ph.D., both work at the Information Systems Security and Assurance Management department of Concordia University of Edmonton in Canada.*

LEARN MORE

IF YOU WOULD LIKE to learn more about the research project that gave rise to these 50 cybersecurity best practices, we invite you to access our research deliverable at https://tinyurl.com/50-Cybersecurity-Practices.

The research document contains information regarding the root cause and estimated damages for 25 security breaches, the complete list of the compiled best practices along with their informative references, the mapping of the 25 security breaches to the compiled best practices, as well as the mapping of the best practices to the NIST cybersecurity framework.

The authors would like to acknowledge the valuable efforts and contributions of Oluwayemisi Ruth Oyewumi in creating the final research deliverable.

—S. Aghili and B. Swar

Help Has Arrived to Help *You* Make a Child's World Safer

by Pat Craven

AS A CYBERSECURITY PROFESSIONAL, I know that you spend your days focused on protecting infrastructure and data against those who would steal your organization's information. But we also have to remember that "data" belongs to individuals as well: you, me, our family, friends and even children.

I also know that while you are very good at what you do, you can't do it alone. Think about how much easier your life would be if people stopped opening attachments from strangers. Or if children stopped posting intimate details about their lives on social media. Or if our parents and grandparents would actually live by the "if it sounds too good to be true, it probably is" adage they taught us as kids. The truth is, people make it too easy for bad actors to disrupt their lives—and yours.

As a cyber expert, I know people ask you for tips and advice and may even invite you to speak to a local group about online safety. That is where the Center for Cyber Safety and Education comes in. We want to help, by providing you with tools to teach online users of all ages how to protect themselves beyond firewalls and anti-malware programs.

Safe and Secure Online is our free program for parents, seniors and middle school-aged children. On our website (www.IAmCyberSafe.org), you will find links to all the materials you need (PowerPoints, tip sheets and videos) that you can download and share with others. We have done the time-consuming work of putting it all together in a user-friendly format for you (including scripts). Your local schools, libraries and community centers would love to have you come and give a presentation to their students and members. And thanks to 367 $(ISC)^2$ volunteers, these lessons are now available in 24 languages!

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

If you want to help teach even younger kids how to be safe online, we have you covered. Three years ago, we launched the first in the series of *Garfield's Cyber Safety Adventures*, which has now delivered more than 170,000 safety lessons around the world to children ages 6 to 11. This classroom-style program has already won two prominent educational awards for the way it engages children and teaches them basic safety practices that will last a lifetime. We have developed Educator Kits that contain everything you need for a class or group of 30 children. It includes an original Garfield cartoon, comic books, stickers, posters, trading cards and more. You can learn more about this program at www.IAmCyberSafe.org/garfield.

Image: skynesher / Getty Images

We have done the time-consuming work of putting it all together in a user-friendly format for you (including scripts).

It is not the goal of the Center for Cyber Safety and Education to train or educate everyone in the world to be safe online, but rather to empower *you* with the resources to reach out to your local community and share your expertise and passion to help them become cyber safe. I know that together we can make it a safer cyber world for everyone! Let us know how we can help at center@isc2.org.

Next Step in Certification, VM, Protecting Credit Card Data, Evading Ransomware

The (ISC)² Community has more than 23,000 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 got my Security+ in April and I would love to get my next security cert. I would like to focus on cloud security. I would like to know should I go for my CISSP or CCSP or SSCP?

—Submitted by freddy91761

SELECTED REPLIES:

Do you have the experience to get the CISSP? If so, that's first as it's the biggest hurdle, followed by the CCSP. (CISSP in good standing counts for all experience requirements for CCSP as well.) If you have 20 years, you're good, I'd imagine.

—Submitted by Cyberconstlearn

Just a friendly reminder: getting certs is one thing, but gaining experience is also important. In my years as a hiring official, I have seen plenty of "cert warriors"—people who were good at taking tests but lacked real-world experience. I'm not saying do not continue your pursuit of certs, just don't only pursue certs. If you have some experience with cloud, then CCSP would be good to go for after the Security+.

—Submitted by CISOScott

Find this complete thread at https://bit.ly/2SRvP1g

QUESTION:

I'm trying to understand perspectives around vulnerability management (VM) scanning. Let's say you VM scan all devices in [a] production environment, disaster recovery environment, and any machine that can connect to said environments at your office. You also work at a budget-conscious company. In this scenario, would you:

(1) Purchase additional VM licenses and champion getting every machine at your office set up with a VM scan?

(2) Do not purchase additional VM licenses; instead, continuing VM scans on machines which connect to production environments? Leverage these scan results as a sampling to address vulnerabilities on all machines?

—Submitted by BennS

SELECTED REPLIES:

VM is a pretty fundamental part of a security program and making sure you have full coverage of your environment is critical. I'd reallocate budget from something else, or even try scanning lower criticality servers with OpenVAS. Risk rate the servers, apply your commercial product to high risk (such as externally connected) and allow low-risk servers to be scanned with something else.

It's like driving at 100 kph down a road. You wouldn't do it if you could only see every fifth car.

—Submitted by Huntington

Everyone is budget conscious. The answer comes down to risk acceptance. At my company, we purchase a site license and install the vuln scanner on all devices to raise the bar and redirect everyone's time and attention to those risk decisions that are more business-facing. Plus, it reduces time pacifying auditors.

—Submitted by denbesten

So why not use a free open source alternative? Yes, it may not be as robust as your current VM solution, but you can use it to supplement for where you do not have licenses, also you can use it to compare. Additionally, depending on your setup, if all your machines are using a baseline template/configuration and you don't have deviations from it, you can just scan the template and not have to worry about the licensing. But be careful with that method as it requires your machines to be exactly the same, otherwise you are ignoring machines.

—Submitted by brandenwagner

Find this complete thread at https://bit.ly/2MUof1R

QUESTION:

I'm using an e-commerce application that collects credit card data and saves it in a database. So far, it's fully compliant and following PCI-DSS standards.

But this credit card data is being sent from an internal app server to a third-party payment processing company by calling third-party REST API. There is no human interface; it happens internally. Currently the data is being passed in a plain text format, card number as is, but the communications between my app server to the third-party API is over HTTPS. I'm wondering if obfuscation/anonymization/tokenization/masking can be used. Does it fall under PCI-DSS compliance? What is the best way to hand over credit card data to a third party in this scenario?

—Submitted by iluom

SELECTED REPLY:

PCI DSS Requirement 4 requires that CHD be protected while in transit

via strong encryption, and that only trusted certificates be accepted. It is perfectly acceptable for you to send plain text CHD over a strongly-encrypted tunnel, as long as you are also validating the TLS certificate being presented by the processor's API to confirm that you are actually connecting to the trusted site that you are expecting to. I also wanted to make sure that you were aware that any system that stores CHD, such as a database, must not be directly connected to the internet.

—Submitted by jimscard

Find this complete thread at https://bit.ly/2NkAHIE

QUESTION:

With so much ransomware in the news I have often wondered if the companies that get hit are simply not following best practices or if there is something I am not aware of. If you are doing your updates, have antivirus and malware which are geared towards ransomware and have proper backups, shouldn't that cover most of this stuff?

—Submitted by JKWiniger

SELECTED REPLIES:

Along with the three you mention, I would add a strong dose of Security Awareness training especially on what is allowed and not allowed on your network, what patching means and why it is done.

—Submitted by dcontesti

I think the most important thing is to have good fine-grained configuration. You can have all the patching and malware protection and backups, but if the configuration is weak then protections can be bypassed, restores can fail, businesses can be unprepared to communicate in an incident.

—Submitted by 4d4m

The prevailing assumption in this thread is that organizations and many local government IT shops are doing the right thing (i.e., the "basics"). Well news flash: they are not. There are lots of organizations that give their users "admin" on their local machines and over-provision roles on databases.

—Submitted by AppDefects

Find this complete thread at https://bit.ly/2FJC67e

CHEERS to your GROWTH in 2020

Take full advantage of **FREE** Professional Development Institute (PDI) courses in the New Year to keep cybersecurity skills sharp and knowledge fresh. Our portfolio is expanding so you never stop learning and growing. In 2020 and beyond, expect more relevant courses, more opportunities to earn CPEs and more value from your (ISC)² membership.

Stay on top of your craft with…

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

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.

LifeWorks PERKS and WELLNESS Support

LifeWorks is a member health and well-being programme which is free for all (ISC)² members.

Members can get their unique invitation code on the member benefit section of their (ISC)² profile.

Wellness Perks EMEA-Wide

LifeWorks is a free, confidential telephone and web-based information and support service designed to give members information and support across a range of issues covering their Life, Health, Family, Money and Work. LifeWorks is available 24 hours a day, as part of your membership.

Member Perks available in the UK

Access personalised, exclusive and relevant perks to save you money! Benefits include discounts on:

- Cinema tickets
- Gym memberships
- Earn cashback online
- Gift cards

Access Perks