TOP WEBINARS AROUND THE WORLD

InfoSecurity PROFESSIONAL

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

MARCH/APRIL 2019

TRUTH OR CONSEQUENCES

Your users aren't the only ones being duped by fake posts and messaging

TALK TO ME

A former CISO discusses how to speak cyber to businesspeople

PROJECT MANAGEMENT

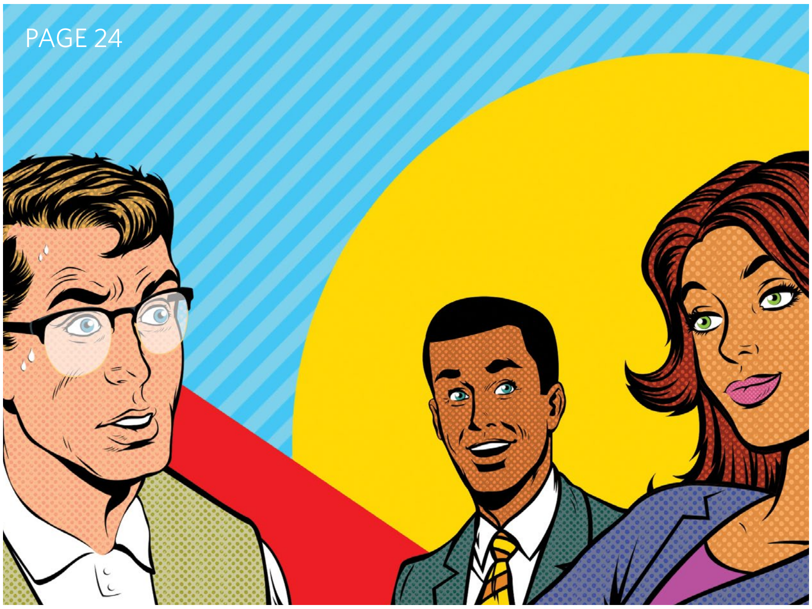
A different way to embed cybersecurity during product development

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

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

contents

VOLUME 12 • ISSUE 2



features

Cover illustration: GORDON STUDER Illustration above: TAYLOR CALLERY

departments

InfoSecurity Professional is produced by Twirling Tiger® Media, 7 Jeffrey Road, Franklin, MA 02038. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)²® on the issues discussed as of the date of publication. For subscription information, please visit www.isc2.org. To obtain permission to reprint materials, please email infosecproeditor@isc2.org. To request advertising information, please email lpettograsso@isc2.org.

editor's note *by Anne Saita*

Let's Get Real

YEARS AGO, when I was an adjunct instructor at a major American university, I saw a request on an education listserv (remember those?) and struck up an email conversation with a professor trying to connect students with professionals in the field. The email address looked legit, so I passed on her request to an old college friend willing to assist. I thought nothing of it until months later, when I got a call from that friend letting me know the professor didn't exist. Something in one of the emails felt off, he said, so he did some digging and discovered we'd both been part of some scam with an elusive endgame.

"Aren't you, of all people, supposed to not fall for this kind of thing?" he said. By then I was about five years into covering the information security industry, and I took that comment badly.

This issue's cover story on how to find credible sources in an era of disinformation touches on something similar. We've written in previous issues about the ongoing success of sophisticated phishing and vishing, but mainly by pointing to the end users that (ISC)^2 members serve. This time, we look more inward. As BeyondTrust's Brian Chappell notes, "While security professionals [as individuals] are—generally—less likely to fall prey to cyberattacks, they are far from invulnerable, and certainly not immune."

It's my hope that after reading James Hayes' article, each of you will reconsider some of the ways you too can be exploited, especially as more LinkedIn-type solicitations show up in your inbox due to a growing global cybersecurity labor shortage. In our other features, you also may pick up some great tips for embedding security in projects, both planned or underway, and learn the language of business from a former CISO to better engage with other units within an organization.

As always, feel free to let me know what you think and what you'd like to see more of in future magazine features. ■

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 certified as a Women's Business Enterprise (WBE) by the Women's Business Enterprise National Council (WBENC). This partnership reflects (ISC)^2's commitment to supplier diversity.

RETURN TO CONTENTS

(ISC)² SECURITY CONGRESS 2019

EARLY BIRD PRICING

–through August 15–

Oct. 28 - 30 • Orlando, FL • Swan & Dolphin

(ISC)² Members SAVE $200 | 4000+ Attendees & 100+ Sessions | Earn up to 46 CPEs

All Access Pass Benefits:

- Educational Sessions, Keynotes & Workshops
- Networking Luncheons
- Expo Hall
- Town Hall & Career Center
- Networking Night
- CSA Summit & Expo Hall Pub Crawl

SAVE $50

Off All Access Pass

with code:

INFOSECD18

REGISTER TODAY!

congress.isc2.org

#ISC2Congress

30 Years of Inspiring a Safe and Secure Cyber World

by David Shearer

HARD TO BELIEVE, but this year marks our 30th anniversary. As we approach 150,000 members worldwide, I wanted to reflect on what we've accomplished recently and where we're heading.

Improved Online Security and Platforms

We added multifactor authentication as an additional layer of security to our members' online (ISC)² accounts, along with an improved web-based member dashboard. The upgrades are part of a huge digital transformation that took place largely in 2018 so members can better manage their memberships, leverage (ISC)² benefits and engage with our staff.

(ISC)² Security Congress Moves to Orlando

This year's annual Security Congress will be held Oct. 28 to 30 at the Walt Disney World Swan and Dolphin Resort in Orlando. After two back-to-back sold-out conferences, we wanted a larger venue in a city with an international-travel-friendly airport so more members from around the globe can attend. Orlando fits that bill and will be the home of Security Congress for years to follow. Registration is open now, so make plans to join us in Florida later this year!

New Advocates in Asia-Pacific and EMEA

Tony Vizza, CISSP, joined our team as Director of Cybersecurity Advocacy, Asia-Pacific. With more than 25 years of experience, Tony is focused on educating the public and private sectors about the need for stronger cybersecurity training, policies and recruitment. Mary-Jo de Leeuw recently joined (ISC)² as our Director of Cybersecurity Advocacy, EMEA. Last year, she was ranked as one of the U.K.'s 50 most influential women in cybersecurity, and we are thrilled to have her as part of our team.

David Shearer is CEO of (ISC)². He can be reached at dshearer@isc2.org.

Helping to Keep Families Safe Online

The nonprofit Center for Cyber Safety and Education continues to expand all its Safe and Secure Online educational and scholarship programs around the world. The award-winning Garfield cyber safety education program for children has been proven to increase cyber safety knowledge by 28 percent. The materials for parents and seniors are currently available in eight languages and the Center's goal is to have them in 30 languages this year.

Workforce Gap and Additional Industry Research

Our latest Cybersecurity Workforce Study found the cybersecurity skills shortage growing to a 2.93 million global gap. But our research is focused on more than the gap as we examine challenges facing the profession to find solutions for not just the profession, but the professional. Other 2018 research reports include Building a Resilient Cybersecurity Culture and Hiring and Retaining Top Cybersecurity Talent.

Think Tank Webinar Channel Lauded

The (ISC)² Think Tank webinar channel, which features 60-minute roundtable discussions with industry experts, last year was named "Highest Growth Channel" in the IT category by BrightTalk. If you're not already taking advantage of these free webinars, I highly encourage you to do so.

Look for More Professional Development Opportunities

A key focus for (ISC)² this year is professional development. We want to ensure that all of our material is deeply enriching to members' careers, no matter where they are in their journey. We debuted multiple new courses last year that are free to (ISC)² members and will introduce more courses later in 2019.

We hope to see many of you throughout the year at our (ISC)² Secure Summits and at Security Congress in October. ■

RETURN TO CONTENTS

(ISC)²

SECURE SUMMIT / DC

ENRICH ENABLE EXCEL

Defining Cybersecurity in 2019

Join us at (ISC)² Secure Summit DC for two days of insightful discussion, workshops and best-practices sharing. Focused on **Defining Cybersecurity**, the event will address our profession's greatest challenges and effective new approaches for preparing and defending national cybersecurity in today's workforce.

Secure Summit DC 2019 will feature these tracks:

- The Profession and Your Responsibilities
- Threats
- New Technologies
- Industrial Control Systems
- IoT

Why You Should Attend

- Gain tools and resources to become a more effective and well-rounded practitioner
- Complement broad understanding of cybersecurity strategies and principles
- Strengthen your organization's security posture
- Network with like-minded professionals
- Earn valuable CPE credits

Register Now

field notes ▮▮▮ EDITED BY DEBORAH JOHNSON

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

Accolades for the (ISC)^2 CISSP Certification

THE (ISC)^2 CISSP is "one of the best known and most widely respected cybersecurity certifications of them all…." That praise is the opening salvo to *Certification Magazine's* review of the CISSP certification, *Salary Survey Extra: Deep Focus on (ISC)^2's CISSP.*

The 2018 Salary Survey placed the CISSP at No. 20, with an annual average salary for certificate holders of $131,030 in the United States and $90,640 (USD) for non-U.S. respondents. Nearly 70 percent of the U.S. respondents reported being satisfied with their salary; the magazine did not cite the percentage of non-U.S. respondents.

> 80 percent of the respondents agree[d] that "since becoming certified, I feel there is a greater demand for my skills."

When it comes to demographics, the CISSP cuts a wide swath. The survey noted the "progressive" makeup of the certification holders, with 10.2 percent women. The age breakout shows that most (89 percent) of the respondents are in prime working age: between the ages of 35 and 44 (25.1 percent), 45 and 54 (39.1 percent), or 55 and 64 (29.1 percent).

The survey also revealed that CISSP holders experience the value of the certification, with more than 80 percent of the respondents agreeing that "since becoming certified, I feel there is a greater demand for my skills." More than half (59.6 percent) agreed that "becoming certified has increased my workplace productivity."

To view the complete results of the survey, visit http://certmag.com/salary-survey-extra-deep-focus-isc2s-cissp/. ■

Images: iStock

2019 Key IT Investments

- Business Intelligence/Data Analytics
- Cyber/Information Security
- Cloud Services
- Core System Improvements
- Digital Business Initiatives
- Customer/User Experience
- Artificial Intelligence/Machine Learning

Source: *CIO* from IDG, *7 Key IT Investments for 2019 (and 3 Going Cold)*
https://www.cio.com/article/3328685/budget/hot-and-cold-tech-investments-budget-trends.html

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=10803

RETURN TO CONTENTS

Top Webinars for 2018*

Webinars produced by (ISC)² in collaboration with a project sponsor

**Ranked by view rating*

NORTH AMERICA

TITLE	SPONSOR	LINK
The Workforce Gap Widens: The Need to Focus on Skills Development	(ISC)²	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=338201
The Hunt for IoT and Its Threat to Modern Life	F5	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=304619
Levers of Human Deception: Science & Methodology of Social Engineering	KnowBe4	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=334390
Threat Detection in TLS: The Good, Bad & Ugly	Gigamon	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=321233
Information Security: Organizational Dynamics	451 Research	https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=315933

EMEA

TITLE	SPONSOR	LINK
Machine Learning in Infosec: Debunking Buzz and Demystifying Use Cases	Splunk	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=332973&top10
TLS Decryption: Critical to Detecting Threats	Gigamon	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=334809&top10
Enriching Your Security Product Stack With the Power of IPAM and DNS	Infoblox/Logicalis	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=337164&top10
GDPR Compliance – Don't Let Your SIEM Be Your Downfall	Splunk	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=304791&top10
As Attackers Evolve, So Must Machines: Advancing Machine Learning Beyond the Hype	Carbon Black	https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=307351&top10

APAC

TITLE	LANGUAGE	SPONSOR	LINK
State of the Internet/Security 2018: Web Attacks and a Case Study of Effective Bot Management	Chinese	Akamai Technologies	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=341849
Control Digital Data and Make a Business: A Key Point for Achieving 100% Utilization of the Cloud and Compliance	Japanese	Symantec	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=339836
Cyber Exposure: Insights into Security Risks/Vulnerability Situation Analysis	Chinese	Tenable	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=335578
Protecting Your Organization Inside Out Using Identity	English	Akamai Technologies	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=340708
Security at Network Speeds	English	Gigamon	https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=312817

Image: iStock

RETURN TO CONTENTS

(ISC)² Names New Cybersecurity Advocate for the EMEA Region

Mary-Jo de Leeuw is an award-winning cybersecurity leader

MARY-JO DE LEEUW, recently ranked as one of the U.K.'s 50 most influential women in cybersecurity, has joined (ISC)² as its Director of Cybersecurity Advocacy for the Europe, Middle East and Asia (EMEA) region. As an advocate, de Leeuw will work to encourage cybersecurity collaboration in developing strong cybersecurity policies, legislation and education in the EMEA region.

"As our recent research shows, our industry has a long way to go to narrow the cybersecurity workforce gap," said (ISC)² CEO David Shearer, CISSP. "That's where Mary-Jo's experience will be so helpful to our membership. Her background is not only as a strategic consultant herself but as a community builder and connector of women in business around the world. We need more women driving the conversation and Mary-Jo has a proven track record of creating interest and excitement around cybersecurity."

> "Ever since my first Commodore 64, I've been fascinated by bits and bytes and the implications of cybersecurity on how we connect."
>
> —*Mary-Jo de Leeuw*

De Leeuw joins (ISC)² after serving as an associate partner for cybersecurity and innovation at Revnext, a Dutch high-tech consulting firm that advises executive management of governments, listed companies and NGOs.

Based in The Hague, The Netherlands, de Leeuw will report to (ISC)² Managing Director for EMEA Deshini Newman. "As we continue our vision to make a difference in the region, it's vital to have strong leaders like Mary-Jo join our mission to inspire a safe and secure cyber world," said Newman. "Her insights globally will be a great asset for (ISC)² in the EMEA region as we serve our growing membership."

"Ever since my first Commodore 64, I've been fascinated by bits and bytes and the implications of cybersecurity on how we connect," said de Leeuw. "I can't think of a better avenue for devoting my energy than promoting the cybersecurity industry with (ISC)² and creating opportunities for those who are interested in joining the profession."

De Leeuw holds a bachelor's degree in information technology from the University of Applied Science, Utrecht. She is a winner of a European Cybersecurity Excellence Award 2018 and was ranked 10th among 50 global influencers for Europe. She was also ranked No. 10 by IFSEC International and received the global "Iconic Women 2017, Creating a Better World for All" award during the 2017 World Economic Forum in The Hague. ■

Steely Dan Founding Member Among Keynotes at (ISC)² Secure Summit DC

Jeffrey "Skunk" Baxter, national security expert and founding member of the band Steely Dan, will be one of two keynote speakers at Secure Summit 2019 held April 23 and 24 at the Washington (D.C.) Hilton Hotel.

The other keynote will be delivered by Tiffany Olson Kleemann, chief executive officer of Distil Networks and a member of the (ISC)² Board of Directors.

More than 80 professionals from the public and private sectors will be on hand to lead discussions and workshops, sharing expertise and insight on key issues facing the cybersecurity community.

This year's Summit focus is "Defining Cybersecurity" and will feature four distinct tracks:

- The Profession
- Threats
- New Technologies
- Industrial Control Systems and IoT

"(ISC)² Secure Summit DC is a tremendous opportunity for cybersecurity leaders in government, military, industry and academia to come together for networking and educational sessions that will help them broaden their cybersecurity strategy toolbox," said Brian Correia, managing director for North America, (ISC)².

Attendees will earn 18 Continuing Professional Education (CPE) credits.

To register for Secure Summit DC, visit https://web.cvent.com/event/036c40ab-432b-4af1-ae86-f5a43d6ef9fc/websitePage:826f4417-ca67-4598-b662-25c5ac6e37da. ■

(ISC)² Richmond Metro Chapter Rises to the Challenge

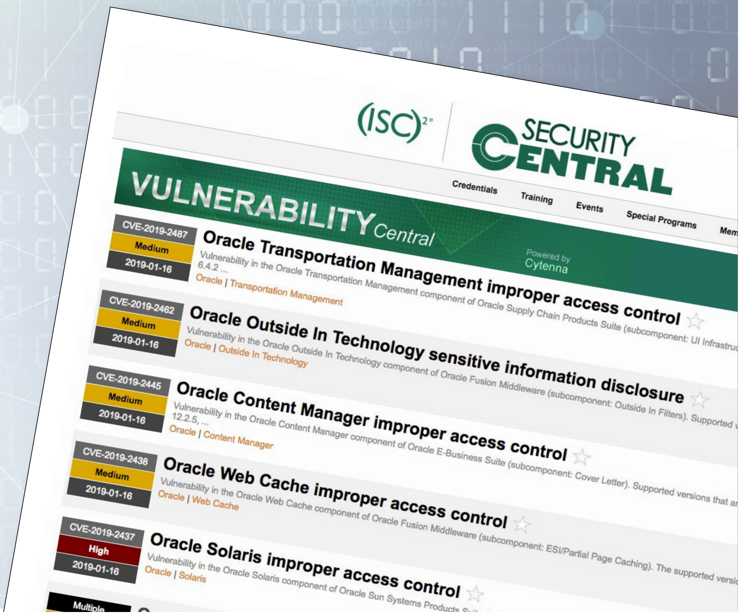
WHEN IT COMES TO CHALLENGES, fundraising can be one of the most difficult. The Richmond Metro (Virginia) Chapter deserves a shout-out for successfully tackling the most recent (ISC)² Scholarship Challenge. Participating chapters are asked to raise at least $1,500, $750 of which is earmarked for the Center for Cyber Safety and Education’s scholarship fund.

Since the chapter’s inception in 2016, the members have raised more than $12,000 and awarded 10 scholarships to area high school students. The chapter partners with local companies and organizations, area schools and its own membership to raise money. In 2018 alone, $5,750 was raised, with five $1,000 scholarships awarded.

Chapter Vice President Chris Schurman, CISSP, GWAPT, CEH, says that the scholarship challenge is one they take on happily. “The Center for Cyber Safety and Education’s Chapter Scholarship Challenge aligns perfectly with [our] chapter’s mission to foster the next generation of cybersecurity professionals. As such, we expect to continue volunteering for the challenge every year that it remains available.”

For more information on the scholarship challenge, see https://iamcybersafe.org/scholarships/chapter-scholarship-challenge/. ■

Richmond Metro Chapter Fundraising Committee: From left, John Styles, membership chair; Michael Stapleton, treasurer; Ivan Gil, president; and Chris Schurman, vice president.



CVE-2019-2487 | Medium | 2019-01-16
Oracle Transportation Management improper access control ☆
Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: UI Infrastruc 6.4.2 ...
Oracle | Transportation Management

CVE-2019-2462 | Medium | 2019-01-16
Oracle Outside In Technology sensitive information disclosure ☆
Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported v
Oracle | Outside In Technology

CVE-2019-2445 | Medium | 2019-01-16
Oracle Content Manager improper access control ☆
Vulnerability in the Oracle Content Manager component of Oracle E-Business Suite (subcomponent: Cover Letter). Supported versions that ar 12.2.5, ...
Oracle | Content Manager

CVE-2019-2438 | Medium | 2019-01-16
Oracle Web Cache improper access control ☆
Vulnerability in the Oracle Web Cache component of Oracle Fusion Middleware (subcomponent: ESI/Partial Page Caching). The supported versi
Oracle | Web Cache

CVE-2019-2437 | High | 2019-01-16
Oracle Solaris improper access control ☆
Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products S
Oracle | Solaris

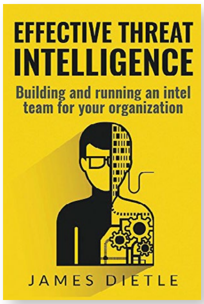
Multiple

RECOMMENDED READING

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

Effective Threat Intelligence: Building and Running an Intel Team for Your Organization

By James Dietle
(CreateSpace Independent Publishing, 2016)


EFFECTIVE THREAT INTELLIGENCE
Building and running an intel team for your organization
JAMES DIETLE

FOR AN ORGANIZATION seeking to build a threat intelligence program and develop its security operations center (SOC) team, *Effective Threat Intelligence* offers clear and methodical guidance. Author James Dietle educates the user in the basic steps: defining requirements, locating data, establishing a timeline, and identifying risks and threat vectors affecting the firm, all in a calm, controlled, no-nonsense manner.

While many firms are experiencing growing pains attempting to quantify threats, controls and risks impacting them, there are also a variety of vendors selling threat solutions, which may or may not be compatible with an organization's needs.

The strength of this book is that Dietle helps readers understand and define their initiatives. Like any other program, he understands that it is a journey and not a race and presents a maturity program from level one—with the absence of a plan for threat intelligence—to level five, a developed plan with a dedicated intelligence team.

> The strength of this book is that Dietle helps readers understand and define their initiatives.

Missing from this book is a contact list of the data feeds and available tools in the marketplace (though that material might be dated given the book's 2016 publication date). And *Effective Threat Intelligence* may not be the right guide for all, as it does not offer a "quick fix" or step-by-step instructions. Rather, it enables the reader to explore the options based on budget and long-term needs.

For me, the book gave me food for thought and showed me that for a new field, it is up to the professional to define requirements and perform a proof of concept on the software that is either purchased or built. ■

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.

HUMAN ELEMENT

50%

of data breaches involve an insider threat

Revealed in a review of 7,800 data breaches

Source: McKinsey & Company, *Insider threat: The human element of cyberrisk*

https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

SPENDING SPREE

$57.6 BILLION IN 2021

Forecast for worldwide spending on cognitive and artificial intelligence (AI) systems

Source: IDC,*Worldwide Semiannual Cognitive Artificial Intelligence Systems Spending Guide*

https://www.idc.com/getdoc.jsp?containerId=prUS43095417

> **"In 2019, cybersecurity engineers will be the best-paid, most recruited tech professionals as organizations struggle to fill vacant cybersecurity positions."**
>
> *—Jan. 9 (ISC)² blog post*

RETURN TO CONTENTS

(ISC)² NORTHERN VIRGINIA CHAPTER

New Chapter Serving Metro D.C. Is Up and Running

Combining strong community support and member opportunities provides a boost

NOVA members at the chapter bylaws ratification meeting.

SINCE BECOMING AN OFFICIAL CHAPTER last summer, (ISC)² Northern Virginia (NOVA) has pursued a variety of opportunities for members to connect, educate, inspire and secure. To get a firsthand look at (ISC)² in action, some of the chapter's board members met with (ISC)² employees and trainers in the Alexandria office. Discussions about certifications and professional development courses gave the chapter leaders exciting and relevant information to bring back to the membership.

Last fall, the NOVA Chapter engaged members in three diverse chapter events. Speakers from Walmart Labs and Freddie Mac shared their concerns and activities in information security. In addition to the formal presentations, the chapter also hosted a "Tech Talk" installment at Nova Labs in Reston. The talks offer members the opportunity to network and learn new skills in a more informal setting. These events give chapter members a variety of both hands-on and lecture-style CPE opportunities.

The chapter has been fortunate to have gracious hosts to provide facilities for the larger meetings, while the board has been very busy working on building a tech stack and supporting processes to help fulfill the needs of a growing chapter with some 170 charter members. The chapter could not do it without its amazing sponsors such as Capital One, CrossCountry Consulting, Cyxtera, IT Availability, RPM, South 6 and Zeneth.

(ISC)² NOVA has gotten a strong start and looks forward to bringing even more opportunities for members to connect, educate, inspire and secure in the years ahead. ■

Chapter members practicing their lockpick skills at a Tech Talk event.

(ISC)² NORTHERN VIRGINIA CHAPTER

Contact: Dan Waddell, President, (ISC)² Northern Virginia

Email: president@novaisc2chapter.org

Website: https://novaisc2chapter.org

Twitter: @NOVAISC2CHAPTER

Q&A

Dan Waddell

President, (ISC)² Northern Virginia Chapter

Your chapter has strong corporate partnerships. What advice do you have for other chapters for recruiting sponsors and lining up corporate partners?

First, make sure you are adding value to your sponsors. We are fortunate to have one of the largest concentrations of (ISC)² members in the world here in Northern Virginia, which gives our sponsors a unique opportunity to engage with members and speakers from all aspects of cybersecurity. Also, appoint or vote in someone to join the board and lead the overall sponsorship effort; empower that person to make decisions and give them the resources they need to accomplish the mission.

How does the chapter develop the various programs you offer?

All members of the board are involved in developing our programs, but they're based on input we get directly from our members. We're still relatively new, but we've been able to offer monthly meetings that feature speakers in an engaging lecture-style/Q&A session as well as more technical hands-on meetups. Both formats offer CPE opportunities for our members, which we submit on their behalf.

I'm also very excited to launch our "intern" membership program this year, which allows undergrads an opportunity to join the chapter for free. We developed this program in response to the data we have seen in the last few (ISC)² workforce reports, which continually highlight the need to get more younger professionals into our career field.

> "I'm also very excited to launch our 'intern' membership program this year, which allows undergrads an opportunity to join the chapter for free."
>
> —*Dan Waddell*

What kind of feedback are you getting from members to the events the chapter presents? Have you seen membership grow as a result?

We had good attendance at our initial meetings in November and December. Plus, we've had a number of recent additions to our board—all of whom have hit the ground running. The chapter has set a goal to hit 200 members this year, and each month there's been an increase, so I'm confident we'll reach and exceed our goal by the end of 2019.

What is the biggest challenge in keeping the membership engaged and the chapter relevant?

With such a large group, there's always the challenge of finding meeting space to host and then executing the logistics necessary to pull off an event that our members can be proud of. We've been fortunate enough so far to find local organizations such as Fannie Mae, Freddie Mac and Capital One to host and, of course, having dedicated and passionate board members to pull it off and making sure we are giving value back to our chapter members. ■

Bad Work Habits Survey

Based on responses from 600 small business employees

Source: Switchfast, *Cybersecurity Mistakes All Small Business Employees Make*

https://cdn2.hubspot.net/hubfs/1747499/Content%20Downloads/Switchfast_SMB_Cybersecurity_Report.pdf

FOOTLOOSE

62%

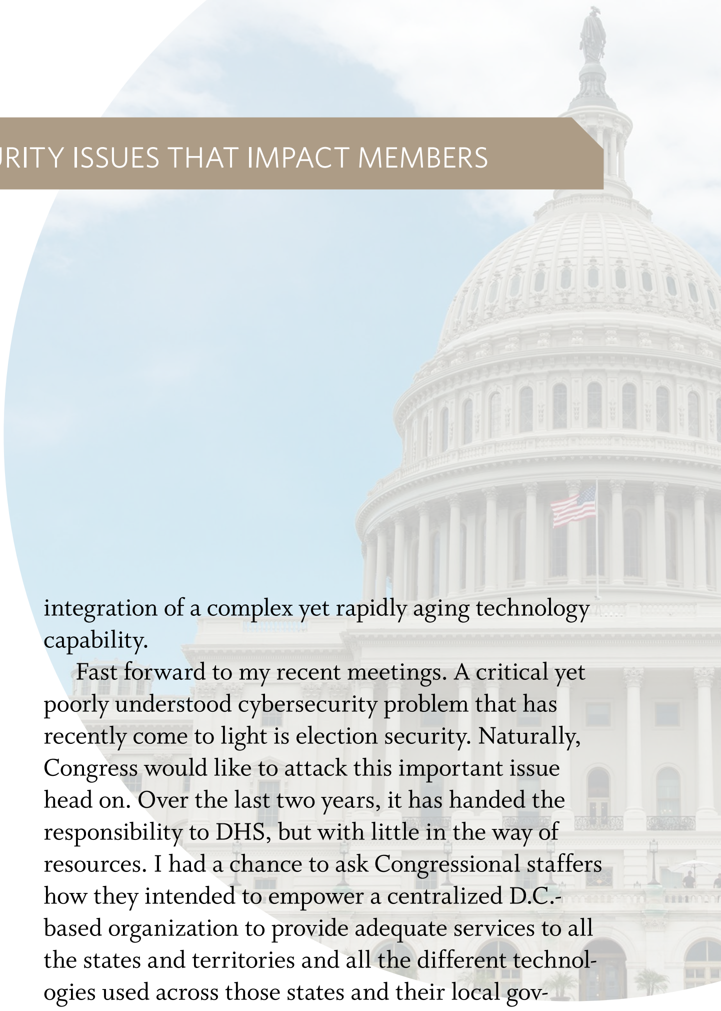
of respondents say they use their work computers to access personal social media accounts

FANCY FREE

66%

of respondents say they connect to public Wi-Fi to do work

RETURN TO CONTENTS



Power to the People

by John McCumber

I RECENTLY COMPLETED another round of meetings on Capitol Hill. My days with the nation's movers and shakers are always busy and fraught with frustration. One vexation is the natural inclination of legislators to try to address all our national concerns with, well, legislation. It's the old saw about your only tool being a hammer. I guess they all mean well, but bill authors often create as many (if not more) problems than they solve. Take cybersecurity, for instance.

I can fill a library with ill-fated laws, regulations, edicts, directives, injunctions, doctrines, tenets and guidance designed to help set the standards for what we now call cybersecurity. Many of them started with the assumption that cybersecurity was just like security, but with more cybery stuff. Sadly, it's not that simple.

One key problematic area remains a thorn in the side of federal, state and local authorities. It's the result of legislation that mandates activities or outcomes without providing any resources needed to enact them. In fact, these new pronouncements rarely even acknowledge that an investment of resources will be required. We refer to these as "unfunded mandates." When these appear in legislation, affected departments and agencies are quick to fight back.

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

Legislators have lately become more sensitive to unfunded mandates, so some recent proposals have included the idea that federal agencies charged with national cybersecurity responsibilities will need to be funded to deliver new, ostensibly more secure, capabilities where they are needed. One such effort saw the Department of Homeland Security (DHS) deploy massive state-level intrusion detection and prevention technology to all American states and territories. It became a maddening mess as the (un)lucky recipients of this federal largesse had to manage the technical integration of a complex yet rapidly aging technology capability.

Fast forward to my recent meetings. A critical yet poorly understood cybersecurity problem that has recently come to light is election security. Naturally, Congress would like to attack this important issue head on. Over the last two years, it has handed the responsibility to DHS, but with little in the way of resources. I had a chance to ask Congressional staffers how they intended to empower a centralized D.C.-based organization to provide adequate services to all the states and territories and all the different technologies used across those states and their local governments to tabulate votes. That drew a shrug from across the table. I suggested a more focused solution.

> **I can fill a library with ill-fated laws, regulations, edicts, directives, injunctions, doctrines, tenets and guidance designed to help set the standards for what we now call cybersecurity.**

"Have you considered empowering the people in those government agencies and departments to do the job themselves?" I asked.

"Well, I don't think they have the necessary skills and knowledge," was the expected reply.

"Precisely," I said, "People are the missing factor. You try to deal with technology, policy and procedures, but you leave out the most critical factor: people. Provide workers with the knowledge tools they need for the 21st century and let them make the best decisions from their perspective. We all win."

Well, the jury is still out on whether my suggestions will find their way into upcoming legislation. Keep an eye on the news coming out of Washington and let me know what you see. ■

Photograph: iStock

RETURN TO CONTENTS

(ISC)²

SECURE SUMMIT / LATAM

#ISC2LatamSummit

ENRICH **ENABLE** **EXCEL**

Join us at the (ISC)² Secure Summit LATAM 2019

September 25-26 | Hotel Camino Real Polanco, Mexico City

The event will offer educational sessions presented by thought-leadership experts from all over the region and abroad.

Come share best practices and knowledge and meet your peers in a relaxed learning atmosphere.

(ISC)² members can earn up to 16 CPEs

latamsummits.isc2.org

REGISTER NOW

(ISC)² Secure Summit LATAM | September 25-26, 2019 | Mexico City

(ISC)²

SECURE SUMMIT / EMEA

ENRICH ENABLE EXCEL

http://securesummits.isc2.org

(ISC)²

ISLA

Europe, Middle East, Africa

(ISC)² Secure Summit EMEA 2019

The 2019 Secure Summit EMEA will be a unique experience, taking place 15-16 April 2019 at the World Forum, the largest international conference venue in The Hague, Netherlands. The pre-Summit day on 14 April will also feature three deep-dive workshops, enabling delegates to learn from the most experienced and brightest in our profession.

REASONS TO ATTEND

- 40+ sessions, six themed tracks
- Deep dive workshops
- Simulation exercises and immersive interactive activities
- Town Hall session with the (ISC)² leadership team
- Networking opportunities
- Earn up to 24 CPEs: 50% more than previous events

Keynotes

At the (ISC)² Secure Summit EMEA, you will hear from thought-provoking, inspiring and industry-leading speakers. Supporting the conference sessions will be a series of keynote speakers including:

Dr. Jessica Barker,
Co-Founder, co-CEO,
Cygenta

Lorna Trayan,
Strategy Leader,
IBM Security Services MEA

Felicity Aston,
MBE, British Polar Explorer,
Scientist, Author

Joseph Carson,
Chief Security Scientist &
Advisory CISO, Thycotic

Register to attend now at: http://securesummits.isc2.org

(ISC)² Information Security Leadership Awards (ISLA) EMEA 2019

The ISLA EMEA awards distinguishes information security and management professionals for exceptional leadership and achievements in workforce improvement.

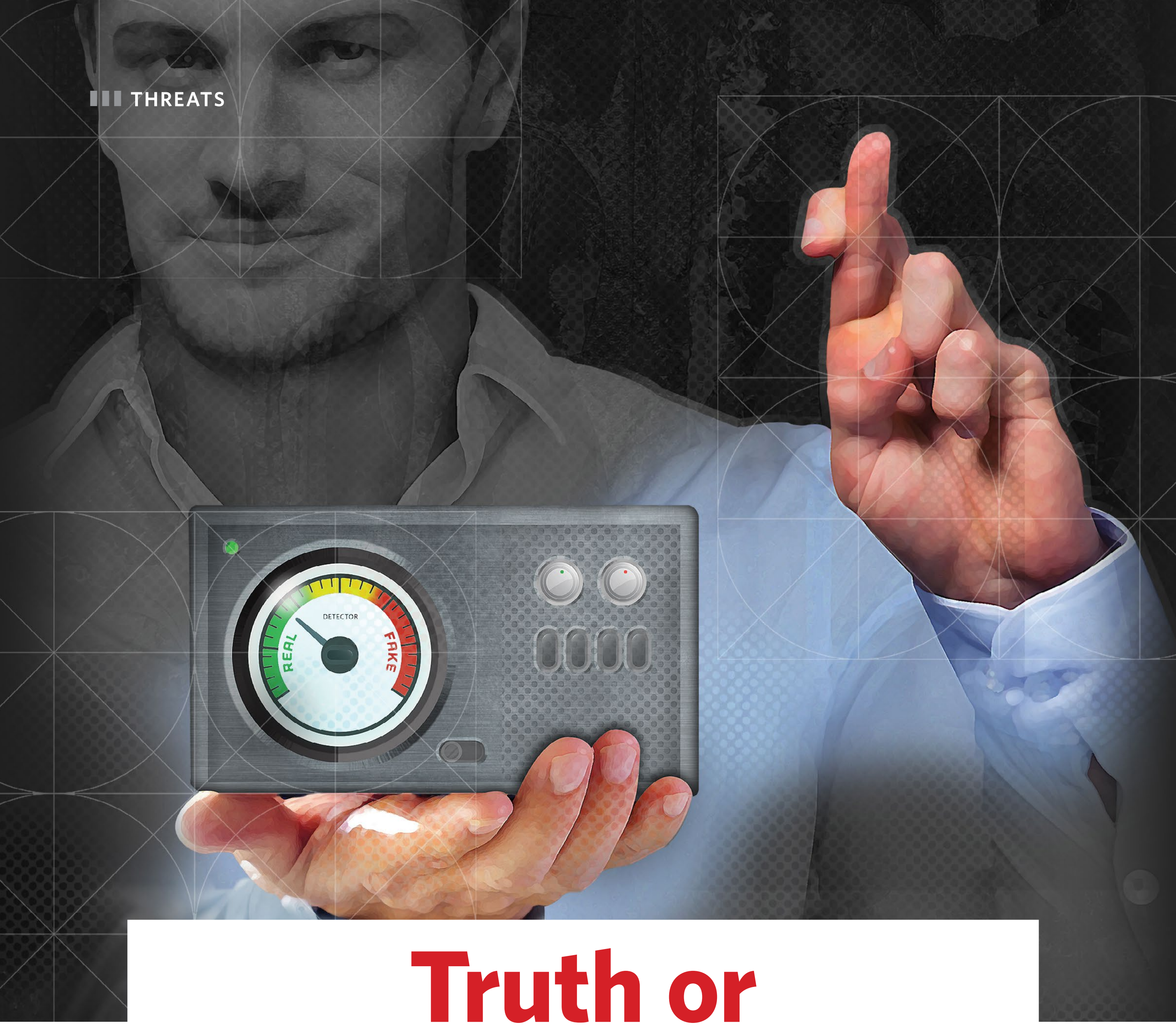
2019 AWARD CATEGORIES:

- Senior Information Security Professional
- Information Security Practitioner
- Up-and-Coming Information Security Professional
- Woman Information Security Professional

Finalists and winners will be recognized by 400+ like-minded industry professionals at the Awards Ceremony lunch on 15 April, during the (ISC)² Secure Summit EMEA 2019.

Have any questions?
Need more information?
Contact isla.emea@isc2.org

(ISC)²



Truth or Consequences

BY JAMES HAYES

It is becoming harder, even for seasoned cybersecurity professionals, to discern what's real and what's fake

ILLUSTRATION BY GORDON STUDER

WHEN ENTREPRENEUR ELON MUSK took to Twitter to call for a website "where the public can rate the core truth of any article and track the 'credibility score' over time of each … publication," he was tapping into wider concerns about how online media now routinely carries misinformation, falsehoods and fabrications.

The issues of misinformation and disinformation have risen sharply in recent years due to geopolitical campaigns now known to have influenced

RETURN TO CONTENTS

democratic elections around the world. Disinformation campaigns also resonate sharply in enterprise IT security, where speed-to-action prompted by alerts and notifications from diverse sources can make critical differences in defensive counteraction to cyberattacks.

In this era of disinformation, unmediated sources of threat intelligence like social networks, web forums and newsfeeds can deliver misguided and misleading information mixed in with actual alerts and malware trends. Cunning cybercriminals leverage ways in which they can use such channels to target IT security personnel for a multiplicity of malicious motives.

So, what's an information security specialist—or anyone in IT, for that matter—supposed to do to not fall victim to increasingly sophisticated phishing or social media scams and fake threat intelligence reports or fraudulent security alerts?

EVERYONE'S VULNERABLE TO BEING DUPED

Spear phishing aimed at specific professional profiles has risen sharply, says Kaspersky Lab, which reported a 27.5 percent increase during Q3 2018. That amounted to more than 137 million attempted phishing attacks—equal to the number aimed at online payment systems, and only 8 percent less than the number of such attacks aimed at banks.

The rapid change dynamics of the information and communications (ICT) sector also provides ideal conditions for cybercriminals to perpetrate fraud and fakery around "breaking" news. "As new technological and informational updates appear, phishers exploit them," cautions Kaspersky Lab security researcher Nadezhda Demidova.

For those who work in cybersecurity, the challenge is twofold: first, to be alert to the methods targeting them and, second, to ascertain which sources of information are trustworthy and which are not. The key is to realize that information security professionals are susceptible to being duped just like everyone else.

"IT security professionals operate in one of the fastest-moving areas of technology," says Brian Chappell, senior director of enterprise and solutions architecture at BeyondTrust, a cybersecurity firm based in Phoenix. "As a result, there's been high reliance on external sources of data regarding threats, albeit combined with output from monitoring tools. While security professionals [as individuals] are—generally—less likely to fall prey to cyberattacks, they are far from invulnerable, and certainly not immune."

Bristol, U.K.-based Red Goat Cyber Security has "increasingly seen successful attacks against cybersecurity experts that highlight that no one is invulnerable to them," reports company partner Lisa Forte. "Attacking cybersecurity organizations and experts yields much kudos for the attackers."

Indeed, the very status of their role makes security specialists an attractive "trophy challenge" to cybercriminals, agrees Rafael Amado, senior strategy and research analyst at risk management firm Digital Shadows: "Infosecurity professionals specialize in learning about, detecting and defending against cyberthreats, and in minimizing the risks to their organizations. It would be very naive for anyone to assume that they won't be targeted."

Overconfidence can also cause security professionals to take additional risks, says Adedayo Adetoye, principal strategic security engineer at Mimecast, a Lexington, Mass., firm that specializes in email security: "Antivirus researchers, for instance, often don't want to work through AV tools that might interfere with their research [and so deactivate them]. Similarly, network security teams might turn off their firewalls for R&D purposes."

TAILORED ATTACK TYPES

IT security professionals will not be surprised to discover that, like every other connected colleague in their organizations, they will likely be targeted by online threat actors. What might come as more of a revelation is the forethought and craftiness cybercriminals apply to tailoring attacks to their specific job profiles. Examples include:

- Counterfeit email invitations to real industry events (e.g., conferences)
- Inducements to download free insight collateral (e.g., reports, infographics)
- Blog posts on bogus "breaking news"
- Made-up warnings about insider threats
- Sham customer messages from technology partners
- Bogus recruitment agencies that pitch mocked-up job opportunities

The obvious intention is to solicit a response from the recipient, often by creating the impression that they have been specially selected for controlled access to privileged information, or for a place at a limited-attendee event. More sophisticated attacks might reference additional information about an individual, such as their involvement with a technology specialty that's been (unwittingly) divulged on social media.

"As with any form of social engineering, cyberattackers look to play on a target's specific interests and craft their lures in a way to make them as appealing as possible," says Digital Shadows' Amado. "That's why there have been phishing campaigns that use cybersecurity industry event lures, or [that use] malicious attachments that claim to be new technical or intelligence reports, [but which in fact] deliver malware."

While a generic phishing attack "is unlikely to get through the natural filters of an IT security professional, spear-phishing attacks can be subtler," says BeyondTrust's Chappell. "Anyone who is overloaded by information and activity in the workplace can almost be excused for responding to what looks like a legitimate email."

IT teams are very busy, agrees Ross Brewer, vice president and managing director of Europe, Middle East and Asia at Boulder, Colo.-based security firm LogRhythm, which can "make it challenging to pay full attention and not click on links that, if they took the time to assess, would seem suspicious. The most seasoned and experienced IT professional can be taken in." When they target information security teams, adds Brewer, cybercriminals are "doing what they think no one would expect. It's a brazen approach that relies on the fact that companies will be less prepared for a dedicated attack than targets whose job it is to protect the company…. To succeed, they require not only persistence and intelligence, they also rely on the element of surprise."

DEPLOYING THE RIGHT LURE

"I'm certainly aware of phishing campaigns where victims have received email lures and malicious attachments that pretend to be invites to cybersecurity conferences," says Digital Shadows' Amado. "In one case the attackers used the actual documentation found on the real conference website."

An example from Red Goat Cyber Security's Forte is the case of a CISO who was, from his LinkedIn posts, clearly keen to get onto the security event speaking circuit.

"The attacker had watched a YouTube video of one of the CISO's talks at a local get-together. In the initial email, the attacker claimed to have been in the audience, cited specific things they liked about the talk and pretended to be organizing an actual upcoming security conference," recounts Forte. "Obviously, as this is a real conference, when the targeted CISO Googled it he assumed it was legitimate. The attacker proceeded to invite him to speak at the event and attached the speaker registration form to the email. What happened next you can probably guess. This is just one of many cases [I've seen] where IT security professionals have been targeted."

Bogus job postings are another area where security professionals can be, and have been, duped, adds Amado. "We've detected examples on both 'dark' and seemingly benign open web forums where users have posted job adverts for security engineers and penetration testers. In some instances, these posts are, in fact, made by cybercriminal outfits to recruit techies to set up and maintain their operational infrastructure [without realizing the true nature of the job]."

According to Andy Harris, chief technical officer at London-based access manager Osirium, "Malicious actors posing as recruiters ask questions like, 'How would you protect hypervisors and backups?' and 'Do you have experience in doing this? Is this how you currently do things?'" Such seemingly routine lines of inquiry can yield valuable background knowledge for cybercriminal tacticians.

"An IT security professional may [in job applications] divulge the particular types of defensive hardware and software their company employs, even naming specific models," says Amado. "[This is] valuable reconnaissance for an attacker looking to socially engineer employees in the organization or to create appropriate tools to perform a network compromise or deliver bespoke malware."

SORTING THE GOLD FROM THE GUILE

With the amount of cybersecurity data available to feed threat intelligence increasingly discoverable in the public domain, and the ease with which unsolicited emails can bypass spam filters by spoofing actual identities, evaluating incoming messages can prove a time-consuming task. The quantities of cybersecurity news available in public domains, plus the ability of targeted phishing attacks to elude anti-spam filters, means that malicious information can reach even the best-guarded inboxes.

We're likely to forget which newsletters we once subscribed to, and therefore fail to recognize the imposters. Clearly, infosecurity professionals who do not want to be cut off from useful channels of threat intelligence must apply procedures that enable them to determine trusted sources of information.

"I tend to think of infosecurity sector news as dots in concentric circles—the closer to the center, the more you trust what you read," says Yiannis Pavlosoglou, co-chair of the (ISC)² EMEA Advisory Board. "When you read something on Twitter, say, you typically place it in the outermost circle of trust and influence to you. With time, and if this news is real, it gets vetted by more sources you trust—it moves closer and closer to your inner trust circle. Always note, however, that 'trust' varies between individuals."

Such procedures don't necessarily have to involve bothersome vetting procedures, adds Pavlosoglou. Cross-referencing should factor in as many "golden sources" as possible, along with some "crowd-sourced" checks. "Cross-referencing sector news with multiple sources always helps. There are also a handful of 'golden sources' that you know and trust. For example, the golden source

RETURN TO CONTENTS

for vulnerability severity scoring is MITRE Corporation's Common Weakness Enumeration list. Using this, we can confirm the severity for publicly known cybersecurity vulnerabilities on its website."

Cross-referencing information with a CERT expert group and tracking back CVE (common vulnerabilities and exposures) numbers "is good practice," agrees Osirium's Harris. "One of the best approaches to be sure of 'trusted sources' is to get out of the office and go to cybersecurity exhibitions and conferences. It would, after all, take a significant effort for cybercriminals to pose as cybersecurity vendors at a trade show."

TECHNOLOGY AS A 'TRUST TOOL'

Security technology itself plays a big part in helping us ensure that sources of data are who they say they are, BeyondTrust's Chappell notes. "Techniques like DomainKeys Identified Mail, Sender Policy Framework and Domain-based Message Authentication, Reporting & Conformance can all come together to help us verify the source of an email—but that should never supplant the simple assessment of whether the email was expected, especially if it asks us to do something sensitive to ourselves or our organization."

Another approach is to look at how known disinformation campaigns are conducted, recommends Digital Shadows' Amado.

"Understand the tools and techniques attackers use and it becomes easier to spot disinformation," he suggests. "For instance, one common technique is the use of domain hijacking and 'typosquats' to spoof legitimate news sources. Recipients should look closely for obvious signs such as misspellings, odd top-level domains—would your 'trusted source' really use a .biz or .xyz domain suffix?"

Looking forward, it's likely that advanced technology from outside mainstream cybersecurity might be able to help identify and reveal fake news and disinformation. Output from monitoring tools, such as vulnerability management, access management and SIEM (security information and event management), could be augmented by principles of AI, and even blockchain technology, to be able to help online news aggregators enable readers to verify the sources of stories.

"Shared ledger technologies can, in principle, help verify news. As Bitcoin tracks financial transactions, published news articles would be tracked and verified in a shared ledger using principles of blockchain authentication," explains Pavlosoglou of (ISC)^2.

"To succeed, though, some financial incentive in the form of a transaction fee or similar would be required. That way, miners would be incentivized to check and improve the 'health' of the news network, adding or removing transactions on the reputation of published articles."

Meanwhile, some basic low-tech checks can continue to work well, reckons BeyondTrust's Chappell: "Check with the sender via a different medium. Pick up the phone, for example, to verify the trustworthiness of the message before you respond. This could slow you down a little—but it's nothing compared with the impact of a successful cyberattack." ■

JAMES HAYES *is a U.K.-based freelance editor and technology journalist.*

BEWARE THE SOCIAL MEDIA HEADHUNTER

WITH CYBERSECURITY PROFESSIONALS in high demand, it's not unusual to hear from job recruiters through email or social networks. Just know this is where cyberattackers lurk too, as Lisa Forte at Red Goat Cyber Security attests in this client story:

"I worked on a case that involved an IT security team leader. Let's call him 'Joe.' Joe was happy in his job but kept his options open for other opportunities. One day he received a LinkedIn message from 'Dave', the 'head of cybersecurity recruitment' at a major firm, who commented flatteringly on Joe's LinkedIn articles and added that he would love to have someone of Joe's caliber on his books.

"He asked how much Joe was earning in his current job, and promised he'd be able to add at least £15,000 to that salary if Joe was minded to make a move. Joe agreed for Dave to run his profile past prospective clients. Next comes this response: 'Joe, you've been with us five minutes and already I have three international companies keen to interview you. Some of the benefits will blow your mind. Please view each role (documents attached) and let me know which you would be up for. Two of them have a deadline this afternoon, so let me know ASAP.'

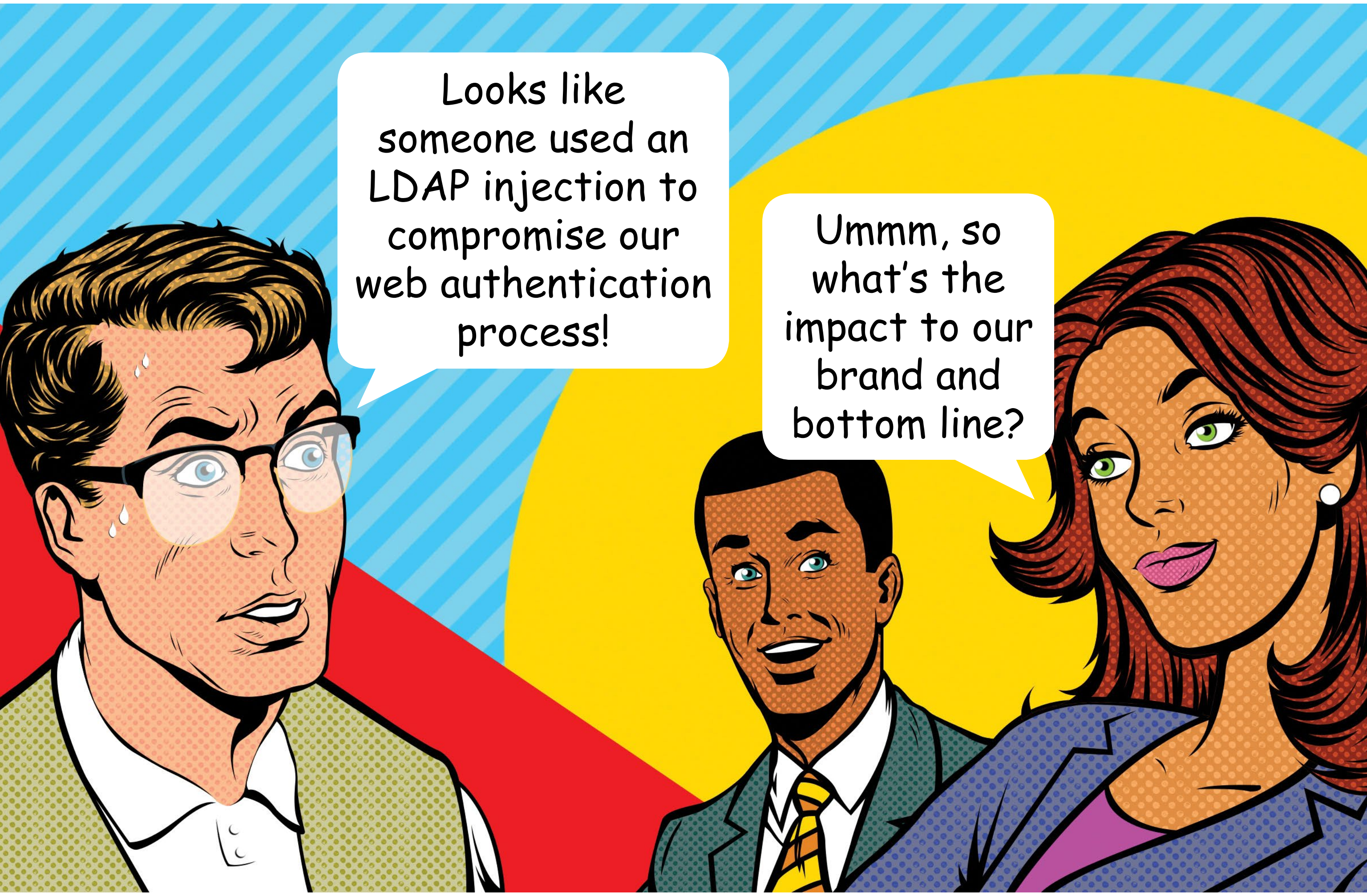
"Joe opens the attachments with eager anticipation—a mistake he was to regret for a long time: at least one attachment contained ransomware. Needless to say, 'Dave' was not a recruiter."

—J. Hayes

RETURN TO CONTENTS

WATCH YOUR LANGUAGE

How to effectively engage 'cyberignorants' to gain buy-in for your security wish list. **BY ADAM WOJNICKI**


Looks like someone used an LDAP injection to compromise our web authentication process!
Ummm, so what's the impact to our brand and bottom line?

JUST A FEW YEARS AGO I worked as an information security officer for a major multinational company. At that time information security had just started to be referred to as cybersecurity. Business executives were mainly concerned with Sarbanes-Oxley compliance, and few really believed in stories about hackers stealing valuable data or cybercriminals trying to ransom companies. Media here and there reported a blackout or nuclear facilities destruction attributed to a foreign intelligence hacking, but all that used to be considered an unlikely event for a normal company.

ILLUSTRATION BY TAYLOR CALLERY

RETURN TO CONTENTS

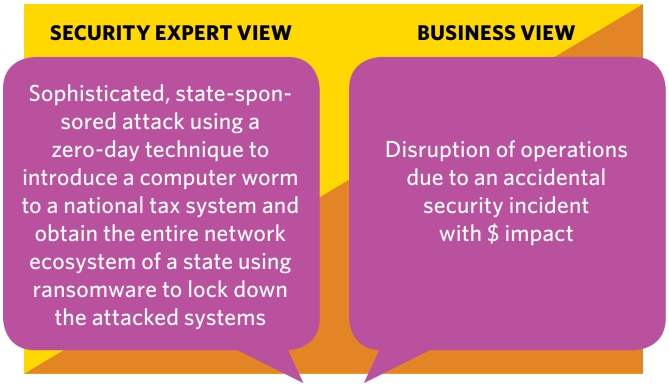
It's a different world now. Mobile and cloud technologies are everywhere. Any single company drives its digital strategy focused on valuation of data owned. Cyberattacks are so extensively covered by news media that cyber operations are now considered to be the No. 1 risk by organizations.[1, 2] This raises expectations on the business side.

Those years spent in a corporate management position helped me understand that we, IT security professionals, and businesspeople speak two different languages. At that time, I decided to enroll in an MBA program to literally learn how to "speak the business language," and it was useful. One key takeaway from those studies: If you wish to convince businesspeople to take action, you must use terms they understand. In other words, when presenting risks, emphasize how they impact both the brand and the bottom line.

Too often, cybersecurity professionals are more focused on speaking with precision when they need to speak with persuasion. To do that, it becomes critical to adopt a language easily understood by "cyberignorants." Why is it so important? Well, the business also is all about satisfying an unfulfilled demand. Therefore, the business leaders are keen to better understanding exposure to cyber risk in how it prevents finance improvements or opportunities.

In the profession, we tend to present a security issue as a risk, but as an IT security risk, not a business one. Cybersecurity is complex and we tend to further complicate it with security jargon.

Let's look at a real-life example:



SECURITY EXPERT VIEW

Sophisticated, state-sponsored attack using a zero-day technique to introduce a computer worm to a national tax system and obtain the entire network ecosystem of a state using ransomware to lock down the attacked systems

BUSINESS VIEW

Disruption of operations due to an accidental security incident with $ impact

The business view of the risk focuses more on the (business) impact side rather than on the threat vector. It is preferably expressed in a quantifiable way ($, €, £, etc.).

IN BUSINESS, IT'S ALL ABOUT THE MONEY

As media report extensively on incidents, executives now are aware of both risks and consequences. They learn this not from reading technical reports but consumer publications—they want to learn from what peer companies or competitors overcame after encountering major difficulties due to security attacks. These are truly business issues and not technical incidents that must be resolved.

When a major pharmaceutical company disrupts production and distribution of vaccines and must use federal stock instead, this denotes loss of revenue, penalties and impacts the bottom line (profits). The loss is counted in hundreds of millions and spreads over two years. This is a quantifiable business risk. To be noted, the chairman of the company was kindly invited to provide explanations in front of Congress. He is not likely to forget the event too quickly.

Too often, cybersecurity professionals are more focused on speaking with precision when they need to speak with persuasion.

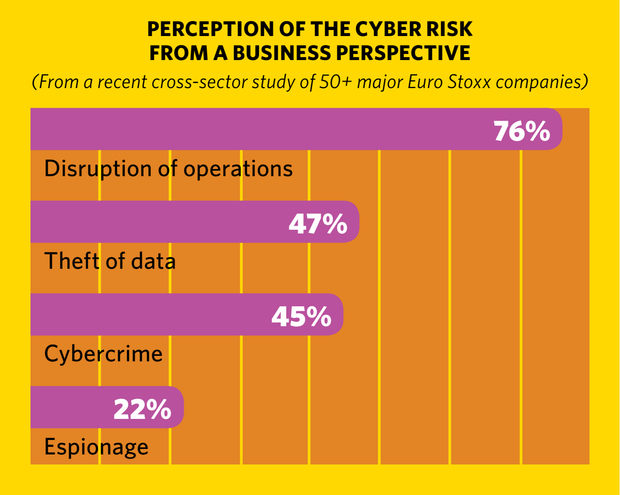
Another example: A shipping company servicing some major global ports lost all IT systems and had to operate "on paper" for a couple of weeks. Interestingly enough, this case is not only about lost revenue and profits. In this case, the company reported a 4 percent loss of share value. This is called value destruction (as opposed to value creation—an important business term). The EVA (economic value added) is what drives any listed public company. It represents what the investors get out of their investments.

Furthermore, while the company in question lost 4 percent of value equivalent to an evaporation of U.S. $1 billon, its competitors grew by 15 percent. In business, this is called lost opportunities. Looking at security from a business perspective, should we talk about a competitive advantage of companies properly managing their security postures?

And there are dozens of similar examples. All provide an opportunity for security professionals to use comparable illustrations to underscore the need to invest more in cybersecurity. Business leaders that see major companies failing will instinctively think: If this happened to these big companies, how safe are we? What if this happened to us? How would we survive?

A recent study of 50 major Euro Stoxx companies in the aftermath of 2017 attacks[3] shows that from a business perspective, the perception of the risk may be simpler than we tend to think *(see figure, next page)*.

The cyber risk anticipated by the business falls into two main categories: theft of data and disruption of operations.



Disruption of Operations

The first category preoccupies more than three-quarters of those surveyed. This is a clear echo of 2017 events that heavily impacted business operations of some major organizations.

Theft of Data

The second category concerns about half of all companies and relates to the recent switch from a traditional economy to the new economy of data. In this switch, data plays a key role and is now recognized as a valuable business asset.

Cybercrime and espionage

Cybercrime is also often mentioned as a risk and, in most of cases, falls into one or both of the previous categories. Industrial espionage is actually less common and only mentioned by about 20 percent, suggesting respondents either don't understand or don't care as much about insider threats.

This analysis also leads to another important conclusion about the business perception of the risk. Rather than describing detailed risk vectors in a complex manner, one could simply consider three categories: accidental, opportunistic and targeted. Cybercrime is an opportunistic risk; espionage is a targeted one. Simplicity helps the business understand this complex topic.

HOW TO COMMUNICATE WITH THE BUSINESS

Let's start with what the communication is about. Communication is a dialogue, meaning it goes both ways—in our case, from IT to the business and vice versa. In our communication to business units, we provide messaging that fulfills our own goals. But business also has its own expectations. Matching the two is where the communication becomes efficient—and more effective.

The theory of communication defines four key constituents of communication: emitter, receiver, language and content. Each of the emitters and receivers has their own worldview, or way of describing the surrounding world.

Effective communication requires the emitter to adapt the language to the audience (aka receiver) so the message is easy to understand. We can adapt the language to the business worldview by describing the risks in a new, simplified way, enriched with some business jargon (EBIT, EVA…) and possibly quantify it based on data and comparables. Let's focus on the content now.

People working on the business side like to measure everything. They measure impact of an investment (ROI), they measure progress in time and performance through key performance indicators (KPIs) and risk with KRIs… the list of metrics is long.

UNDERSTAND YOUR AUDIENCE

Let's look at marketing, as an example. What image immediately comes to mind? You probably envision campaigns on the scale of Apple, when the late Steve Jobs was its frontman. New products were released with much panache, leading many business students to want to follow in Jobs' footsteps as a marketer extraordinaire. But marketing in reality is rooted in metrics that measure campaign successes. There are entire books, several hundreds of pages long, describing dozens of marketing measurement KPIs *(see an example in Footnotes, no. 4)*.

> **What would businesspeople need, or at least want, to better understand the state of security at their company? Chances are the answer is metrics.**

But paradoxically, even though cybersecurity falls under the science of computing, it tends to be more qualitative than scientific. Our security dashboards, often based on a random collection of all available technical indicators, hardly reflect the exposure of the business to the cyber risk in a way that is consistent and understandable to the business.

But what should we measure then?

Let's think again about the receiver, especially if that person works in marketing. What would businesspeople need, or at least want, to better understand the state of security at their company? Chances are the answer is metrics. They want proof the systems are secure or that vulner-

RETURN TO CONTENTS

BUSINESS TERMS

GLOSSARY

EVA or value creation/ destruction	Economic value added is the value created in excess of the required return for the company's shareholders
Top line/revenues	Money received from the sale of products and services before expenses are taken out
Bottom line/EBIT	Earnings Before Income and Taxes; the result after all revenues and expenses have been accounted for
KPI	Key performance indicator evaluates the success of an organization or of a particular activity
KRI	Key risk indicator is a measure used in management to indicate how risky an activity is
ROI	Return on investment
Lost opportunities	"Cost" incurred by not enjoying the benefit associated with the alternative
Competitive advantage	The attribute that allows an organization to outperform its competitors

Source: Wikipedia

abilities have been patched. And they want it presented in a manner that mirrors their own dashboard reports.

This means measuring threat exposure through 3 KPIs: posture, dynamics and performance. The posture indicators measure how the business is exposed to anticipated risks at a point in time. The dynamics measure how this posture evolves in time and within different time ranges. Finally, the performance indicators should reflect the efficiency of controls as well as the operational and even economic performance of security efforts.

Knowing the expectations of the business, we can define a system of meaningful indicators and match them to existing information. With this approach we build multiple levels of data consolidation that help provide the right level of synthesis to the right level of audience.

"Keep it simple" should be the motto while talking to the business on security. It takes great skill to make the complex simple, but it's something top performers in any field learn to do well.

Remember the concerns of the business on risks and focus on what counts to the business: financial loss related to the disruption of operations or data theft. Express the business impact in terms of top and bottom line, talk about potential value destruction. Use recent examples to illustrate. Employ the language of risk, but from a business perspective.

Last but not least, make sure what you propose is measurable so performance can be tracked on a regular basis. This is truly where you, as a security professional, can prove an investment will pay off.

For too long, we in the information security industry by default have been too paranoid or too optimistic in how we present what we do and why it's vital to the organization. It's time we all join our business brethren on the other side of the aisle and become more transparent and measured. The future of the company may depend upon it.

ADAM WOJNICKI, *CISSP, is Director Innovation & Expertise at Harmonie Technologie, a leading risks and security consultancy in Paris.*

FOOTNOTES:

[1] https://www.agcs.allianz.com/insights/white-papers-and-case-studies/allianz-risk-barometer-2018/

[2] https://www.risk.net/risk-management/5424761/top-10-operational-risks-for-2018

[3] https://www.bearingpoint.com/fr-fr/notre-succes/publications/regulatory-intelligence-initiatives-1810/

[4] *Key marketing metrics* by Paul W. Bendle, Neil T. Pfeifer, Phillip E. Reibs Farris

RETURN TO CONTENTS

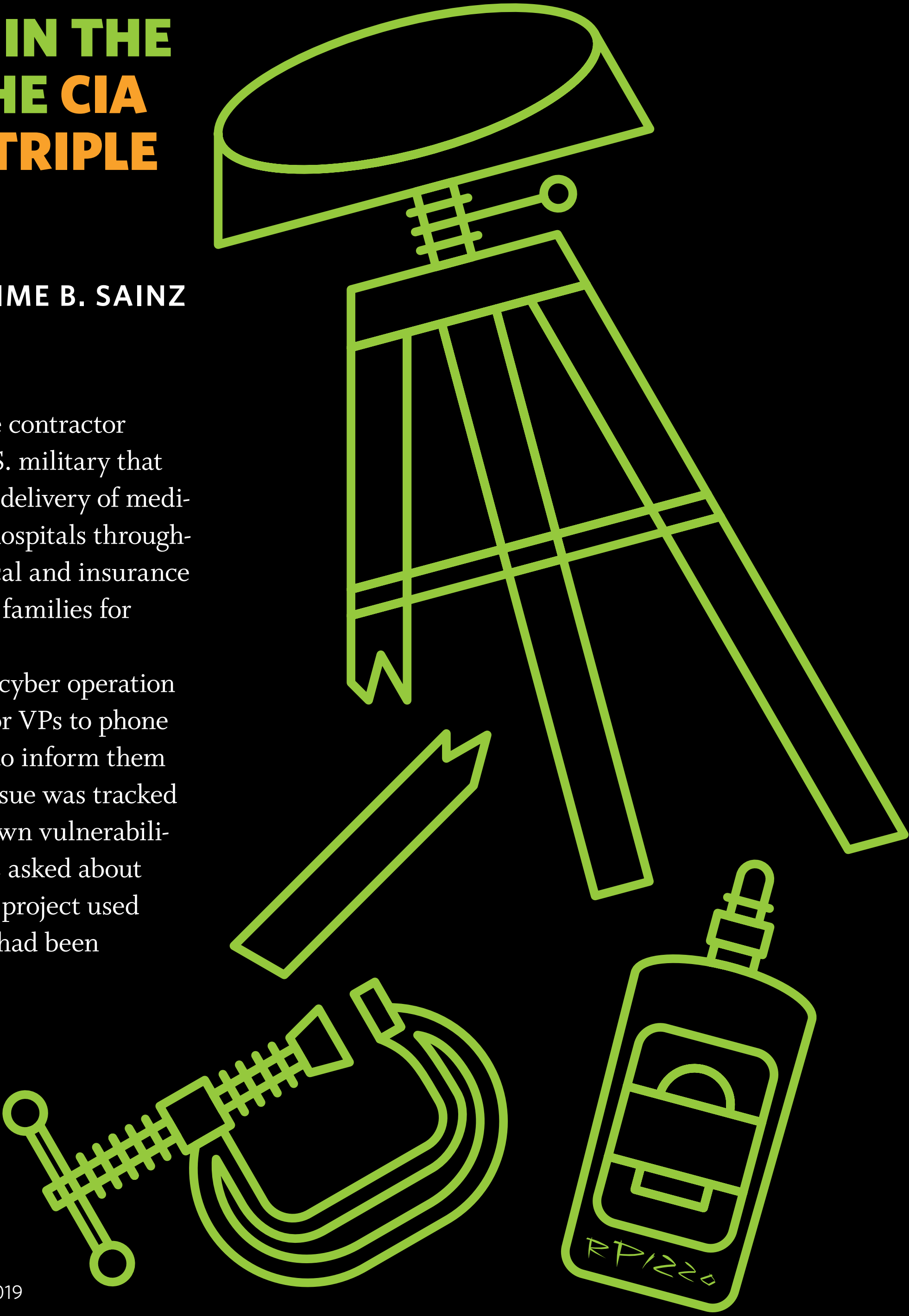
Cybersecurity's Project Management Impact

WORKING WITHIN THE JUNCTION OF THE CIA TRIAD AND PM TRIPLE CONSTRAINT

BY CHIP JARNAGIN AND JAIME B. SAINZ

SEVERAL YEARS AGO, a major defense contractor developed an application for the U.S. military that maintained the information for the delivery of medical services for American military hospitals throughout the world. It included the medical and insurance data for service personnel and their families for several branches of the military.

Unfortunately, a state-sponsored cyber operation hacked the system, prompting senior VPs to phone generals in the middle of the night to inform them that their data was breached. The issue was tracked back to a vendor's product with known vulnerabilities. When the project manager was asked about the vendor code, he denied that the project used the product. He didn't know that it had been incorporated into the application.



ILLUSTRATIONS BY ROBERT PIZZO

It turned out that in their frenzy to meet deadlines, the developers included the faulty piece of technology into the application, unaware of the cybersecurity ramifications. As cybersecurity had not been an integral consideration for the project, the vulnerable code was not discovered.

While this is an extreme example of what can happen when cybersecurity is not a priority for a firm's projects, not including it from the beginning of any project can cause major issues.

Doing so is more important than ever, yet integrating cybersecurity into project management from the start continues to be ignored. One way to improve the overall quality of a product or service being delivered, including reducing the risks of it being leveraged or targeted in a cyberattack, is to consider incorporating two fundamental models into one program: the project management Triple Constraint and the cybersecurity Confidentiality, Integrity and Availability (CIA) Triad.

THE CYBERSECURITY AND PROJECT MANAGEMENT INTERSECTION

Most fields of expertise maintain specific best practices or frameworks that enable their value delivery. Both cybersecurity and project management have well-proven concepts and standards through which their functions are performed. Within project management, one of the most basic concepts is the Triple Constraint *(see Fig. 1, below)*.

Figure 1:
The Project Management Triple Constraint

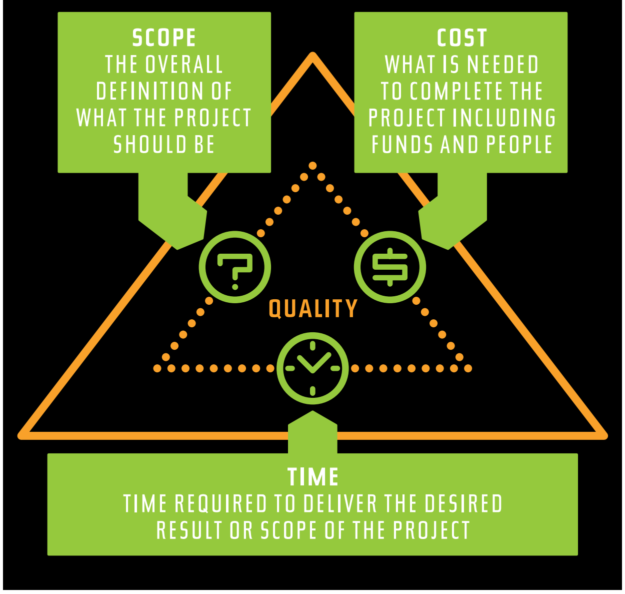
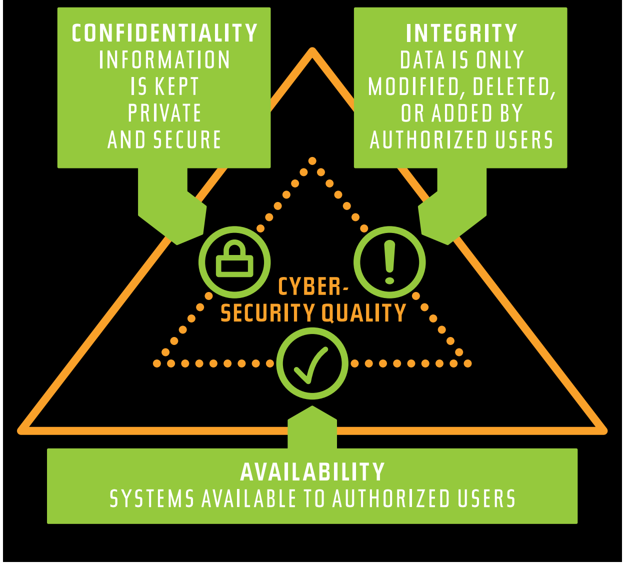

SCOPE
THE OVERALL DEFINITION OF WHAT THE PROJECT SHOULD BE
COST
WHAT IS NEEDED TO COMPLETE THE PROJECT INCLUDING FUNDS AND PEOPLE
QUALITY
TIME
TIME REQUIRED TO DELIVER THE DESIRED RESULT OR SCOPE OF THE PROJECT

Figure 2: **The CIA Triad**


CONFIDENTIALITY
INFORMATION IS KEPT PRIVATE AND SECURE
INTEGRITY
DATA IS ONLY MODIFIED, DELETED, OR ADDED BY AUTHORIZED USERS
CYBER-SECURITY QUALITY
AVAILABILITY
SYSTEMS AVAILABLE TO AUTHORIZED USERS

In cybersecurity, the CIA Triad is foundational.

A project that follows both the best practices of both disciplines is more likely to produce a quality result.

The project management Triple Constraint has three components: scope, time and cost, which are considered to be equal in importance. Quality is said to have been achieved by satisfying all three.

If one of the legs changes, the remaining legs of the triangle must be adjusted to maintain the quality of the project.

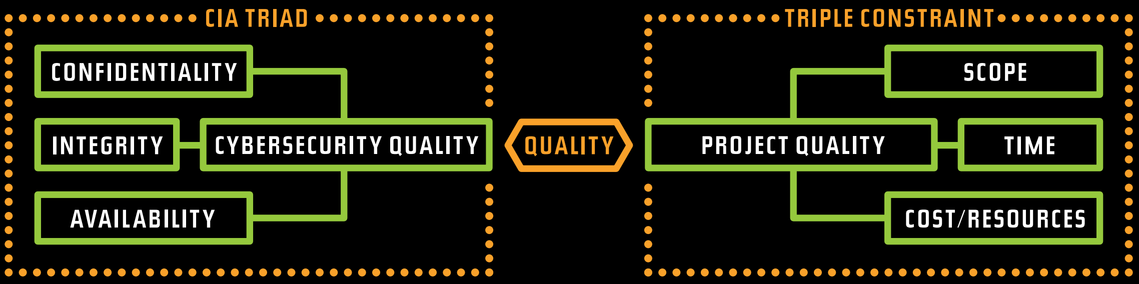
Each leg of the triangle is dependent on the others. If one of the legs changes, the remaining legs of the triangle must be adjusted to maintain the quality of the project. Although adjusting the other legs is not always possible, the Triple Constraint should always be considered when a change in the project scope, time or budget is introduced.

The CIA Triad's three key components are confidentiality, integrity and availability *(see Fig. 2, above)*. By implementing security controls that support all three factors, the data and services those controls protect will be secure.

Confidentiality ensures that the given resource is accessible to specifically authorized personnel. Security controls

RETURN TO CONTENTS

Figure 3:
The Intersection between the CIA Triad and Project Management Triple Constraint



such as encryption and identity and access management (IAM), along with the technologies and processes that enable them, are part of this section of the triangle.

Integrity ensures that the organization's data is unmodified by an unauthorized entity. Whether data is in motion or in storage, it must be kept in a state that is trustworthy. Among the controls that provide integrity are access controls (e.g., file permissions) and the use of cryptography.

Whether data is in motion or in storage, it must be kept in a state that is trustworthy.

Availability ensures that the given data or service is accessible to authorized individuals when needed. Numerous controls enable availability along with the network and infrastructure supporting them.

Both the CIA Triad and the Triple Constraint are focused on the quality of the end result: one is a secure environment and the other is a project delivered successfully. The key is to focus on the benefits of implementing best practices in both disciplines. Figure 3 *(above)* illustrates the relationship between the two concepts.

Placing cybersecurity phase gates throughout the project will improve the quality of the project deliverables.

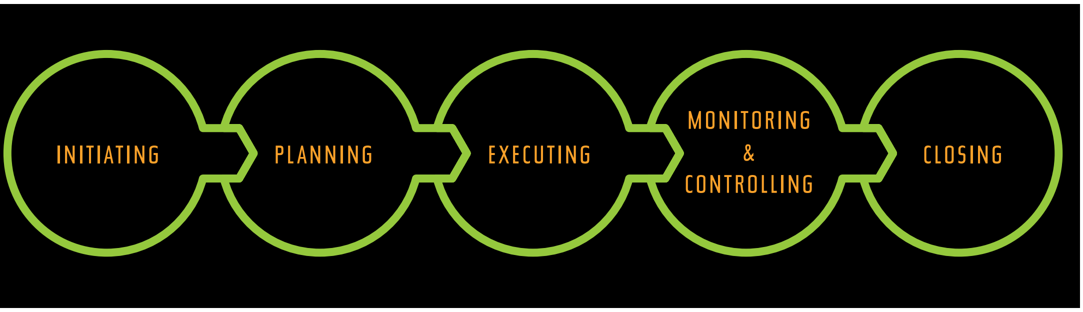
PROJECT RISK VS. CYBER RISK

Project management risk and cybersecurity risk have different characteristics.

The Project Management Institute's (PMI) Project Management Body of Knowledge (PMBOK) defines project risk as "[a]n uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives."[1] Under the Project Risk Management knowledge area, PMI defines six different processes that are necessary to control risks on a project. All of these processes are directed toward impact on a project itself and do not take cyber risk into account.

On the other hand, cyber risk is defined as "[t]he level of impact on organizational operations (including mission, functions, image or reputation), organizational assets or

Figure 4:
Project Stages



RETURN TO CONTENTS

individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring."[2]

Going forward in this article, any reference to risk is a reference to cyber risk.

CYBERSECURITY CONCERNS WITHIN THE FIVE PROJECT STAGES

PMI's PMBOK identifies five stages (process groups) every project goes through. In order, they are: initiating, planning, executing, monitoring and controlling, and closing.[3]

They are defined as follows:

Initiating: Includes activities through which the definition of a new project is developed and authorization is granted to begin.

Planning: Includes the activities defining the project scope. The objectives of the project are developed during these activities along with the development of the action plan and schedule to accomplish the project objectives.

Executing: Includes the completion of the activities identified in the project plan to meet all of the project requirements.

Monitoring and controlling: Includes all activities performed to ensure the project remains on track and encompasses the management of any changes to the plan, scope, schedule or budget.

Closing: Includes all activities required to officially complete and close the project or a given phase of the project.

The following is a list of general questions and actions to include cybersecurity in each of the five project stages. This is not an exhaustive list because some projects will have special requirements that need further investigation/assessment.

Initiating

- Can the project impact the security of the organization?
- Identify and document cybersecurity decision owners. Outside of IT, ask the business to identify who can make project-specific decisions regarding data access, data retention, data destruction, data classification, disaster recovery and business continuity planning.

Planning

- Plan the required levels of security for each data type based on its classification (e.g., public, confidential, restricted, company proprietary, etc.).
- Outline what data requires encryption during transmission, what data requires encryption at rest and what data requirements apply if the data is transmitted to a third party. Also determine what levels of encryption are required.
- Set the standards for compliance, including considerations for PCI, GDPR, PII, HIPAA, etc.
- Validate (and document if necessary) with the IT team their responsibilities for providing the hardware, operating systems, software patching, maintenance and systems support.
- Plan and document any disaster recovery and business continuity plans that need to be implemented.
- Develop a detailed document regarding the standards and procedures for access control (including physical security), logging and monitoring, privileged access management and compliance guidelines for backup data retention and any other relevant processes.
- Include the implementation of data loss prevention (DLP) software if it can be funded because it adds real-time, preventative control for keeping data secure.
- Create a cyber risk management plan for the project deliverables.

Executing

Ensure compliance with all standard cybersecurity processes and documentation identified above.

Monitoring and Controlling

- Confirm that all ongoing cybersecurity processing and controls are maintained through regularly scheduled reviews.
- Ensure that all preventative and corrective actions are taking place.

Closing

Remediate any remaining cybersecurity concerns.

Under some limited circumstances, during the initiating stage, it may be determined that the project has no impact to the firm's data security, IAM, network connectivity or physical security. If that is truly the case, then the rest of the assessments are not needed. However, a project team must be very careful in reaching this conclusion.

CYBERSECURITY AS A CONCERN FOR ALL OF A COMPANY'S PROJECTS

Consider the example of the threat of a direct kill chain to valuable IT corporate assets posed by IoT (Internet of Things) devices now being installed for building automation.[4] Currently, IoT cybersecurity is an oxymoron. In most

RETURN TO CONTENTS

All independent PMOs should be integrated with the firm's overall PMO to ensure that cybersecurity concerns are standardized for all projects.

firms, those building projects are outside of the purview of the cybersecurity organization, creating vulnerabilities that can be hacked.

For example, in what has to be one of the greatest "fishing" attacks ever (https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4), hackers breached the automated thermostat of a casino lobby aquarium and exfiltrated the casino's high-roller database.[5] According to a 2017 study involving more than 3,000 companies, 84 percent had experienced some type of IoT breach.[6]

Because the cybersecurity attack surface has become so broad and pervasive, a company's Project Management Office (PMO) must make the risk assessments described above a requirement for all the firm's projects. It has become an imperative that cybersecurity operations have insight into all of the firm's projects, including those outside of traditional IT, to assess whether they impact the cybersecurity stance of the organization and, if so, determine what mitigation/controls are needed.

Also, in some companies there are multiple PMOs. This is very much like having shadow IT. All independent PMOs should be integrated with the firm's overall PMO to ensure that cybersecurity concerns are standardized for all projects.

In fact, a logical argument can be made for a company's PMO to reside within the cybersecurity organization. This would help ensure that cybersecurity oversight is incorporated in all of a firm's projects.

CONCLUSION

No company wants to experience a breach like the one recounted at the beginning of this article. By incorporating cybersecurity safeguards into every stage of a project, vulnerabilities that previously would not have been considered nor discovered can be mitigated.

In summary:

- Cybersecurity should be taken into account for all of a firm's projects.
- The company-wide PMO should adopt the recommendations detailed in the above list of what cybersecurity assessments should be done in each of the five project stages.
- A firm should only have one PMO to ensure that cybersecurity concerns are standardized across all of the organization's projects.
- All of a firm's projects should be run by the company-wide PMO starting with the Initiating stage of the projects to ensure that all cybersecurity vulnerabilities are recognized and mitigated.

Shutting down the threats of a direct kill chain to valuable corporate assets posed by a firm's projects can be accomplished by following the recommendations in this article. ■

CHIP JARNAGIN, *MBA, CISSP, PMP, CSM, Lean Six Sigma Green Belt, is a consultant at LatticeWorks Consulting. He has more than 20 years of experience in cybersecurity, telecommunications and IT. He is published in the fields of cybersecurity, organizational cultural, project management and IT governance/management.*

JAIME B. SAINZ, *MBA, CISSP, CISM, PMP, is a security strategist at a Fortune 100 company. He has more than 20 years of experience in IT, cybersecurity and project, program and portfolio management. He is also an adjunct professor of cybersecurity at William Jessup University.*

FOOTNOTES:

[1] Project Management Institute; Project Management Book of Knowledge, p. 720; Project Management Institute, Inc., 2017; Newtown Square, Pa.

[2] NIST; "FIPS Pub 200: Minimum Security Requirements for Federal Information and Information Systems," p. 8, NIST, March 2006, https://csrc.nist.gov/csrc/media/publications/fips/200/final/documents/fips-200-final-march.pdf

[3] Project Management Institute; op.cit., p. 554

[4] For more information on how IoT is expanding firms' attack surface, see "'Building' a case for stronger IoT-related cybersecurity," the feature article in the February 2019 (ISC)^2 enewsletter *Insights*, https://www.isc2.org/News-and-Events/Infosecurity-Professional-Insights

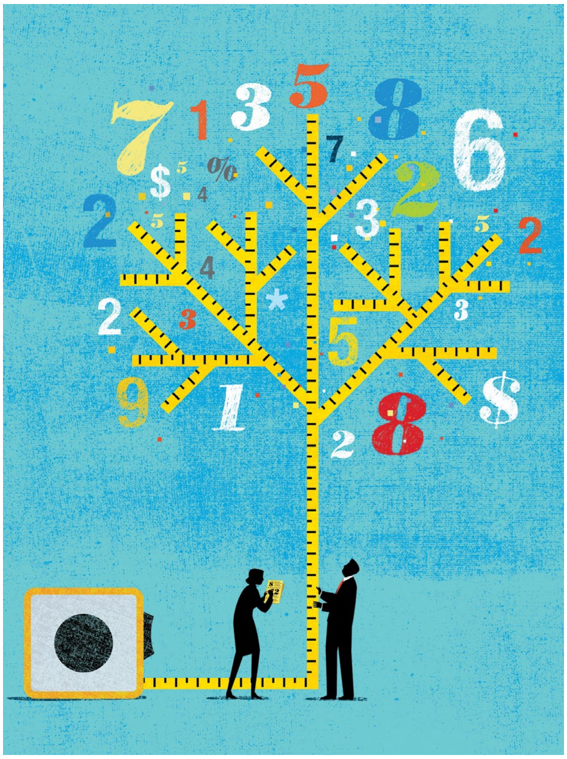
[5] Williams-Grut, O.; "Hackers Once Stole A Casino's High-Roller Database Through A Thermometer In The Lobby Fish Tank," Business Insider, April 15, 2018, https://www.businessinsider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4

[6] Colley, A; "More Than 80 Per Cent of Companies Hit with IoT Breaches: Study," CSO, March 1, 2017, https://www.cso.com.au/article/615124/more-than-80-per-cent-companies-hit-iot-breaches-study/

RETURN TO CONTENTS

It's All in the Numbers

by Pat Craven



CYBERSECURITY IS ALL ABOUT NUMBERS—a bushel basket full of ones and zeros. Well, have I got some numbers for you this month—numbers that equal lives changed, and potentially saved, from the terror of being bullied online or having personal information stolen, leaving lives in ruins. Every cyber safety lesson that you help us deliver through our Safe and Secure Online and Garfield's Cyber Safety Adventures program is another life changed forever.

Check out these numbers for 2018:

- 623 Middle School Presentations downloaded, reaching **23,676** children ages 11 to 14.
- 685 Parents Presentations delivered, teaching **18,215** adults how to help protect their families online.
- 523 Senior Presentations given, making **10,255** senior citizens safer from fraud and online scams that could wipe out their entire retirement savings.
- 1,051 Award-Winning Garfield Educator Kits distributed around the world, delivering **31,530** critical cyber safety lessons to children 6 to 11 years old.
- Another **7,587** Garfield digital lessons delivered online.
- 467 of the free Garfield PowerPoint presentations downloaded, delivering another **14,010** safety lessons.

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

My friends, that's **105,273** cyber safety lessons delivered in one year!

Combine that with the 65,000 lessons delivered last year, and that means we have provided nearly as many safety lessons to parents, seniors and children these past two years than we delivered in the last 10 years combined.

And that is just what we can measure. These numbers don't include the literally millions of people who received tips on how to be safe and secure online from our television appearances, radio interviews, podcasts, blogs, social media posts, seminars and magazine articles or from the 140,000 unique visitors to our websites this year—(www.IAmCyberSafe.org)—which are loaded with safety tips for the entire family in multiple languages, with more being added all the time.

As you read this, hundreds of volunteers are in the process of translating our materials into more than 30 languages.

To say we are on a roll making the world a safer cyber place for everyone would be an understatement, but the credit goes to all who volunteer and support the Center for Cyber Safety and Education in ways big and small. Simple things like following us on social media or making a presentation at a local school or even within your own company to fellow employees and parents. Want to be a part of this fast-growing give back program? Check out our new Garfield S.A.F.E. program (https://iamcybersafe.org/corporate-responsibility/) for ideas on how you and your company can get involved, anywhere in the world.

This year is already off to a record-breaking start, so please join us in our effort to make it a safer cyber world for everyone by volunteering or donating to the effort. We can only make this work with your support. ■

Illustration: Theispot/Michael Austin

RETURN TO CONTENTS

(ISC)²® community SHARING INSIGHTS FROM BUZZWORTHY THREADS

Join at https://community.isc2.org

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.

Editor's Note: Usually, at least two topics are posted on this page. However, the question below elicited a tremendous and varied response, which is sampled here.

QUESTION:

Chipping pets has been around for years. Chipping people has too, but not nearly so widespread. *The Guardian* has reported that the idea of chipping employees is being discussed by employers and unions are expressing concern. (See "Alarm over talks to implant U.K. employees with microchips — Trades Union Congress concerned over tech being used to control and micromanage" at https://bit.ly/2B168Sx).

Having chips in all employees and readers placed around the facility … could greatly benefit physical security and insider threat protection. Of course, that same system could become an amazingly intrusive invasion of privacy.

Would you recommend a chip program as part of the security program at a company you were advising? Alternatively, if your employer set up a voluntary chip program, would you get a chip?

Or, if your employer announced a mandatory program, would you quit?

—Submitted by CraginS

SELECTED REPLIES:

Personally, I would be happy to be chipped if it meant not having to carry door entry cards and smart cards for system access. I would also consider this for home locks. However, I could see this being a major challenge to try and implement this in our organization, an NHS site.

—Posted by chinoblue

I wouldn't volunteer to have a chip implanted in me, and if the organization mandates it, I'll want to resign. . . .

—Posted by Shannon

I guess you have to ask the Swedes their opinion; they are embracing it wholeheartedly: https://theconversation.com/thousands-of-swedes-are-inserting-microchips-into-themselves-heres-why-9…. They see the advantages, benefits—in an interview on New Zealand Radio, one of the advantages quoted was reducing the chance that the employee forgot their security pass!

—Posted by Caute_cautim

I don't understand why there is a need to implant tech inside the human body for identification purposes when we are carrying around our identifiers every day, all day long. Our thumbprints, our faces. For a contactless identification, a camera can do. You can recognize a person from his face, his walking.

—Posted by Micael

I don't see a way for such a ridiculous policy to become mandatory unless people became someone else's property, a practice stamped out hundreds of years ago. Ultimately what is the purpose? To subjugate the employee (I'll keep the ID badge, thanks).

—Posted by Kempy

While I am against the premise for privacy reasons, there is an advantage to bio-chipping.

You cannot lose a chip. It is less expensive and can be combined for two- or three-factor authentication to increase security access. If the chip is inserted in the hand, a special glove can mask the chip for privacy.

—Posted by bucknerj

Employers should mind their business and stay out of their employees' bodies…. The technology may be OK and very attractive but it crosses a fine line of responsibility. If chip technology is implemented, I need the option to opt-out. It gives the business too much control over my life!

—Posted by wpatterson2

I can see the amazing benefits of a microchipping program. I [hear] a lot of rhetoric around invasion of privacy but, to be fair, I'm not as concerned as others. Right now, we carry smartphones, tablets, laptops and other forms of tech provided by our employers that can be used to track our activities and movements. Swipe tags, anyone?

—Posted by SOC_Puppet

IAM is my passion. I've matured with IAM for 25+ years as it has matured… I have never thought embedded tech was the way to go…. I like the Yubi key. It's small, highly compatible with OpenID and has PIV integrated with it. I think this device would reduce many security issues and not impact the privacy of the individual.

—Posted by Flyslinger2

Find this thread at https://bit.ly/2G0y0J7.

RETURN TO CONTENTS

(ISC)²
SECURE SUMMIT / APAC

In partnership with
image engine

ENRICH **ENABLE** **EXCEL**

Registration Now Open

10-11 JULY 2019 • CONRAD HONG KONG

2 Days • 6 Tracks • 35+ Sessions • 40+ Speakers

(ISC)² Secure Summit APAC 2019 is the perfect opportunity for you to gain insight from great minds in the cybersecurity industry and participate in Enriching sessions, panels and best practice sharing designed to sharpen your skills and hone your craft. Meet over 400 peers from all levels and across a range of industries and immerse yourself in discussions that will Enable you to better secure your organization and Excel as a cybersecurity professional.

REGISTER TODAY

Don't miss this must-attend event!
Have questions? Talk to us!

Sponsorship - Michaella Park (mpark@isc2.org)
Registration - Helena Cortes (hcortes@isc2.org)

Enjoy member discount
& earn up to

24 CPEs

WHAT'S YOUR NEXT CAREER MOVE?

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

GET CERTIFIED.

Join (ISC)² on stand A180 at Infosecurity Europe
4 - 6 June 2019 Olympia London

(ISC)² Member Reception on 5 June

(ISC)² members can claim CPEs for attending workshops or educational talks taking place at Infosecurity Europe.

CPEs cannot be claimed for only visiting the expo floor.
Please refer to the CPE guidelines for information on how to submit.

(ISC)²®

www.isc2.org