THE NEWEST WAY TO BOOST YOUR CAREER ACUMEN

InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

MAY/JUNE 2019

TIME TO Smarten Up

Advancing consumer AI technology while upholding the CIA tenets

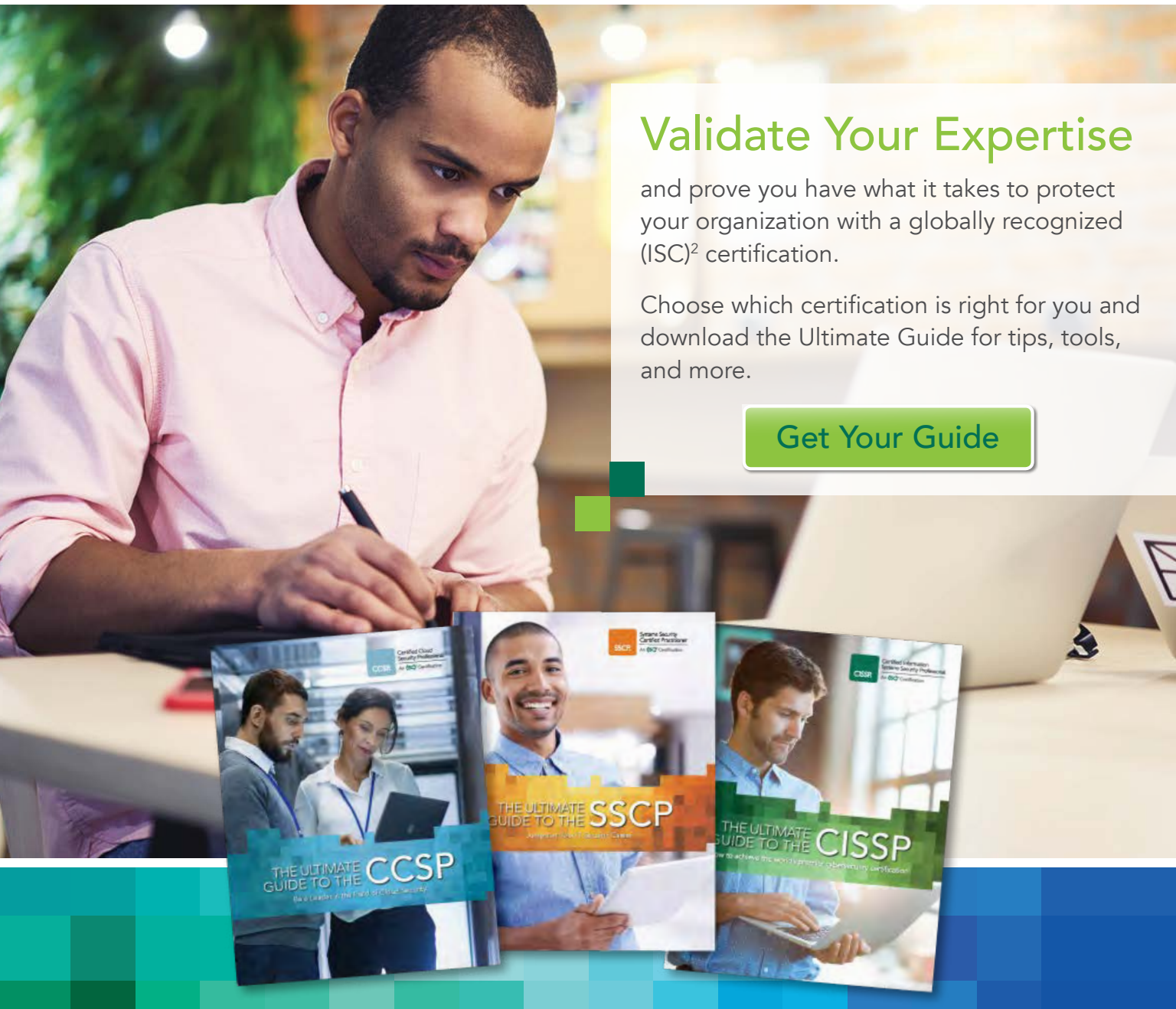
PRIVACY

The race to protect consumer data marches on

LESSONS LEARNED

A member's takeaways from securing a move to microservices

The Ultimate Guide to Your (ISC)² Certification



Validate Your Expertise

and prove you have what it takes to protect your organization with a globally recognized (ISC)² certification.

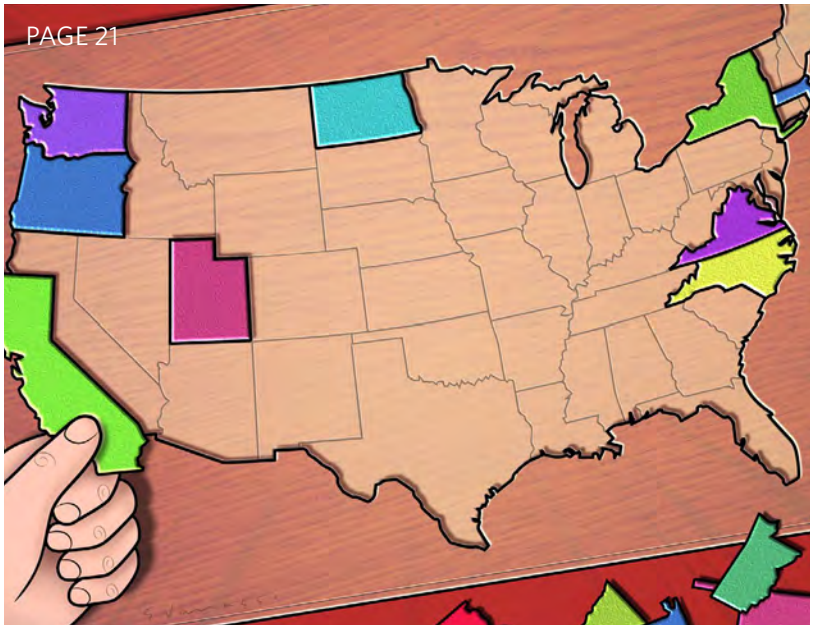
Choose which certification is right for you and download the Ultimate Guide for tips, tools, and more.

Get Your Guide

CISSP® SSCP® CCSP® CAP® CSSLP® HCISPP®

contents

VOLUME 12 • ISSUE 3



features

PRIVACY

17 **Time to Smarten Up**
Our AI devices may be giving away too much information. What should we do? **BY ANITA J. BATEMAN, CISSP**

GRC

21 **CCPA vs. GDPR**
An overview of growing pro-privacy legislation in California and across the U.S. **BY JENNIFER J. SOSA, ESQ.**

TECHNOLOGY

24 **10 Lessons Learned Securing a Microservice Ecosystem**
How cybersecurity can impact project management.
BY EMIL P. MAN, CISSP, CCSP

departments

5 EDITOR'S NOTE
What This Magazine Is ... and Isn't
BY ANNE SAITA

7 EXECUTIVE LETTER
Answering the Call for Professional Development
BY MIRTHA COLLIN

9 FIELD NOTES
New opportunities to advance your career; securing mobile devices; tips before diving into machine learning; recommended reading and more.

14 #NEXTCHAPTER
(ISC)² Melbourne Chapter

29 CENTER POINTS
Speaking the Universal Language of Cyber Safety
BY PAT CRAVEN

30 COMMUNITY
Right to be Forgotten impacts backups; advice on a career switch to cybersecurity.

5 AD INDEX

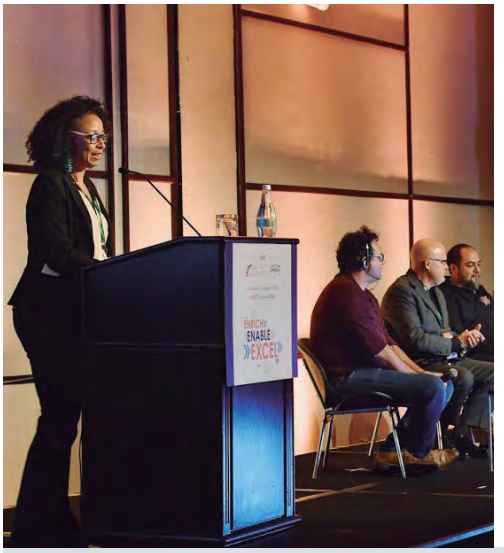
Cover image: JOHN KUCZALA
Illustration above: ENRICO VARRASSO

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

(ISC)²

SECURE SUMMIT / LATAM

ENRICH ENABLE EXCEL



ENGAGE WITH LATIN AMERICA'S BEST

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

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

(ISC)² members can earn up to 16 CPEs

REGISTER NOW latamsummits.isc2.org

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

What This Magazine Is ... and Isn't

EVERY TIME an issue of the magazine is published, readers email me to let me know what they like or what they find lacking. I love hearing from people, even those delivering constructive criticism. Others prefer to speak through online forums or social media posts. Based on some recent comments, I want to explain why we produce this publication.

This is an association magazine. Not a consumer publication, like *Wired*, nor a trade publication like *SC Magazine*. This periodical delivers a mixture of (ISC)² news and independently written and edited features focused primarily on professional development for cybersecurity professionals. Some of the material may seem repetitious if you regularly follow (ISC)² social media. However, not everyone does; nor do they opt in for (ISC)² emails. The magazine provides another channel for (ISC)² leadership to communicate with its growing global membership.

Our content is heavy on management because most members aspire to greater influence as they reach a new rung on their career ladder. We cover perennial threats and defenses too, like other magazines. Our magazine, however, features member-authors writing from their distinct vantage points. This, along with the outstanding work from our Creative team, helps *InfoSecurity Professional* look and read a bit differently from other publications.

Then there's the quiz to earn education credits. Some questions are easier than others by design. All are to ensure you understand and maybe learn something to help you better serve your organizations and communities.

We're all tested now and then—you, me, and this magazine that relies on members to make it better. It's my hope that when there's a crisis, or a career is on the line, something you once read here will help you navigate those rough waters, because you belong to an organization devoted to helping you do just that. ■

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

ADVERTISER INDEX

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

(ISC)² Certifications 2
(ISC)² Secure Summit LATAM 4
(ISC)² Secure Summit APAC 6
EMEA InfoSec Europe 8
Duo Security 11
(ISC)² Secure Summit Denver 13
(ISC)² Security Congress 16
Egress 27
Cofense 28

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.

(ISC)²

SECURE SUMMIT / APAC

ENRICH ENABLE EXCEL

In partnership with: image engine

REGISTRATION NOW OPEN

10–11 July 2019 | Conrad Hong Kong

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

Secure Summit APAC 2019 is the perfect opportunity for you to gain insights from great minds in the cybersecurity industry. Participate in Enriching sessions, panels and best practice sharing, designed to sharpen your skills and hone your craft. Meet over 400 InfoSec professionals from the region 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.

Tracks include:

- Identity Access Management
- Cutting Edge Technologies and Ideas
- IoT/OT Security
- Professional Development
- Security Operations
- Governance, Risk and Compliance

Industry networking reception is open to all conference attendees

#ISC2Summits

25%
discount available for (ISC)² members

REGISTER TODAY

securesummitapac.isc2.org

For sponsorship and registration enquiries, please contact ***isc2asia@isc2.org***

Answering the Call for Professional Development

by Mirtha Collin

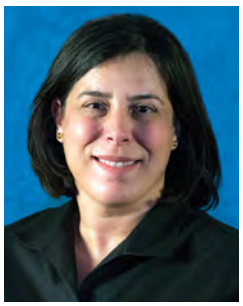
(ISC)² HAS ALWAYS stood for the advancement of the cybersecurity profession. For the past 30 years, that commitment has taken the form of training and education that helps members achieve certification.

While that's just as true today, in our constantly changing industry, (ISC)² also saw the need to evolve to support the continued professional growth of our global members as they work to acquire new skills. After several years of work and input from many of our member experts, we recently announced the launch of the (ISC)² Professional Development Institute (PDI).

PDI is a go-to resource for timely and relevant continuing educational opportunities to keep members' skills sharp and curiosity piqued. It recognizes that cybersecurity learning is a journey, and certification is just one step along that path. These courses are available to members at no cost, but in order to improve the educational opportunities available to our entire industry, non-members can also purchase access.

By the end of June, nine immersive courses will be available, including new offerings covering such topics as leadership, cloud security and IoT. In fact, there are plans for as many as 30 new courses this year alone.

Staying at the top of your game as a cybersecurity professional is an ongoing challenge. Doing so while meeting the demands of a high-pressure, high-stakes security position, working long hours and then balancing responsibilities to family in your personal life can be tough. Our hope is that by offering these courses online and on-demand we can at least ease the burden of accessing useful learning tools that are relevant to our profession and built with career growth in mind.



Mirtha Collin is the education director at (ISC)². She can be reached at mcollin@isc2.org.

Our amazing community of members continues to provide feedback to us, so that our PDI courses can grow accordingly. We will refresh the catalog of courses we provide based on ongoing dialogue with and input from our membership.

PDI is a go-to resource for timely and relevant continuing educational opportunities to keep members' skills sharp and curiosity piqued.

We've made it simple for members to get started by preloading PDI courses to our learning center, so all they need to do is log in to their account and see what's available. New courses will be added as soon as they are ready, so make sure to check back often.

We know that the hard work of cybersecurity professionals is at the heart of what helps keep data secure and people safe. We hope that PDI will help keep their cybersecurity abilities at their sharpest.

For more information on the Professional Development Institute and to access online courses, please visit www.isc2.org/development. ■

Photo: iStock

WHAT'S YOUR NEXT CAREER MOVE?

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

The (ISC)² Professional Development Institute is Growing

Even more opportunities for members to expand their skills

IN RESPONSE to the growing demand from members, (ISC)² earlier this year established its Professional Development Institute. The Institute offers a variety of free online development courses to members and associates, which are also available for purchase by non-members.

A successful pilot launch in 2018 offered three development courses: GDPR for Security Professionals; DevSecOps; and Building a Strong Culture of Security.

"The Professional Development Institute is a recognition that cybersecurity education is a lifelong journey, and that achieving professional certification, while important, is only one stop along the way," says (ISC)² CEO David Shearer, CISSP. "These new CPE opportunities are enriching and rewarding and provide valuable, topical insights that will help our members continue to grow and progress."

Mirtha Collin, education director for (ISC)², leads the Professional Development Institute, including a growing team that will manage content development, curriculum building, quality control, communications, logistics and administration. In this edition's Executive Letter, she describes PDI as "a go-to resource for timely and relevant continuing educational opportunities to keep members' skills sharp and curiosity piqued."

> **"These new CPE opportunities are enriching and rewarding and provide valuable, topical insights that will help our members continue to grow and progress."**
>
> *—David Shearer, CISSP, CEO, (ISC)²*

The program is expected to grow quickly. By mid-2019, there will be nine courses available covering topics including leadership, cloud security and IoT. By the end of this year, Collin estimates that there will be as many as 30 new courses offered. Her team will be looking for feedback from members as well, she explains. "We will refresh the catalog of courses we provide based on ongoing dialogue with and input from our membership."

Inquiries related specifically to PDI, including topic ideas, can be directed to pdi@isc2.org. For more information and to access online courses, please visit www.isc2.org/development. ■

RISING RISKS

1 IN 10
URLs are malicious

UP 33%
Mobile ransomware attacks in 2018

48%
Of malicious email attachments are Office files, up from 5% in 2017

Source: *2019 Symantec Internet Security Threat Report* https://www.symantec.com/security-center/threat-report

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=10814

Time to Focus on Mobile Security

We may have improved information security in the office but are we secure on the road?

Mobile devices are often able to access the most crucial company data, but does that mobility put our data at greater risk? Despite drums sounding on mobile security for years, Verizon's *Mobile Security Index 2019* shows that mobile devices continue to be ignored or dismissed when it comes to security protections.

Verizon surveyed 700 professionals involved in buying, managing and securing mobile devices for their organizations. Some 67 percent acknowledged they were less confident about the security of mobile devices than other devices. Not surprising, then, that more companies admitted they'd suffered a compromise that involved a mobile device—33 percent in the 2019 survey compared to 27 percent in 2018.

The vast majority, 83 percent of survey respondents, though, say the risk from mobile threats remains high, and a similar number (85 percent) say they need to take mobile device security more seriously.

When companies were asked what they're doing to improve mobile security, more than two-thirds—69 percent—said they would be spending more next year on mobile protections. At the same time, 77 percent thought that the biggest barrier to protecting data on mobile devices was a lack of user awareness.

Be it money or education, the directive is clear, according to Thomas T.J. Fox, SVP, Wireless Business Group at Verizon: "It's time to close the chasm between levels of protection."

To read the survey in full, go to https://enterprise.verizon.com/resources/reports/mobile-security-index/#report.

Look, Don't Leap: What to Know Before Diving into Machine Learning

Excerpted from the April (ISC)² Insights e-newsletter

Paulo Shakarian

IDC ANTICIPATES a $57.6 billion worldwide investment in cognitive and artificial intelligence (AI) by 2021, which means there's a good chance your company is considering, if not already buying or building, AI and machine learning (ML) solutions for both business processes and security operations.

Paulo Shakarian, CEO and co-founder of CYR3CON, which uses AI to predict cyberattacks, offers some words of advice—and a few warnings—to make sure AI and ML implementations and ongoing usages work as intended and do not lead to data leakage and other potential cybersecurity threats.

Beware of the hype.

Do your homework before you spend a dime (or thousands of dimes), cautions Shakarian. "The hype is mainly coming from vendors. … The CISOs then feel pressure from the executive suite."

What to do before you buy.

Shakarian recommends doing adequate due diligence before an AI/ML purchase.

Engage the board.

"Board members often come across innovations. It's up to the CISO," Shakarian says, "to coach board members on the pros and cons."

Know your business needs.

Not every solution requires AI, Shakarian counsels. "If you're looking to predict something; if you're looking to find something that is abnormal and that would normally require human interaction; if you're looking to optimize the decision-making process in an automated way—I see those as the holy trinity of AI, probably 90 percent of what you need AI and machine learning for."

Challenge the vendor.

When listening to a pitch from a vendor, Shakarian advises information security professionals get answers in some crucial areas.

Peer review.

The first question to ask, Shakarian says, is whether the underlying technology in the product has undergone peer review. "If it's not, that should be a big alarm bell if they're vetting their own stuff."

Relevant data.

Does the data fed to algorithms make sense? Shakarian posed that question in a blog post on this subject. "Regardless of how fancy an algorithm or piece of software is, it's making the prediction based on some piece of data—and you should ask the vendor what that is and ask him or her why it makes sense."

Data security and reliability.

Unless your company is large enough to afford a data scientist or data science department, you're going to outsource to an AI/ML provider. This raises the scrutiny required to ensure these providers keep your data safe and available at all times.

"Transparent" algorithms.

In order to monitor accuracy, you need transparency, Shakarian warns. If the algorithm is a "black box, you can't tell the difference between failure and your normal error rate. Whereas, if there's some level of transparency of how it's producing the results, the user can check up on it."

Updates to the machine learning model.

"…expect that the model is being updated on a regular basis by the vendors. If it's not, that, I think, is a major red flag because there's a high chance that the product might not work as advertised."

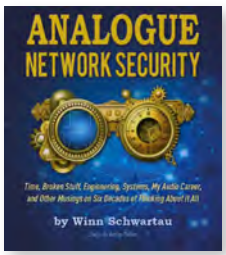
Before succumbing to the siren song of machine learning as the business solution, Shakarian believes you should ask if such a solution is needed at all. "Does the business need/require AI or machine learning to address it in an impactful, sustainable way?" If the answer is yes, then you have a roadmap here to follow. ■

RECOMMENDED READING

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

Analogue Network Security: Time, Broken Stuff, Engineering, Systems, My Audio Career, and Other Musings on Six Decades of Thinking About It All

By Winn Schwartau
(SchwartauHaus, 2018)



CYBERSECURITY VETERAN Winn Schwartau asks us to rethink how we approach security. Rather than focusing on the standby clichés like "A user cannot be 100 percent hacker proof," and "Vendors don't guarantee their products," or "Firms can't measure the effectiveness of the security they already have in place," he suggests a more active approach. In *Analogue Network Security*, Schwartau advocates faster detection time, and faster response time with highly automated policy-driven planning.

Schwartau's analog review relies on a time-based, out-of-band review of authentication. DDoS can be mitigated, he maintains, with graceful degradation. He provides a survey form to help the security professional track designed times and designated times. Implementing redundant mirroring, reaction matrix command and control servers and real-time information sharing can provide several answers for security professionals to consider. Same goes for machine learning and probability models created by vendors and firms that can help analyze their threats and risk and actions that are considered.

Schwartau acknowledges that we are not perfect and we can't be right in all circumstances, but we must try to measure with a level of precision and granularity. He doesn't advise the best security tools for specific circumstances but, rather, tackles the current issues with a more holistic approach.

Winn Schwartau has been honored as a "Power Thinker" and one of the 50 most powerful people in networking by the online resource *Network World*. He was voted one of the 25 most influential people in the security industry by *Security Magazine*. Schwartau is the founder and president of the Security Awareness Company (formerly Interpact, Inc.) and is the chairman of the board of security and compliance company Mobile Active Defense.

Security professionals looking for quick checklists for actions that can be implemented should consider some of the author's approaches. Thanks, Winn, for giving us the alternatives. ■

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.

(ISC)² Security Congress 2019

A reminder that early bird registration for this year's Security Congress, which will be held in Orlando from October 28 to 30, is open through August 15. If you're interested in hearing from fellow member experts about the latest trends, networking with colleagues and partners in the cybersecurity industry, and earning CPEs while you do it, click here to register today. ■

PAYOFF

Paid in 2018 in response to SamSam ransomware attacks

Source: Sophos Labs 2019 Threat Report

Image: iStock

(ISC)²

SECURE SUMMIT / DENVER

JUNE 28, 2019

ENRICH ENABLE EXCEL

Defining Cybersecurity

Join us in Denver for Official (ISC)² Pre-Conference Training. 2-Day and 5-Day courses offering more education opportunities, more CPEs, and a discount on registration if you attend classes and the Summit.

CISSP® CAP® SSCP® CCSP®

Secure Summit Denver will feature these four topics:

- Defining the profession and your responsibilities
- Defining threats
- Defining new technologies
- Defining industrial control systems and 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

(ISC)² MELBOURNE CHAPTER

Engaging the Community in Cybersecurity

(ISC)² Melbourne Chapter uses its meetings to spread the word on current needs

(ISC)² Melbourne Chapter meeting: "Cloudy with a Chance of Hackers"

"CLOUDY WITH A CHANCE OF HACKERS"—that's one of the recent presentations hosted by the (ISC)² Melbourne Chapter as part of its bimonthly meetings. Focusing on key security challenges and perimeter controls, the meeting is typical of the knowledge-packed sessions the chapter hosts. "As an official chapter of (ISC)², we're keen on ensuring quality cybersecurity is brought to the community, keeping in mind the essence of knowledge sharing," says chapter president Dhananjaya "DJ" Naronikar.

The chapter, with 641 members currently (and growing rapidly), relies on its meetings and presentations to attract a wide variety of attendees, including university students pursuing cybersecurity programs, graduates keen to pursue a career in cybersecurity, experienced professionals and even CISOs from organizations who attend not only for the knowledge shared, but also to network for talent. Adds DJ, "Our meetings are hugely popular as the chapter looks to bring in the best speakers from around Australia to present about very topical areas of cybersecurity."

Another incentive is that the chapter does not charge members for attending the knowledge sessions/networking events, which is enabled by strong partnerships with local sponsors, including E&Y and PwC and other Melbourne firms.

Chapter President Dhananjaya Naronikar leading a discussion.

Getting the word out to the community is key. The chapter uses social media platforms like LinkedIn, Facebook, Twitter, Eventbrite and the chapter's own website. The chapter board is committed to presenting topics that are timely and critical to members and other attendees, from cloud security, to DevSecOps, OT/ICS security and beyond. ■

(ISC)² MELBOURNE CHAPTER

Contact: Dhananjaya Naronikar, President, (ISC)² Melbourne Chapter

Email: dj@isc2melbourne.com

Website: http://isc2melbourne.com

Q&A

Dhananjaya "DJ" Naronikar

President, (ISC)² Melbourne Chapter

"The board has representation from a cybersecurity startup company, Big Four consulting firms, professional services firms and industry verticals."

—Dhananjaya "DJ" Naronikar

What tactics do you use to attract top speakers as well as strong sponsors?

One of the key factors to attract speakers and sponsors alike is the composition of (ISC)² Melbourne Chapter's board of directors. We have diverse representation from across the industry that helps in reaching out to talented professionals (CISOs, cyber specialists, etc.). The board has representation from a cybersecurity startup company, Big Four consulting firms, professional services firms and industry verticals. This helps in initiating conversations necessary to rope in speakers and sponsors. Where necessary, we also post a call for speakers through our social media channels. This is to make sure we have speaker representation from across the spectrum.

What methods do you use to gauge members' interests in various topics?

We use several methods: the interactions the board members have with the wider security community, the trends that we notice on social media, and when we come across a talented and skilled professional who is keen to share his/her knowledge, then we tailor the topic to suit their skills.

This is to provide equal opportunity and encourage more participation in the chapter activities.

You mentioned that you have quite a few students attending the chapter presentations. Given the predicted shortfall in cybersecurity professionals, how does the chapter encourage more students to become members of the tech community?

The Melbourne Chapter is working with many universities locally (e.g., La Trobe University). We're plugged into working directly with the professors/lecturers of these universities to increase student memberships into the local chapter and participation in chapter meetings. The Melbourne Chapter also works with Tony Vizza, CISSP, (ISC)² director of cybersecurity advocacy for the APAC region, when it comes to establishing connections with various universities and their students.

Looking at the future, what are the key cybersecurity challenges facing members?

Key challenges are:

- Easy access to certification study material.
- (ISC)² memberships (to enable students to access member-only material).
- Training costs for students (and professionals) who are looking to pursue various (ISC)² certifications.
- The availability of too many security programs/certifications in the market, often making it difficult or confusing to students/graduates when trying to select the appropriate program.

STRATEGIES NEEDED

55%

Of organizations do not make "protecting" part of their strategy

AFTER THE BREACH

76%

Of organizations increased their cybersecurity budget after a serious breach

DANGER ABOUNDS

6.4 BILLION

Fake emails sent worldwide every day

Source: Ernst & Young Global Information Security Survey 2018-19 of 1,400 respondents including CISOs, CIOs and other managers

(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

ENRICH ENABLE EXCEL

SAVE $50
Off All Access Pass
with code:
INFOSECD18

REGISTER TODAY!

congress.isc2.org
#ISC2Congress

TIME TO Smarten Up

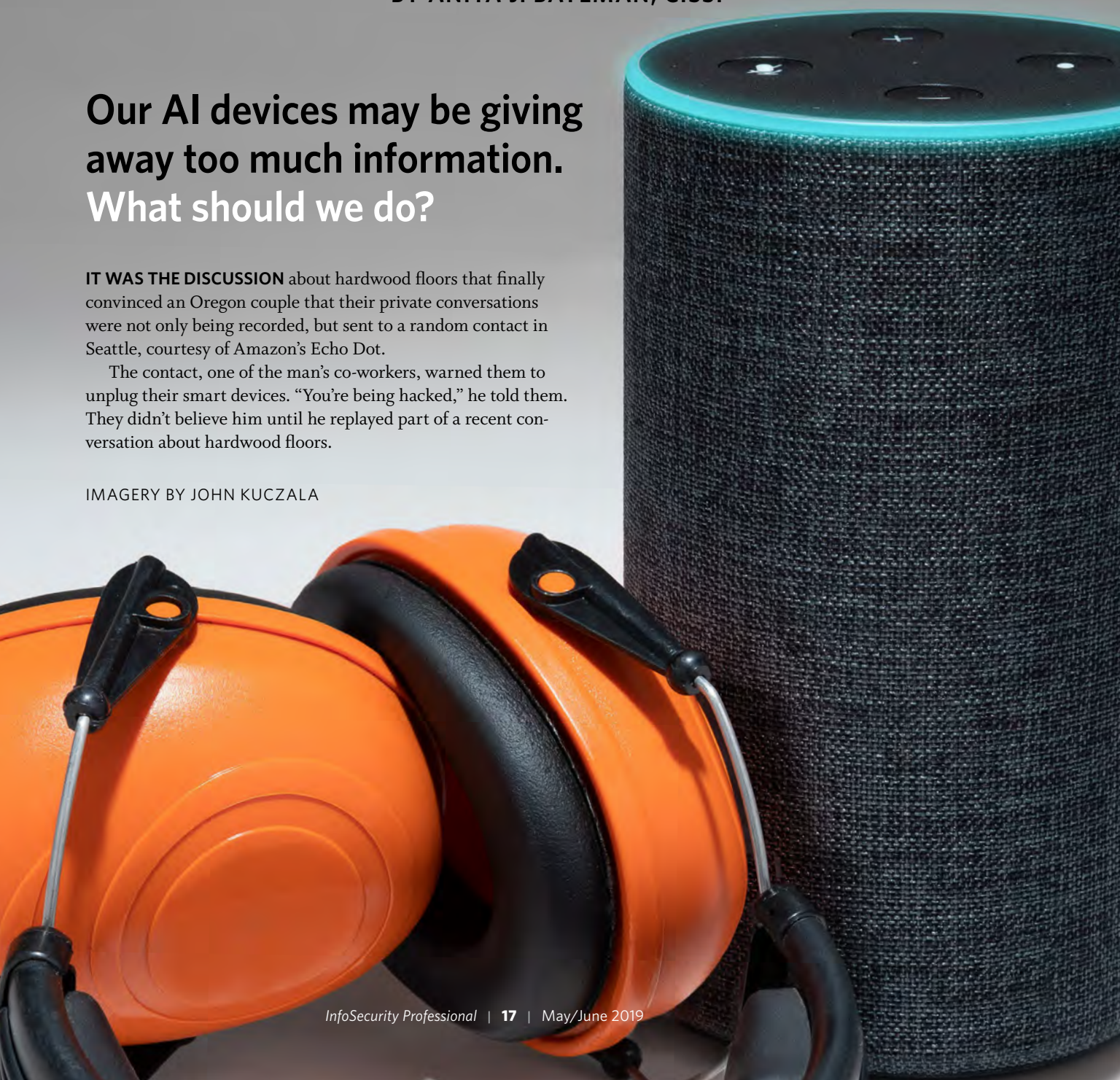
BY ANITA J. BATEMAN, CISSP

Our AI devices may be giving away too much information. What should we do?

IT WAS THE DISCUSSION about hardwood floors that finally convinced an Oregon couple that their private conversations were not only being recorded, but sent to a random contact in Seattle, courtesy of Amazon's Echo Dot.

The contact, one of the man's co-workers, warned them to unplug their smart devices. "You're being hacked," he told them. They didn't believe him until he replayed part of a recent conversation about hardwood floors.

IMAGERY BY JOHN KUCZALA



Amazon called it an isolated incident, most likely triggered by someone using words that were interpreted by the machine as "record" and "send."

As with most new technology areas, the smart speaker and AI home device market has quickly accelerated over the past five years since Amazon introduced the Alexa and Echo in November 2014. The major players—Amazon, Google, Microsoft and Apple—have a large range of products, and other global vendors have rolled out new solutions in the past two years *(see A Timeline of Voice Assistant and Smart Speaker Technology From 1961 to Today)*.

We are challenged as consumers and as cybersecurity professionals to keep up with this technology pace. Beyond the challenges for end users to understand these devices, the growth of the technology in this space provides interesting legal, ethical and personal dilemmas for us to examine with our cybersecurity "hats" fully on.

From music and weather to home security, thermostats, appliances, smart offices, healthcare and even fashion advice, the use cases are multiplying rapidly for smart speakers and other smart assistant devices *(see "The Buzz" on p. 19)*.

So, how do we approach this broad topic as cybersecurity professionals?

Let's look at how smart speaker devices are handling the cybersecurity CIA triad of confidentiality, integrity and availability, and let's add privacy as a component of confidentiality for this discussion. Most of us are familiar with these critical tenets, but to help ground us, here is a quick refresher from the Infosec Institute.

Confidentiality "…states that access to information, assets, etc. should be granted only on a need to know basis so that information that is only available to some should not be accessible by everyone.

Integrity makes sure that the information is not tampered [with] whenever it travels from source to destination or even stored at rest.

Availability [as a] concept is to make sure that the services of an organization are available."

Privacy, as defined by the Merriam-Webster dictionary, is "freedom from unauthorized intrusion," whereas the legal interpretation of privacy includes a person's right to control how their information is collected and used.

CONFIDENTIALITY AND PRIVACY

Smart speaker vendors provide access to your audio files in several ways. Amazon and Google provide you with access to your recording history for replay and allow you to delete the recordings. Apple analyzes logs and then erases them, so there is no history for you to replay or erase.

The question around confidentiality comes down to how much we trust our device vendors to abide by their privacy and security claims. In addition to your audio files, these devices connect to your other personal accounts, such as your Amazon Prime account with credit card and other sensitive data, or your Google email account and other Google services. We need to hold vendors accountable to make sure that they protect our sensitive data, especially when a device can be accessed by multiple users.

"Those who choose to use this technology can't and shouldn't expect 100 percent privacy."

—Bill Brenner, research director, IANS

The confidentiality topic is closely tied to privacy. Capturing audio data to learn about us as consumers is critical to the business models of Amazon and Google, as well as other vendors. The sharing of our data with third parties is broader and wider than we might have initially imagined.

Bill Brenner, now a research director at IANS, wrote in a 2017 NakedSecurity blog post: "Those who choose to use this technology can't and shouldn't expect 100 percent privacy. If not for the ability of Amazon Echo and Google Home to listen, these things would become nothing more than doorstoppers and paperweights."

Brenner provided a few recommendations to protect ourselves when using these devices.

- Mute your device when you are not using it. Or even better, consider unplugging it.
- Don't connect your sensitive accounts to your device.
- Erase your old recordings on a regular basis.
- Tighten up and review your device security settings.

Dr. Florian Schaub, an assistant professor at the University of Michigan, is focusing his research around understanding privacy and security behaviors and perceptions in order to identify the security flaws in these products. In a recent article, Schaub and his co-authors make the case for "strong standards for IoT security and privacy protections … in order to establish a reasonable baseline consumers can rely on. Security certifications of devices could further ensure that certain standards are met by a device … similar to safety seals for electronics products.

THE BUZZ

HERE ARE SOME recent news stories and usage scenarios that have everyone talking:

- Amazon Workers Are Listening to What You Tell Alexa
- Google Nest Secure home security system revealed to have a microphone that can be enabled as a smart assistant.
- Did Alexa Hear a Murder? We May Finally Find Out
- Alexa and Third Parties' Reasonable Expectation of Privacy
- CSI Alexa: The Smart Home Has Become the New Crime Scene Witness
- Amazon Alexa Will Come Built-In to All New Homes from Lennar
- Toyota and Lexus Vehicles Will Add Amazon Alexa This Year
- Panasonic Adding Google Assistant and Amazon Alexa to Future In-car Infotainment
- Kia adds Google Assistant to Infotainment System
- Google Assistant Is Coming to Android Auto
- Amazon's Blockbuster Alexa Event Made Zero Mention of Privacy Concerns
- Research has demonstrated an approach for how to attack smart speaker systems using directional sound beams.[1]
- The Amazon Echo Look with Alexa provides fashion advice.
- Smart speakers in healthcare remind patients to take medication, check blood sugar or provide other daily activity reminders.
- Additional research projects are branching out into voice recognition of individuals, sentiment recognition, inferring child behavior, keyword identification (for advertising, law enforcement or other use) and leveraging wearable technology for security improvements.[2, 3]

FOOTNOTES:

[1] "POSTER: Audio Hotspot Attack: An Attack on Voice Assistance Systems Using Directional Sound Beams," CCS '18, October 15-19, 2018, Toronto, ON, Canada; By Ryo Iijima, Shota Minami, Zhou Yunao, Tatsuya Takehisa, Takeshi Takahashi, Yasuhiro Oikawa and Tatsuya Mori

[2] "Understanding the Long-term use of Smart Speaker Assistants," by Frank Bentley, Chris Luvogt, Max Silverman, Rushani Wirasinghe, Brooke White, Danielle Lottridge; Proc ACM Interact. Mob.

[3] "Wearable Technology Brings Security to Alexa and Siri," *GetMobile*, March 2018, Volume 22, Issue 1, pages 35-38.

—A. Bateman

Companies need to truly provide transparency about smart speakers' data practices to consumers, including what data is collected, how long it is stored, who has access to it and how it is protected."

In a recent discussion with Schaub, he highlighted that most smart speaker vendors' privacy policies and terms of service are vague and do not provide consumers with much concrete information or assurance about how their data is being stored, accessed, used or protected. Many of us may not realize that our voice data may reveal a great deal about us—including gender, age, nationality or even mental state. We need to pay attention to how our personal data is being used and shared.

Consider the scenario in which you have a smart speaker

in your home and you have a visitor. Then ask yourself:

- Where is your smart speaker located in your home?
- What is your visitor's expectation of privacy?
- What is your obligation to them?
- Are you obligated to inform them of the presence of a smart speaker and its on/off status?
- What about other audio-enabled devices, like thermostats or appliances, that you have in your home?

There are plenty of positive use cases for these devices, including providing more accessible technology for those with disabilities. However, we must also consider our individual responsibilities and the expectations of privacy for visitors to our homes. This technology is recently starting to make its way into the business office environment, introducing more confidentiality challenges to consider.

This technology is recently starting to make its way into the business office environment, introducing more confidentiality challenges to consider.

INTEGRITY

Integrity involves the assurance that information is not tampered with in transit or at rest. Tampering with voice data requires more technical know-how but is still feasible.

Research from October 2018 in Japan was able to demonstrate the ability to insert inaudible voice commands into the environment and manipulate the behavior of both Amazon Echo and Google Home devices.

Other research has looked at possible attack vectors for the Amazon Echo. The multiple user scenario can be problematic when it comes to integrity, as a guest could get access to information on a device for which they are not authorized.

Amazon and Google allow their devices to be configured to access multiple, different accounts. While Amazon and Google devices can be trained to recognize your voice, this does not appear to be the default configuration. "An amusing story of an African grey parrot able to mimic its owner's voice activating a smart speaker and conducting internet shopping illustrates some of the technical limitations of smart speakers," according to a health law blog post.

AVAILABILITY

Availability is an interesting characteristic to examine as the main intent for smart speakers is to be available to you when you want to use them. The devices are "always on"—waiting for their special "wake word" or keyword. The ability to change the wake word is available from Amazon and Google; however, Apple has not caught up yet (you are not allowed to rename Siri).

The ability to easily turn your device off and back on is another feature to consider. Most products provide a physical button that will mute the device or disable the speaker; however, you must physically take action to use it. The ability to issue a voice command to turn off or mute your speaker has not been implemented.

In general, if you are concerned about availability, the default settings will provide what you need. If you are more concerned about privacy than availability, you might consider when to mute or even unplug your smart speaker devices in your home.

Availability can also be balanced with providing the necessary parental control capabilities. Google and Amazon both have options that support content filtering and profile setup for kids' use. The Amazon Echo Kids Edition even includes a manners setting that requires the speaker to say "please" and "thank you."

We have taken a very brief look at smart speakers and how they support confidentiality, privacy, integrity and availability today. This article did not delve into third-party data sharing or third-party "skills" for Amazon devices or Google Play apps. Those are topics for another day and are additional threat vectors for smart speaker devices.

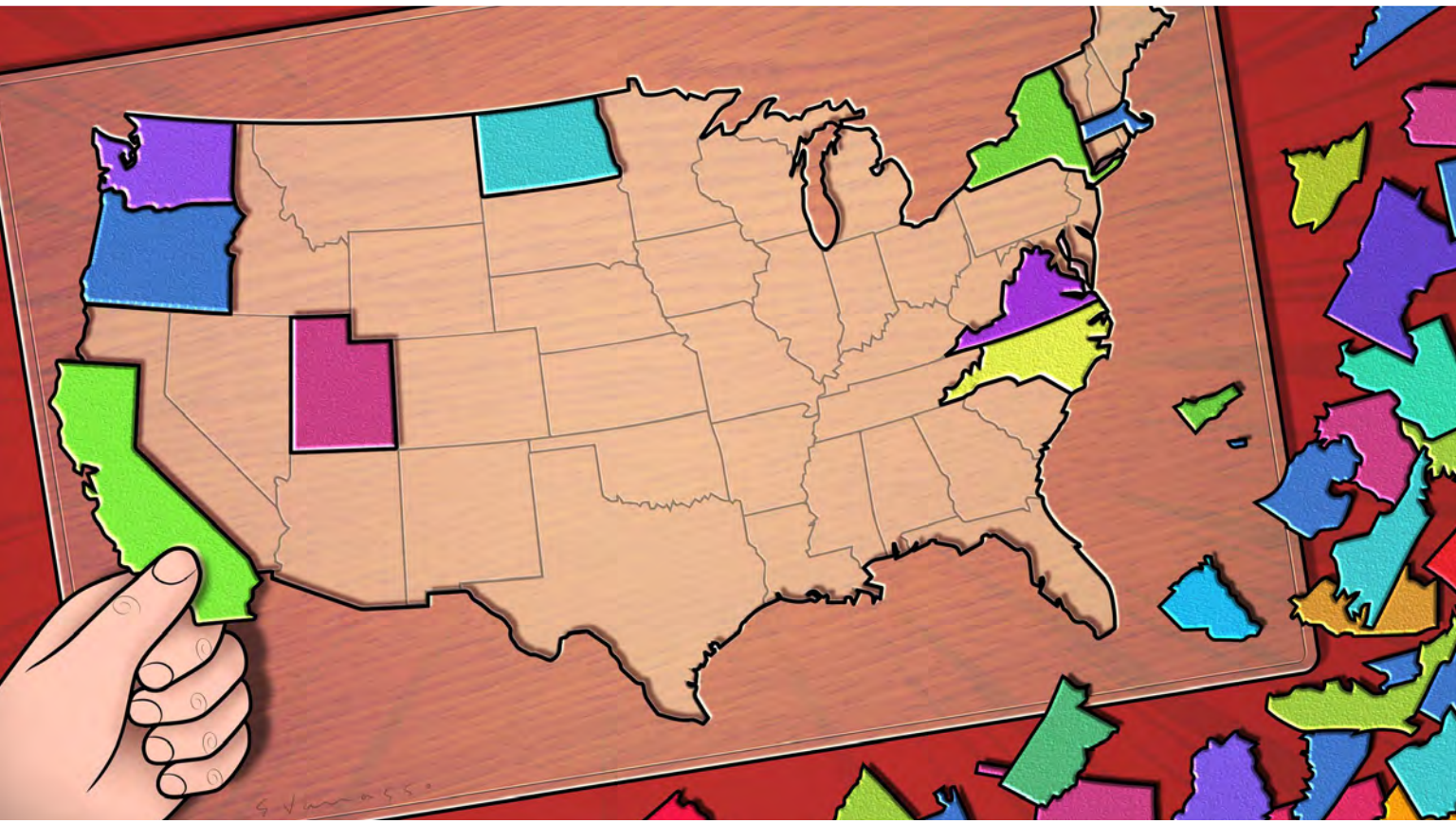
I expect some of us in the cybersecurity community are involved directly in product development for smart speaker technology, and more of us may be involved in the expanded use cases described earlier. We are beholden to our community and for the greater good to work diligently to continue to advance smart speaker technology and uphold the CIA tenets within our spheres of influence.

ANITA BATEMAN, *CISSP, is director of IT services for Ohio-based automotive manufacturer Dana and a past contributor to* InfoSecurity Professional.

CCPA vs. GDPR

An overview of growing pro-privacy legislation in California and across the U.S.

BY JENNIFER J. SOSA, ESQ.



PERSONAL DATA is a critical asset for many companies, and governments are requiring greater transparency and accountability in how they use and manage it.

Last May, the European Union's General Data Protection Regulation (GDPR) came into effect after being highly anticipated by both domestic and international businesses. GDPR unified the data privacy laws of EU-member countries through a wide-ranging piece of legislation that affects companies doing business with any citizen of an EU country. The regulation is designed to expand consumer rights and control over personal information and require transparency in how companies treat personal data.

ILLUSTRATION BY ENRICO VARRASSO

Many organizations felt compelled, even prior to the enactment of GDPR, to evaluate their business processes and policies regarding the use of data and proactively implement programs to facilitate regulatory compliance with the regulation. That trend should now accelerate.

The CCPA is often described as being modeled after the GDPR and shares many similarities with its EU counterpart.

Nearly a year later, several U.S. states have not only taken notice of GDPR, but they also have drafted or adopted legislation that mimics or even extends the EU regulations. As the regulatory landscape surrounding data security and privacy continues to expand beyond GDPR, the critical question becomes: What more is needed to be compliant, or prepare for compliance, with such regulations?

California is currently at the forefront of state data privacy law efforts. As a hub for many science and technology leaders, California developed legislation to prioritize consumer rights concerning the privacy of collecting and using personal information. To that end, on June 28, 2018, California hurriedly enacted the California Consumer Privacy Act of 2018 (CCPA). The CCPA takes effect on January 1, 2020 and aims to create new and powerful consumer rights over personal data and to set data protection standards for businesses.

The CCPA is often described as being modeled after the GDPR and shares many similarities with its EU counterpart. For instance, both regulations encourage transparency, require businesses to report data breaches, and attempt to provide greater security for personal information.

However, there are a number of differences between the two regulations. Organizations that took steps to comply with GDPR will now need to assess whether additional processes should be added to their current compliance programs in order to be better prepared for CCPA enactment.

The chart *(see next page)* highlights certain differences between the GDPR and the CCPA.

The implementation of the CCPA will create challenges for businesses attempting to translate its requirements into business operations, policies and practices to facilitate compliance. The importance of developing such processes cannot be overlooked, as potential civil fines and damages arising from private action have the potential to quickly become significant.

The requirements of the CCPA are likely to be replicated or even expanded throughout the United States. At last count, nine states have either amended or introduced bills concerning data privacy and data security. For example, on January 19, 2019, Massachusetts amended the state's data breach law, providing in part that "any entity that owns or licenses personal information about a Massachusetts resident is currently obligated to develop, implement and maintain a comprehensive written information security program that incorporates the prescriptive requirements contained in the regulation."

An important takeaway here is that states seem to be evaluating their privacy regulations and are likely to require companies to adopt or update their data governance programs.

As legislation spreads throughout the United States, it will become more difficult to recommend or rely on one rigid set of practices for data privacy compliance. Companies should not rely on piecemeal preparation for compliance, but rather should aim to create a baseline information governance program that can be adapted to meet unique state requirements.

Although it is unclear at this time how a company can demonstrate complete compliance with the CCPA and other new regulations, entities should make reasonable efforts to leverage their GDPR compliance work and other existing data management policies to install programs that will help them prepare for data breaches and data requests before they occur.

Features of an effective and defensible data management program should include:

- Understanding what data is being collected, from whom it is being collected, the purpose of the collection, where the data is stored and the lifecycle of the data;
- Creating and implementing best practices to respond to requests for access, deletion and opt-out;
- Creating universal privacy policies and implementing them companywide to ensure consistent best practices;
- Implementing data security protocols to prevent and be alerted to data breaches;
- Creating systems and protocols for responding to emergency security incidents; and
- Instituting straightforward methods of communicating about data privacy issues and problem solving.

Data privacy should be central to a company's information security and compliance program. It is critical for legal, IT, business, human resources, marketing and security compliance teams to work together to identify changes in requirements of existing and new regulations and continually update the company's data risk control mechanisms. ■

JENNIFER J. SOSA, *Esq., is the director of information security and compliance services at TransPerfect Legal Solutions.*

CCPA	GDPR
WHO IS REGULATED	
Any for-profit entity doing business in California that satisfies one of the following tests: • Has gross annual revenue in excess of $25 million; or • Annually buys, receives, sells or shares the personal information of more than 50,000 consumers, households or devices for commercial purposes; or • Derives 50 percent or more of annual revenue from selling personal information. The law also applies to any entity that either: • Controls or is controlled by a covered business; or • Shares common branding with a covered business.	Data controllers and data processors that are either: • Established in the EU and process personal data in the context of the activities of an establishment in the EU, regardless of whether the data processing occurs in the EU; or • Not established in the EU that process the personal data of EU data subjects in connection with offering goods or services in the EU or monitoring their behavior.
WHO IS PROTECTED	
Consumers—a natural person that is either: • In California for other than a temporary or transitory purpose; or • Domiciled in California but outside of California for a temporary or transitory purpose.	Data subjects, defined as identified or identifiable persons to whom personal data relates.
WHAT INFORMATION IS PROTECTED	
Personal information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular consumer or household.	Personal data is any information relating to an identified or identifiable data subject.
PRIVACY NOTICE	
Businesses must notify consumers of: • The categories of personal information collected; and • The purpose for which the categories will be used.	At the time that personal data is obtained, the data controller must provide information about its personal data collection and processing. The notice must include specific information that is dependent on whether the data is collected directly from the data subject or from a third party.
OPT-OUT RIGHT	
Businesses must notify consumers of their right to opt-out of the sale of personal information to third parties, and must comply with consumers' opt-out requests.	The GDPR does not enumerate a specific right to opt-out of personal data sales.
RIGHT OF ACCESS	
Consumers have a right to obtain their personal information collected by any regulated entity, as well as additional information, including the business or commercial purpose for collecting or selling the information and categories of third parties with whom the business shares information.	Data subjects have a right to access personal data that is being processed, and data controllers are obligated to provide a copy of the personal data undergoing processing and disclose certain information about the processing.
RIGHT TO DELETION	
A consumer has the right to request that a business delete any personal information about the consumer that the business has collected, subject to certain exceptions. Upon receipt of such a request, the business must delete the consumer's personal information from its records and direct its service providers to delete the data.	Data subjects have the right to request erasure of personal data from the controller under six circumstances. Data controllers who have made personal data public must take reasonable steps, including technical measures to inform controllers that are processing the personal data that the data subject has requested the erasure.
CIVIL FINES	
The California Attorney General can bring an action for up to $7,500 per violation of the CCPA if a business does not cure its violations within 30 days of being notified.	Administrative fines can reach €20 million or 4 percent of annual global revenue, whichever is higher.
PRIVATE RIGHT OF ACTION	
The CCPA provides a private right of action for certain data breaches of nonencrypted or nonredacted personal information. Consumers may seek the greater of actual damages or statutory damages ranging from $100 to $750 per consumer per incident. Companies are given a 30-day window to cure violations, if possible.	The GDPR recognizes a private right of action for any person who has suffered damage caused by a data controller or data processor's infringement of the GDPR.

10 LESSONS LEARNED SECURING A MICROSERVICE ECOSYSTEM

BY EMIL P. MAN, CISSP, CCSP

DRIVEN BY THE NEED to remain competitive and to meet today's consumer expectations, organizations modernizing their IT infrastructure are rapidly adopting decentralized software architectures and adding layers to the tech stacks. Factor in reliance on public, cloud-hosted applications, and the ever-increasing complexity can be quite daunting.

While every path to modernization can be quite different, my team is managing such a digital transformation, and perhaps the lessons we've learned will benefit your organization in building and securing your microservice ecosystems.

ILLUSTRATIONS BY BEN O'BRIEN

1. Software supply chains and the entire infrastructure have become more complex.

Concerns run the gamut from the mobile client that runs your app and how it authenticates and authorizes, all the way to the back-end identity and access management. Furthermore, automated software deployments can allow a bad actor to make a change much faster, making it harder to detect. The speed at which an internal threat becomes a public vulnerability is growing in velocity.

2. The entire ecosystem needs to be on your radar.

For example, an automated method to increase deployment speed brings increased risk. By adding functionality so that new features can be A/B tested and customers can start seeing improvements earlier, more of your continuous integration/continuous development (CI/CD) pipeline needs to be automated.

This also increases the potential for a small piece of malware to "sneak" into production. Despite static code analysis at build time, or even dynamic and penetration testing before a build is released, the predominance of "shadow IT" tools hiding in your organization makes it simple enough for an attacker to inject malware that can turn into a side-channel attack on your entire infrastructure without your knowledge.

This is why it is absolutely critical to monitor:

The source code and device being used to develop that code. Picture a star developer who has shadow IT software on his laptop and gets infected with malware that makes it into the source at build time. This is what it means to monitor the entire software supply chain. One recent example was the "BitPay wallet vulnerability" in which a node.js library was used to specifically target crypto wallets. The library in question was an "event-stream" used for streaming data in all node.js applications and had a wide reach but targeted crypto wallets specifically.

The build server. Not many methods are easier than compromising a company or an application than by simply injecting malware at the build server where often it will automatically get pushed to deployment after validation.

Test infrastructure. A prime target for attackers, it will most likely have the necessary permissions to push infected code down the supply chain into production, enabling them to push their malware further downstream.

Deployment tools such as Ansible or Puppet. Through automation, these servers usually have the necessary permissions to push whatever code makes it to this stage. If necessary controls aren't in place, attackers can insert malware into applications here and use often-undetected side-channel attacks to get access to personally identifiable information (PII) at "run-time."

Image repositories and secure images. A lightweight image that has a minimal footprint, with just the bare essential packages to run your component, is absolutely essential. Once that image is built with your software, it needs to be stored in a repository if you want other teams to use that component or to ensure you are using the latest version. Keep up with your images in the repository by using tagging methodologies and eliminate stale images that may contain vulnerabilities.

Persistence and immutability of the image you have built. A core concept of microservice architecture environments, it's essential to have a clean image and not store data within it.

3. Revisit your API security strategy.

Application workloads increasingly are moving to the cloud. Carefully consider your API security strategy for the framework DevSecOps teams will use to do their work and deliver products to your customers.

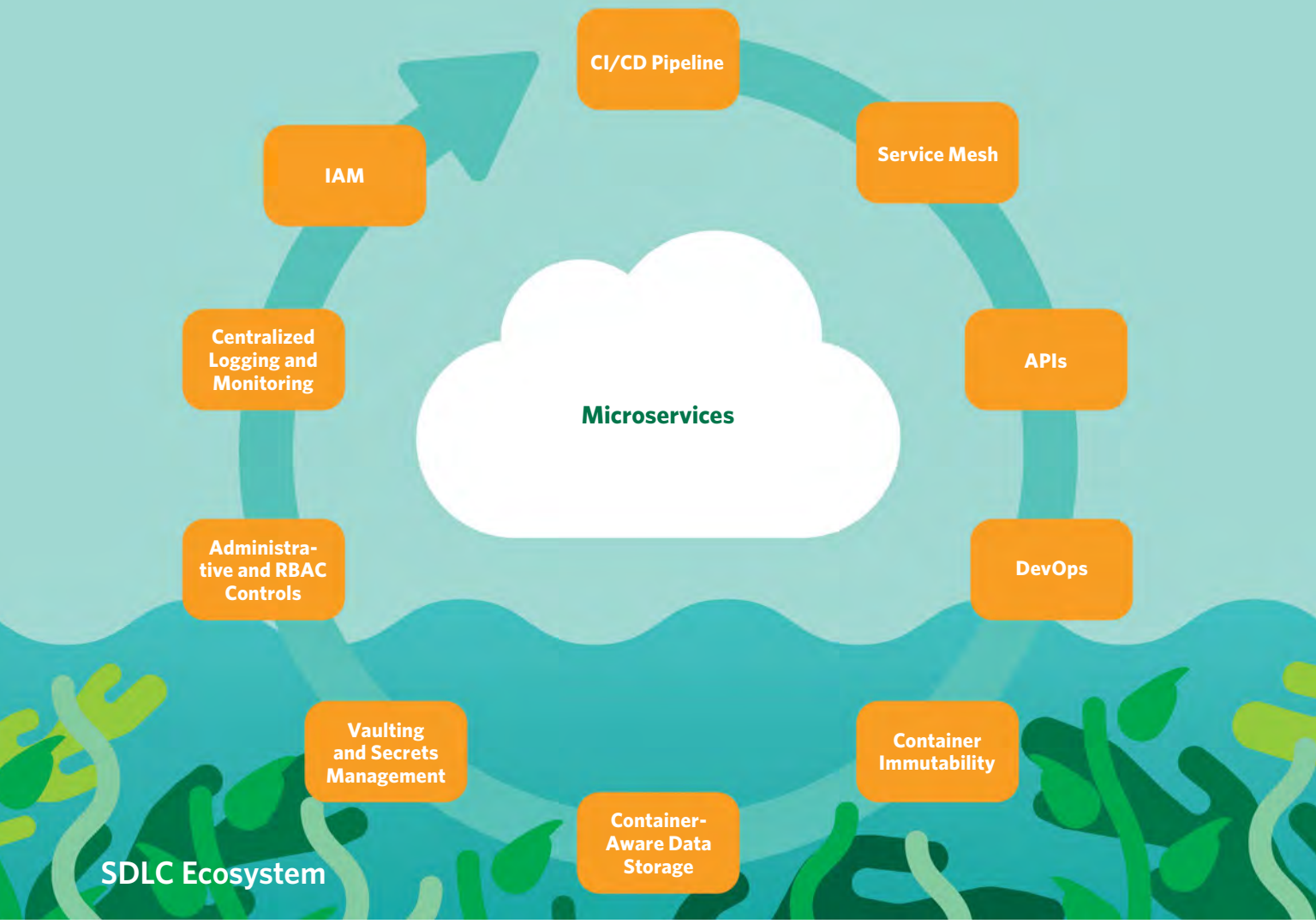
Teams should not publish public APIs without at least the following: (a) authentication; (b) load balancing; (c) a web application firewall; and (d) input and output validation of the data that is moving in and out of your application through that API. It would be best to map and correlate this to a data dictionary that was defined by the team, but it is often not available, or is constantly changing. A data dictionary can also be used by the analytics group and data scientists to build their models, so it serves multiple purposes.

4. A compromised container can be extremely dangerous.

Analyzing "east-west" traffic is complex in a containerized environment running hundreds or thousands of microservices. A compromised container means an attacker could have visibility to inter-container traffic, or possibly to extract sensitive data. It also means that a container could be dead (containers are supposed to be short-lived) before necessary logs are retrieved to do a forensic analysis. Centralized logging can help while you send container and application logs to a central repository outside of the container. Look at Fluentd as a possible solution and combine it with Prometheus.

5. Implement a service mesh.

At a high level, a service mesh within a microservice architecture provides a dedicated infrastructure layer built into an app to allow more control over how data is shared between apps in this environment. This adds a layer of complexity, but without a service mesh in place, it will be difficult to encrypt between services and is necessary for total, end-to-end encryption.



The idea of a "zero trust approach" to security has been on everyone's radar recently. For a zero-trust microservice architecture, we would need to verify each identity and not assume that if you are in the same namespace, a service should be trusted. Furthermore, to ensure that no east-west traffic sniffing is going on, a service mesh is the only possible way to achieve transport security. It looks like the default standard here will be the open-sourced Istio.

6. Vault for secrets management.

Storing encryption keys, API tokens and authentication keys between services and managing how one microservice talks to another one are essential in this type of architecture. It is also vitally important that you recycle and rotate these credentials as needed, for example, after an incident.

In the security industry, we have known for a long time that hard-coding secrets into code is a *faux pas*. Making it easy for developers to inject a secret into their running application is an absolutely essential need. Popular tools include open sourced HashiCorp Vault or CyberArk Conjur.

7. Achieving maturity is hard. Expect a lot of growing pains.

A lot of applications and diverse product lines mean that there is a tendency for the external architecture of supporting tools to become quite complex and hard to manage. In large organizations where individual needs must be satisfied, there will always be a tendency to try to centralize people around their specific function. This type of control can endanger the microservice architecture and the benefits it can otherwise bring to your customers and organization.

This requires empowering teams that include developers, security and operations engineers to make their own decisions and maintain ownership of the product while delivering on tight deadlines. We need to keep them responsible for their product and provide them flexibility to use tools that fit into a framework. At the same time, when you try to control things too tightly, there is a tendency for people to engage in shadow IT.

That's why it's important to consider the following:

- Once you prove the transition to microservices is something that works and adds value to your

customers and your organization, it will be adopted faster by others including development teams. It is absolutely critical that an organization starts small and breaks down a product to make a transition easier. Unfortunately, many organizations start in the middle and want to break down their most complex products first. This rush can cost you greatly in the long term.

- Failing to break down monolith software and simply adding microservices around current software can bring significant security and operations implications down the road.
- Do not take securing the orchestrator (most likely Kubernetes) for granted. A number of controls (resource limits, K8S API RBAC, workload limits, privileges of containers running, etc.) need to be in place before you have a solution that can work for containers deployed to production.

8. Data storage, security and governance should be a priority as data becomes the new gold.

Microservice architecture allows faster development and reduced costs for applications, but this is meaningless without the data you are processing or generating for yourself or your customer.

Data persists outside of the container and needs to be stored in a secure manner. This means storage blobs that have the proper controls in place and the ability to achieve multi-tenancy through encryption keys that your customer owns and controls. If you don't think about this aspect from the very beginning of designing your solution, it will be that much harder to implement later when your customer will ask about it.

9. A maturing CI/CD pipeline with adjoining practices is essential.

You should get started on your microservices journey while building the foundation of your CI/CD environment and

normalizing your tech stack. Breaking down and simplifying everything you will be sending out to a customer in production will also help achieve a certain level of maturity.

I highly recommend the latest 2018 State of DevOps Report published by Puppet and Splunk for best practices when starting on the path of maturity for DevSecOps in your organization. Without having continuous integration practices, culture and tools in place, you will never be able to deliver in a containerized environment, where your applications need these capabilities even more than in a monolith software environment with typical waterfall development methodologies. The security of your microservice-based application is absolutely dependent on your CI/CD and DevOps practice as it serves the software supply chain of your products.

10. Integrate identity and access management into one common tool across the ecosystem.

Using one common IAM for all tools with the proper role-based access lets you painlessly move developers around teams and projects. Identity and access management around the entire ecosystem is essential and needs to be integrated across all of your tooling. As developers will jump around your agile organization, keeping track of "scope creep" along all of your toolsets will otherwise be an insurmountable task. Furthermore, if IAM is not easy to manage and integrated throughout your SDLC, project managers and administrators will simply fall behind in the management of user rights, and this could become a vulnerability.

Not all of these lessons may apply in your case because every organization is unique, but my hope is that by better understanding some of these lessons we've learned during my company's digital transformation, you'll achieve success sooner and more securely. ■

EMIL P. MAN, *CISSP, CCSP, MBA, is a product security leader at Honeywell in Atlanta.*

Speaking the Universal Language of Cyber Safety

by Pat Craven

Safe, seguro, veilig, sûr, 安全, sábháilte, sicher, säker, bezpečný.

No matter how you say it, it's what we are all trying to do—keep our children and families SAFE online. But until now, you and your audience had to speak English to take advantage of the tremendous educational programs provided by your nonprofit Center for Cyber Safety and Education. Well, that limitation exists no more.

At the 2018 (ISC)² Security Congress in New Orleans, we announced that we were beginning a project to translate all our parent, senior and middle school educational materials and presentations into some 30 languages. Under the direction of our Community Engagement Coordinator, Beatriz Parres, and our Educational Program Specialist, Ciera Lovitt, we are well on our way to reaching our goal.

Thanks to a growing list (more than 200 so far) of bilingual (ISC)² volunteers from around the world, we are adding new language materials almost every week. Just go to https://iamcybersafe.org/parent-presentation/, and you'll see examples of the work they're doing to make sure that we reflect our global membership and the communities we serve.

Don't see your language yet? Here's how this works. As Language Teams are formed, they communicate with the new (ISC)² Community platform. The groups are in charge of how they will operate and share the projects. Under the Center team's direction, the groups will translate the Parents' Presentation and appropriate tip sheets first, then move on to the materials for senior citizens, and then to the content for middle schools (children ages 11–14) and simpler Garfield Basics.

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

WAIT! Did I just say Garfield will be in other languages? Well, sort of. We do hope to announce soon that the award-winning *Garfield's Cyber Safety Adventures* lessons will be re-created into other languages, but we just aren't there yet (as of this writing). What we do have are several simple PowerPoint presentations featuring Garfield that are available in different languages and cover some fun safety basics for children. They are available for download right now at https://iamcybersafe.org/garfield-basic-program/. It is not the full Garfield lesson available in the Educators Kit or digital version, but it's free and provides a great starter program to introduce cyber safety topics to younger children.

Image: iStock

No matter where you live, we are committed to providing you and the people in your community with the best educational materials on the planet. If you want to help us expand our library of materials in a language we haven't covered and you are an (ISC)² member, we would love to have you join one of our volunteer Language Teams. Just send us a note at safeandsecure@isc2.org and let us know your fluent language(s), and we will put you on an existing team or create a new one if needed. Our goal is to have our free educational materials available in 30 languages by the end of the year. This takes more time than you might think, so if you don't see yours, be patient—or better yet, offer to help.

Our goal is to make it a safer cyber *world*. Thanks to your help, we are closer to making that possible. ■

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

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

QUESTION:

One of the more curious things I've wondered about is how the Right to be Forgotten impacts backups. Obviously, you can't go to a backup (tape) and erase a particular record—at least easily. How are people addressing this right with backups?

—Submitted by DHerrmann

SELECTED REPLIES:

The only thing that would work would be some kind of "register" of those forgotten to ensure you're not pulling out their data when you do a restore or the like.

—Submitted by emb021

I once took part in an exercise for an ISP to drop all historic DHCP data backups because law enforcement could request that data for various purposes, if it was held. This represented a very significant possible cost and it was circumvented by dropping those file-sets so they could not be recovered. Morality notwithstanding, it's a nifty capability to have.

—Submitted by ed_williams

Most of what has been written, argued and opined about RTBF has to do with search engines. Most of the decisions are slaps and fines against Google for allowing decisions and events to be searchable. (As such, there is a strong case for those who say that RTBF is not actually a right, but a cash cow.) Actual stories don't have to be taken down, just the Google links to them.

By extension, therefore, backups are not subject to RTBF. As soon as someone or some corporation finds a way to make huge amounts of money charging people for cloud backups, then the EU will extend RTBF to ensure that they can fine the heck out of that corporation for keeping backups.

—Submitted by rslade

Here's some useful guidance on this from the Information Commissioner's Office, the public body responsible for upholding information rights in the U.K.

"If a valid erasure request is received and no exemption applies then you will have to take steps to ensure erasure from backup systems as well as live systems."

—Submitted by AlecTrevelyan

I created and maintain a DB that holds all requests for deletion and in case [I] run a restore of my backups, all deletion requests will be re-run against the restored data so, as with beginning of usage of the "restored-DB," none of the users who requested the deletion of their data are in the DB.

—Submitted by RRehm

Find this complete thread here.

QUESTION:

I want to switch my career to cybersecurity professional. The issue, of course, is that I do not have any experience in the field. I'm doing a few online courses but not sure how much they would help with the job. [Is there] a process of what can be done in order to start being acknowledged by the industry? Would continuing courses help eventually, or is there some exam ... [that] would give some kind of recognition? Your help would be appreciated.

—Submitted by Ayazm

SELECTED REPLIES:

I don't want to ruin your enthusiasm but I think the best tool, and mostly recognized, is experience in the field. IT security often touches a wide range of items, which is hard to capture in a single training. Which is also why the CISSP certification requires a number of years (of) working experience.

—Submitted by gert

My recommendation for you is try and get a job as a help-desk specialist and work your way up from there. In my experience, the best security professional is the one with the full breadth of knowledge regarding operating systems, hardware/software, databases, networking, vulnerabilities, etc., and all the little intricacies that make them function—things you don't really learn by reading books.

—Submitted by dharvey32

Gain as much experience as you can. Even if you have to do it yourself. I set up a lab environment and practiced all kinds of setup and hacking to gain the experience I couldn't gain at work.

—Submitted by CISOScott

Find this complete thread here.