NEW BOARD CHAIR ON (ISC)² CEO'S LEGACY

InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

MAY/JUNE 2020

MAKING YOUR WAY THROUGH THE CLOUD

Who's in control of your cloud security—you or your service provider?

PLUS

Building a Hardened Container Infrastructure

Every Cybersecurity Professional's Worst Nightmare

Why Security and Privacy Need to Play Nice


CCSP
Certified Cloud Security Professional
An (ISC)² Certification
FREE CCSP WEBCAST SERIES
Get a Look Inside the CCSP Domains
Watch Now ▶

contents

VOLUME 13 • ISSUE 3

PAGE 27

features

Cover illustration: TAYLOR CALLERY Illustration above: ROBERT NEUBECKER

departments

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

Going the Distance

BACK IN EARLY FEBRUARY, when we were starting to put together content for this issue, someone suggested a piece addressing the novel coronavirus that was then disrupting parts of Asia. I turned down the idea, believing that by May the COVID-19 outbreak would be passé.

Boy, was I wrong. We are, and will, continue to deal with the economic, health and social consequences of this global pandemic that swiftly changed the way we work, live and interact. Times like the past few months show the power of community, creativity, commitment and compassion when the world sorely needs it.

Unfortunately, the outbreak also provided more opportunities for malicious activity, with bad actors taking full advantage of teams or solo practitioners scrambling to secure an entirely remote workforce. Swift adoption of online communications channels created their own risks, as did discovering that not every employee was equipped for telecommuting, nor did everyone use protected Wi-Fi to send confidential emails or employ encryption when accessing or storing corporate data in the cloud.

I'd like to think that (ISC)² members prepared for this global crisis, at least to the extent they could have.

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

I'd like to think that (ISC)² members prepared for this global crisis, at least to the extent they could have. That they had a business continuity plan in place that now represents the new normal. That those plans took into account uncooperative employees or contractors and the uptick in cyber intrusion attempts. That because they acted swiftly and thoughtfully, everyone continues to work, if still at a distance.

I'd also like to think that maybe, in some small way, everyone at (ISC)² contributed to sound decisions made with little notice and used common-sense measures when everyone else panicked. I hope that by the time you read this issue, public health plans will be working as intended. That you and those close to you remain secure—and healthy. ■

InfoSecurity PROFESSIONAL

(ISC)² MANAGEMENT TEAM

EXECUTIVE PUBLISHER
Timothy Garon
571-303-1320
tgaron@isc2.org

SENIOR MANAGER, CORPORATE COMMUNICATIONS
Jarred LeFebvre
727-316-8129
jlefebvre@isc2.org

CORPORATE PUBLIC RELATIONS MANAGER
Brian Alberti
617-510-1540
balberti@isc2.org

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

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

TWIRLING TIGER MEDIA MAGAZINE TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

EDITORIAL ADVISORY BOARD

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

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

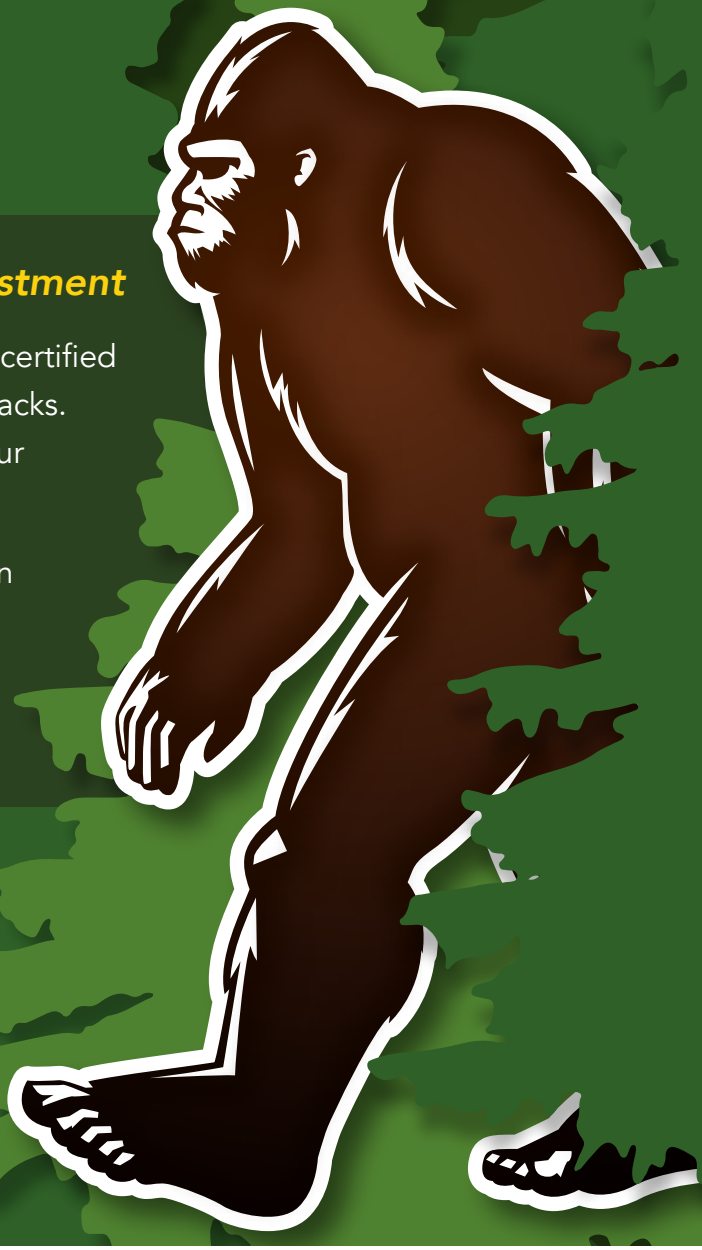
Twirling Tiger® Media is a women-owned small business. This partnership reflects (ISC)²'s commitment to supplier diversity.

RETURN TO CONTENTS

(ISC)²

6 TRAINING MYTHS EXPOSED

Don't Fall for FICTION. Know the FACTS.



We're Looking Out for Your Training Investment

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

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

Get the Facts ▶

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

Recognizing Progress and Pushing for More

by Dr. Kevin Charest, CISSP

IN JANUARY, I was honored to be elected to serve this year's term as Chairperson of the (ISC)² Board of Directors for the second time, after previously serving in the role in 2018. I'm happy to be back at such an important time in the association's history, and I wanted to share my thoughts here as we map out the future. You can't plan for where you're going, though, without knowing where you've been.

As was announced earlier this year, CEO David Shearer will step down from his post at the end of December after serving in the role for six years and being with (ISC)² for more than eight years. We have a selection committee working hard to identify his replacement, which is no small feat. David's contributions have been numerous, including overseeing the launch of the CCSP cloud security certification, establishing Security Congress as a premier global security conference and overseeing a period of unprecedented membership growth. But I'd like to focus on two specific accomplishments that required David's expertise and vision to position us for the next era. His steadfast commitment to modernizing our association and to delivering member value have revolutionized (ISC)² from both an operational and programmatic standpoint.

Dr. Kevin Charest chairs the (ISC)² Board of Directors and is the divisional senior vice president and CISO for Health Care Service Corporation. He can be reached via LinkedIn.

Back in 2018, I was writing to you in this very space about the plans for digitally transforming the many legacy IT systems that (ISC)² had been using for decades. This was a massive undertaking, and the kind of project that requires grit and ingenuity but comes with no glamour. Still, foreseeing the need to deploy cloud systems to scale alongside a rapidly growing, global membership, David led the charge to future-proof the systems that would ultimately make it easier for members to interact with (ISC)². Within two years, the upgrades were in place and the transformation had been accomplished.

The other initiative that David knew was of critical importance was to provide the best membership value in the industry. As members, we pay for the privilege of holding our certifications, and the association has a duty to not only maintain the certifications, but to deliver programs that warrant that investment. One of the criticisms of certification is that any one exam can't possibly affirm an evolving set of required skills in a changing cybersecurity landscape. While the exams are routinely assessed and updated to compensate, David envisioned an industry-first portfolio of on-demand learning opportunities that provided insights on emerging trends in real time.

Within a year of coming to the Board with an aggressive proposal to not only build out a library of such courses, but to offer them at no additional cost to (ISC)² members and associates, the Professional Development Institute (PDI) was launched in February 2019. In the first year alone, more than 30 courses were offered through PDI, representing a total value of more than $10,000. The engagement with the content has been superb, as more than 12,000 courses were completed before the end of 2019, representing $7.9 million in value delivered.

This is the legacy David leaves, and we thank him for all he's done for our members all around the world.

It's an exciting time for our association as we look at what's next. Our Board of Directors is working as we speak to chart the course forward as we approach a new era, and you will see those plans start to solidify later this year as we welcome a new CEO for 2021 and roll out new training and continuing education opportunities. The (ISC)² Security Congress in November will be our best yet and we hope many of you will attend.

I encourage you to stay involved, to offer your unique perspective on what we can be doing better, and to walk with us into this next decade as we continue to build our industry. ■

RESPONDING TO A GLOBAL PANDEMIC

Multi-factor Authentication Is Needed Now More than Ever

BY SAURABH GUPTA, CISSP, CCSP

IN THE WAKE of the novel coronavirus global pandemic, nearly everyone was mandated to socially distance themselves to avoid spreading the contagion. Employees were advised to work remotely, if possible. To enable such a new workforce, companies have had to adopt various online collaboration tools and remote access technologies.

Multi-factor authentication (MFA) plays an important role when disasters, like the COVID-19 pandemic, disrupt normal working life. MFA also fits well in the enterprise security architecture to mitigate security and privacy concerns. It enhances security, safeguards access to data and applications, prevents security breaches and meets regulatory requirements such as PCI-DSS (payment transaction), HIPAA (medical records) and NIST 800-63 (digital identity guidelines), among others.

WHY MULTI-FACTOR AUTHENTICATION?

Most (ISC)² members are familiar with MFA, which requires verifying an individual's identity with two or more types of evidence. The three predominant types of evidence are:

- Something you know (password, PIN, passphrase)
- Something you have (phone, hardware devices)
- Something you are (biometrics—fingerprint, face recognition)

Risk-based authentication, or adaptive authentication, uses a non-static approach to assess risk profiles associated with the transaction and initiate higher authentication requests for high-risk profiles. Adaptive authentication uses data science to analyze and respond by prompting the user to provide second-factor authentication when the organization's risk threshold is exceeded.

Typically, organizations opt for MFA when an employee wants to connect to a company's network and access sensitive applications or data from outside the corporate network using either organization-provided devices or personal devices (BYOD).

Furthermore, as organizations shift workloads from on-premises to cloud, they want another countermeasure from their cloud service provider (CSP) for assurance and compliance purposes. Today, all major CSPs support MFA using a mobile app, phone call, email, SMS and/or dedicated hardware devices as second factors.

CHALLENGES IN MFA ADOPTION

Despite the concept being around for decades, MFA experienced slow adoption until recently due to infrastructure limitations and availability of cost-efficient technology. Some of the challenges and accelerators that influenced the adoption of MFA include:

- **Requiring dedicated hardware devices.** Users initially were reluctant to carry additional hardware devices for second-factor authentication, and distributing hardware devices to all the users was costly for the organization. Technology advances in telecom and increase in smartphone usage now provide convenient options for second-factor authentication.
- **Malicious actors exploiting security vulnerabilities.** Security incidents like channel jacking, which involves taking over an authenticator communication channel, and phishing to intercept authentication messages using man-in-the-middle attacks led to slow adoption of MFA.
- **Complexity in implementing MFA.** Another challenge was the lack of effective solutions to easily configure MFA for sensitive applications and not disrupt users' productivity. With the rise of cloud solutions, adoption of MFA improved significantly.

Getty Images

IMPLEMENTATION CONSIDERATIONS

During MFA implementation, consider the following to ensure a smooth rollout.

- **Enrich the end-user experience.** Users are initially resistant to new technologies like MFA out of fear it will reduce their productivity. However, these fears can be alleviated by providing user-friendly interfaces, end user training, helpdesk support and advanced rollout communication.
- **Configure conditional access.** Users become frustrated if they must repeatedly authenticate their identity to access sensitive applications and data. To improve ease of MFA usage, systems can be configured not to initiate MFA when a request originates from registered trusted IP, locations and devices. Secondly, leveraging single sign-on along with MFA can improve MFA adoption, as a user can sign in to multiple applications without authenticating repeatedly.
- **Manage technical gaps and complexity.** Like every technology, MFA also provides various options to reduce misuse.
  - Managing lost devices: When devices used for second-factor authentication are lost, allow users to deregister the app and remotely wipe devices to prevent security breaches.
  - Failover alternative: An MFA solution offers several backup options when a second factor does not work. When a cellular signal is too weak, use a mobile app connected through secured Wi-Fi. Allow users to authenticate with one factor only and bypass second factor for a limited period (onetime bypass) when absolutely necessary. Lastly, use offline scanned QR codes and a onetime PIN to authenticate.
  - Secure the MFA registration process: Generally, the registration process is separate from the application to be secured. The threat of malicious users trying to change the second-factor authentication is mitigated by requesting that users confirm a code sent to their registered email or device before making any changes.
  - Applications not supporting MFA: Legacy applications that do not support MFA should support an alternative mechanism such as "app password" to authenticate.
- **Send threat alerts.** Users should be notified of suspicious activity so that they can take precautionary measures to mitigate a security incident. For example, if a user tries to access an account from two distant locations in a short duration of time, he or she should be notified immediately so that user can take action.
- **Implement a strategically effective rollout.** To ensure smooth MFA implementation, organizations can do phased rollouts to minimize the impact on the entire enterprise. Start with a partial rollout to sections of employees for a few, resolve any issues, and then roll out to the remaining organization.
- **Audit and report.** Analyzing MFA usage provides insights into user authentication history and authentication methods used. This helps in identifying security breaches and sending fraud alerts.

With all the benefits provided by the MFA at reasonable costs, particularly as we are experiencing a spike in remote workers, organizations should reconsider MFA to enhance their security posture and provide flexibility to those employees and users working from home by choice or forced by adverse situations like the pandemic outbreak. ■

SAURABH GUPTA, *CISSP, CCSP, is a project manager at a technology company in the Seattle area.*

What's Needed for MFA to Work

Typically, prerequisites for MFA implementation include identifying users, devices, applications and networks that should be secured. From there, the following steps are recommended:

- Configure a chosen authentication method[s] for the organization, such as notification through mobile app, verification code from mobile app, call to phone and text message to phone.
- Select users or groups to roll out MFA initially, so you can work out issues before deploying the technology enterprise-wide. This step provides options to include or exclude users and groups for MFA authentication.
- Configure conditional access policies. Here, an admin can specify trusted IPs, locations, devices and facilitate identification of risky sign-ins.
- Enable MFA for the cloud. For instance, Microsoft Azure provides three options:
  - Enable changing a *user state* that requires a user to perform two-step verification every time they log in.
  - Enable a *conditional access policy,* which provides flexible two-step verification for users in the cloud environment.
  - Enable *Azure AD Identity Protection* in which the Azure AD identity protection risk policy for two-step verification is based on the sign-in risk for all cloud applications. Other cloud providers likely have a similar mechanism.
- Let users select their preference for second-factor authentication.

—*S. Gupta*

RESPONDING TO A GLOBAL PANDEMIC

Remote Access Checklist

SINCE EXPERIENCING a swift shift to working from home, (ISC)² members have had to rapidly bone up on how to secure remote employee access to data, applications and systems required for them to do their jobs remotely.

Protections are must-haves on both sides of the equation: the remote devices as well as the business's network structure. Both the Federal Trade Commission (FTC) and the National Institute of Standards and Technology (NIST), as well as private security companies and organizations like (ISC)², immediately offered guidance on best practices for securing users and hosts during the COVID-19 global outbreak.

They include:

- Installing WPA2 or WPA3 encryption for routers.
- Installing VPNs on user devices and Internet Protocol Security (IPsec) and/or Secure Sockets Layer (SSL) to encrypt traffic between personal computers needing to access data using the internet.
- Providing each user with a separate, standard virtual desktop or putting in place tools to lock down laptops and tablets and even personal smartphones in the event of an incident.
- Limiting a user's access to applications.

In addition, there are best practices to help prevent intrusions for employees using their smartphones or personal laptops/desktops to work from home.

- Discourage using public or neighbors' unprotected Wi-Fi. If someone must use it, make sure it's done with a company-issued VPN.
- Require multi-factor authentication to access all corporate files and use certain applications.
- Disable network capabilities such as Bluetooth and near-field communication except where absolutely needed.
- Do not use unknown charging stations if out in public.
- Install anti-malware on smartphones.

It's also a great time to update staff on the need to comply with security provisions. It doesn't hurt to remind them that if someone doesn't follow best practices, and the company suffers a breach during these trying times, everyone—not just the offender—may be out of a job because the company could go out of business.

Telecommuting, which was already growing, will now become even more prevalent once the global pandemic passes. Best to try to instill good cyber hygiene habits now, to prevent more headaches later. ■

MORE INFORMATION

- NIST User's Guide to Telework and Bring Your Own Devices (BYOD) Security
- Cybersecurity for Small Business: Secure Remote Access
- (ISC)² Webinar: "Always On, Always Working – Securing the Mobile Workforce"
- (ISC)² Community Forum Discussion on Securing Home Workers
- National Cyber Security Alliance Tips for Staying Safe Online

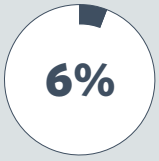
SURGE IN REMOTE WORK

To measure the employer response to the COVID-19 crisis, law firm Seyfarth Shaw sent a flash survey to its clients and collected responses from 550 U.S. employers from March 12 to 16.

Employers that were taking steps to allow employees to work from home who don't normally do so

Employers that were encouraging employees to work from home on a case-by-case basis

Employers that were actively encouraging all employees to work from home in some or all parts of the country



Employers that were encouraging employees to work from home in hot spots

(ISC)² and Tokyo Police Join Forces to Fight Cybercrime

Specialized training will be available to officers

A NEW PARTNERSHIP between law enforcement and cybersecurity professionals is underway in Tokyo, Japan. (ISC)² has signed a memorandum of understanding (MOU) with the Tokyo Metropolitan Police Department (TMPD). The TMPD will adopt (ISC)² credentials for selected members within law enforcement agencies throughout Japan. In addition, the TMPD will provision official Common Body of Knowledge (CBK) training classes to offer its officers the highest-quality cybersecurity training. By encouraging members of its agency to earn the CISSP, the TMPD is ensuring that its staff has the requisite skills to understand, investigate and prosecute cybercrime.

Signing the memorandum: David Shearer, CEO, (ISC)², and Tokuya Matsushita, Assistant Commissioner, Tokyo Metropolitan Police Department.

> "This partnership will help us access the best training available in the market so that we can better protect and serve the people of Tokyo."
>
> —TOKUYA MATSUSHITA

Signing the memorandum in Tokyo were: David Shearer, CEO, (ISC)², and Tokuya Matsushita, Deputy Director of the Cyber Security Control Task Force and Assistant Commissioner at the Tokyo Metropolitan Police Department. Also on hand from (ISC)²: Wesley Simpson, COO; Clayton Jones, managing director, Asia-Pacific; and Greg Clawson, global VP for sales and marketing.

"It's become increasingly important that we arm our law enforcement and government agencies with the tools they need to keep us safe and secure in digital environments, and the Tokyo Metropolitan Police Department is taking steps to grow cybersecurity competencies within Japan," said Simpson. "The fact that an agency as prestigious as the TMPD selected the CISSP as its measuring stick for cybersecurity skills further validates the value and trust that our industry places in the certification."

"(ISC)² certifications represent a standard of proficiency and excellence that we expect from our men and women fighting on the front lines of cybersecurity," said Assistant Commissioner Matsushita. "This partnership will help us access the best training available in the market so that we can better protect and serve the people of Tokyo."

To view a video about the signing of the MOU between TMPD and (ISC)², please visit https://youtu.be/FdD4Dhxa_vo. ■

Training Opportunities Expand in Japan

(ISC)² has expanded its partnership with Japanese computer services firm NTT Advanced Technology Corporation (NTT-AT). Now an official training provider of (ISC)², NTT-AT offers public training on the Certified Cloud Security Professional CBK. The Japanese-language CCSP exam has been available since April, and now, Japanese-language CCSP courseware will be available for training starting in June. ■

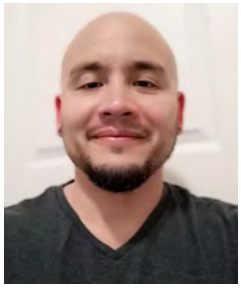
New Cybersecurity Partnership in Australia

An agreement between (ISC)² and the Australian Security Industry Association Limited (ASIAL) aims to advance the information security profession in Australia. As outlined in an MOU, ASIAL recognizes (ISC)² certifications, including the SSCP, CISSP and CSSLP, as measures of experience and knowledge related to information security. And (ISC)² will promote ASIAL as a "peak body" for physical and electronic security in Australia. The two organizations will join forces in advancing the cause of the cybersecurity profession. ■

Getty Images

MEMBER'S CORNER

5 Ways to Make Sure You Hire the Right Cybersecurity Team Member



BY JASON McDOWELL, CISSP

COMPANIES FROM ALL INDUSTRIES are looking for qualified cybersecurity professionals to fill the skills gap in their current workforce. Demand is high, and many companies are willing to pay top dollar to those who possess the skills they need. With this high-demand, high-paying environment, what could go wrong? Plenty.

With the exception of companies that specialize in information security, accurate valuation of the cybersecurity role in many companies is still very challenging, and many managers lack even a basic understanding of what cybersecurity professionals do within the organization. Add in the urgency to meet industry-specified cybersecurity requirements, and things can quickly lead to corporate desperation and poor decision making.

Here are five fundamental considerations for every hiring manager to build their cybersecurity teams.

1. Look beyond words to past actions

This should go without saying; however, some industries have been led to believe obtaining specific certifications qualifies the candidate to perform at full capacity for senior information security roles. If the candidate has the experience to back up his or her previous roles, then requesting some detailed descriptions of past projects will likely be met with excitement and pride, rather than abstraction and half-baked answers.

2. Post thorough job descriptions that make filtering easier

With soft and vague job descriptions comes soft and vague candidates. Taking the time necessary to create comprehensive job announcements will pay off in the end—and will increase the likelihood of attracting legitimate candidates with the right skills and the right amount of experience.

3. Remember the importance of character

The cybersecurity role is a position of trust and, as such, the character of the candidate is of utmost importance. Character is not subjective, but rather an objective quality that can be assessed during an interview. A key and fundamental trait of good character is honesty, which can be initially assessed through consistency. Looking for inconsistencies in a candidate's background should not be seen as rude, but rather prudent, considering the importance of the cybersecurity role. Also, don't forget basic vetting of a candidate's references.

4. Watch your wallet

The cybersecurity field is ever-growing, and compensation is continuing to create an understandable draw to the industry. Take notice of what a candidate's primary initial concern is. Red flags include the candidate calling out a specific salary target before the meat of the interview even begins, or unusual focus on what the company can do for the candidate, not the other way around.

The cybersecurity field is ever-growing, and compensation is continuing to create an understandable draw to the industry.

5. Know *what's* needed, not just *who's* needed, to do the job well

The landscape businesses operate in today demands a basic understanding of information security, and the lack thereof opens the door not only to traditional logic-based attacks, but to human-based exploits by unscrupulous characters looking for fast cash. Ensuring a basic level of information security knowledge for those hiring officials screening cybersecurity candidates is critical for proper vetting.

Cybersecurity is experiencing immense growth, and that means more opportunities for those willing to devote themselves to the field through education, training and job experience. A small amount of due diligence goes a long way in properly vetting new hires. The five considerations above are a great start. ■

JASON MCDOWELL, *CISSP, is a past contributor.*

An expanded version of this article appears in the April edition of the companion e-newsletter Insights.

Filling in the Gap

One (ISC)² member discovers skills we may not know we lack

BY DR. RICHARD KNEPP, CISSP

IF YOU ARE LIKE ME, you likely are skilled at working with technology and machines, but not so good at managing people and their wide range of emotions, the so-called soft skills. That gap between technical and soft skills could impede the upward trajectory of your career.

DISCOVERING THE GAP

Like any good project manager, start with a gap analysis. Investigate and understand your "emotional intelligence"—how you handle the interpersonal issues at work. Then, recognize where you need to improve.

As security professionals advancing in our careers, we will eventually interact with management and other business leaders, whether briefing on budget requirements, spillages, risk management or other incidents. The book *Emotional Intelligence 2.0*, by Travis Bradberry and Jean Greaves (2009), can help you. It provides an online 28-question self-test called an Emotional Quotient (EQ) Assessment that the authors suggest taking before reading the book. The results of your assessment will provide strategies to help improve your level of emotional intelligence among these four skills:

- Self-awareness
- Self-management
- Social awareness
- Relationship management

These skills are considered crucial by employers, critical for personal and professional development for any security professional hoping to advance in their career. Bradberry and Greaves discuss how each point increase in your EQ may potentially add $1,300 to your annual salary!

LEARNING TO 'READ' EMOTIONS

There is no better expert in nonverbal communications than Joe Navarro, a former special agent for the FBI with more than 25 years of experience in nonverbal communications. Navarro has written several books, including *What Every BODY is Saying* (2008), *Louder than Words* (2010) and *The Dictionary of Body Language* (2018). In addition, he has many interesting YouTube videos where you can see nonverbal communications being decoded in action.

For me, the biggest gap was being able to interpret and use nonverbal signals to determine comfort/discomfort levels in business situations and what may be the cause of this comfort/discomfort level. This was where Navarro helped.

Understanding these comfort levels can increase your EQ. For example, why did that person in the meeting look uncomfortable (concerned/doubtful) when reviewing the budget and what can I do to fix it (make them more comfortable)? Or, "I understand you are very busy, so I'll keep this short," based on their body language—how they are standing next to you.

Nonverbals include what you wear, your work practices, your habits and how they influence others. Are you projecting that you are actively listening? Do you really care? What is your body saying?

Navarro not only focuses on the body language of others; he also focuses on your body language. What are *you* projecting? Nonverbals include what you wear, your work practices, your habits and how they influence others. Are you projecting that you are actively listening? Do you really care? What is your body saying?

These are just some of the soft skills necessary to grow your career. Take the time to fill in any gap you may have with highly desirable interpersonal skills such as communications, reasoning, team coordination and more. It will definitely pay off. ■

DR. RICHARD N. KNEPP, *CISSP, is a business process analyst with Battelle.*

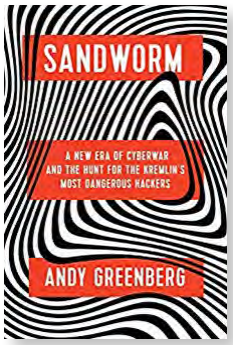
RECOMMENDED READING

Suggested by Andrew Hitt, CISSP, CEH, GICSP

Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers

BY ANDY GREENBERG

(Doubleday, 2019)



THE CAPABILITY of the virtual world to remotely touch and destroy the physical world is recent to the art of war. Presuming that you are reading this online, it is because threat agents haven't yet pressed their enter keys.

For insight into the vulnerabilities of the physical infrastructure that keeps our electricity flowing, look no further than *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, by Andy Greenberg. *Sandworm* details the author's search for the group responsible for cyberattacks that brought down Ukraine's power grid. *Sandworm* reads like a geopolitical spy story. If knowing the risks to our civilization doesn't keep you up at night, the Tom Clancy-ness of the story will.

Sandworm reads like a geopolitical spy story. If knowing the risks to our civilization doesn't keep you up at night, the Tom Clancy-ness of the story will.

The author unravels connections among a trove of secret (but stolen) NSA tools, zero-day vulnerabilities in Microsoft code, malware called Stuxnet, WannaCry and NotPetya, and a cyberattack on the 2018 Winter Olympic Games opening ceremony. You will gain insight into the skills of specialists who disassemble cyber weapons to trace the malware's author. The book describes the method behind a 2007 experiment at the Idaho National Laboratory that, in seconds, remotely destroyed a diesel generator using 140 kilobytes of code. If you are looking for in-depth details on how to write code for hacking tools, *Sandworm* is not for you. It is a survey-level clarion call of the vulnerabilities of the industrial control systems upon which our civilization relies, and the hackers attacking them.

I recommend that you get a physical copy of *Sandworm*. That way you'll have something to read by candlelight when the power goes out in the coming cyberwar. ■

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.

How to Get That Raise

1. Talk salary with your co-workers (yes, it's difficult!).
2. Find out about salaries in the marketplace.
3. Research salary guides and websites.
4. Don't be afraid to negotiate.

"What sets people apart is the people who are willing to do the research to improve their compensation."

—RYAN SUTTON, district president, Robert Half

Source: Information Week, "Want a Raise? Don't Ask Mom and Dad for Advice," *IT Careers: Tech Derives Constant Change*, Feb. 12, 2020

READ. QUIZ. EARN.

Earn Two CPEs for Reading This Issue

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

Note: To access this members-only platform and quiz, you'll need a Blue Sky account. If you don't have an account, go to the Blue Sky home page via the link and click on "Create User Profile" in the upper right-hand corner.

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&ACTION=SI&CatRedirect=10843%7C10843

Getty Images

Protecting Your Cloud Toolchain

by Brandon Dunlap

AS WE HAVE WATCHED DevOps adoption increase as an alternative to waterfall and other development methodologies, security still seems to be an afterthought, testing after deployment. Critical to this trend is the adaptation of security tools, and processes, to protect the toolchain itself, without slowing down the release process. A tall order with more and more developers going "full stack" and owning much of the infrastructure being deployed as well.

With the advent of "infrastructure as code," programmable and able to be configured and deployed with automation, more of the "traditional" skills of IT are being subsumed in software. This shift in delivery means that we need new skill sets in our IT shop.

When I started in this industry, you were either a developer or an infrastructure person. Now those worlds are blurring. How many of your infrastructure team members do you think have the skills of a professional developer and the discipline of their years of practice? The opposite is also true. DevOps teams are often more focused on the security of the software they write than the tools used to do so. However, software can only be as secure as the toolchain used for creation and deployment.

As more and more infrastructure becomes code, secure coding principles must also apply to the scripts that build the automatic configuration, and those source code repositories must be secured. Like source code, the configuration files and scripts used to deploy modern cloud services should be scanned for errors and machine image vulnerabilities.

Brandon Dunlap is a leadership partner for security and risk management for Gartner. He can be reached at bsdunlap@brightfly.com.

Any item of infrastructure that is configurable by text files should have its configuration files centrally stored and version-controlled in a central repository. Eventually, all the infrastructure configuration files must be treated just like application source code, and with the same levels of protection. This includes full version control (with rollback capabilities), as well as auditing, logging, and robust identity management.

Just as we maintain and manage an on-premises data center, the DevOps toolchain is a privileged space, but access to the toolchain is often loosely managed.

Information security management must defend the toolchain from malicious and non-malicious actors alike. As new packages are created and integrated into the development cycle, these images (such as virtual machines, Amazon Machine Images, and containers) should be scanned throughout the lifecycle for vulnerabilities at the operating system, application platform and orchestration layers. These scans must include the correct configuration of the settings of the entire stack according to prevailing practices for secure configuration and hardening.

Information security management must defend the toolchain from malicious and non-malicious actors alike.

Look no further than Uber's 2016 breach.

According to news reports, Uber's developers had published code that included privileged credentials on a private GitHub account. The attackers leveraged those credentials to access the developers' privileged accounts on Uber's network, and also their Amazon Web Services account. The result was the loss of 57 million rider and driver records.

Often, privileged credentials are found embedded in application source code, environment variables, deployment scripts and other tools. As the proliferation of developer tools into the lines of business continues, organizations cannot lag in rolling out identity and access management controls to these tools.

Take the time to inventory the tools being used by the developers, regardless of where in the organization they report, and look long and hard at how the security controls are being applied to those tools, in addition to where and how security testing is being integrated into the build and deployment processes.

This wave is already cresting, but there is still time for information security professionals to get on top of this trend to ensure the integration of security into the development lifecycle, as well as protecting the tools necessary for the creation of value in today's enterprise. ■

Build on your CISSP credential and prove mastery of your domain on your own schedule. Gain flexibility and confidence with **(ISC)² Online Self-Paced Training**.

Take advantage of an online training and exam voucher bundle that **saves you more than 50%** on Official (ISC)² CISSP-ISSAP, ISSEP or ISSMP self-paced exam prep. You can pursue any CISSP Concentration for $1,398.

Bundled Online Self-Paced Training courses include:

- 180 days of access to Official (ISC)² content
- FREE access to CISSP refresher materials
- Exam voucher

Now's your time.

Build for Your Future with a Concentrated Skill Set.

GET THE DETAILS

MAKING YOUR WAY THROUGH THE CLOUD

Who's in control of your cloud security—you or your service provider?

BY ANNE SAITA

IN 2012, a Fortune 500 oil and gas company joined the early adopters migrating assets and business processes to "the cloud." Corporate executives' biggest security concern then was the potential for a rogue administrator from a chosen cloud service provider to pilfer all of its data.

"That was the big fear at the time," explained Jon-Michael C. Brook, CISSP, CCSK, a principal at Guide Holdings who consulted with the company during its initial cloud migration. "They weren't as worried about errors that they might make; they were more worried about the trusted insider within the cloud service provider."

Those concerns haven't gone away, but eight years later a different insider threat is forcing companies to step up their cloud security posture. Today, a cloud-based breach is much more likely to come from an honest mistake rather than malicious attack.

ILLUSTRATION BY TAYLOR CALLERY

This commonplace lapse in configurations, combined with a growing global reliance on cloud services and increasing complexity of cloud infrastructures, is expanding risks and challenging vendor relationships. It's also requiring cloud consumers to "own" their security, rather than rely on providers to carry a greater load.

CLOUD-BASED APPS AND DATA

Commercial cloud usage in recent years has moved up the technology stack, from an early reliance on renting virtual machines and storage space with infrastructure as a service (IaaS) and platform as a service (PaaS), to widespread use of highly scalable software as a service (SaaS). With the new focus on SaaS, application developers are becoming far more removed from default or designed protections.

"If you start doing stupid things, or your supply chain does stupid things, you are at risk. As far as the third- and fourth-party vendors are concerned, you need to have vendor management. That's tough to do."

—JON-MICHAEL C. BROOK, CISSP, CCSK, principal, Guide Holdings

At the same time, organizations are moving from monolithic public and private cloud usage to multi-cloud programs that offer different types of virtual services from a multitude of vendors. The result: serious cloud sprawl, more complex cloud infrastructures and a complicated supply chain—all of which hinder visibility at a time it's most needed.

In FireMon's most recent report on the State of Hybrid Cloud Security, the cloud services industry is expected to grow at three times the pace of overall IT services by the end of 2022. A major driver: digital transformations that promise to improve productivity and drive down operational costs. But the majority (60%) of IT participants in the study admit deployments are outpacing security's ability to place controls around these cloud services.

Then there are data breaches that send shockwaves, like the 2019 Capital One breach that compromised sensitive data on some 100 million customers. Authorities said an apprehended former system engineer at a major cloud computing company was able to gain access by exploiting a misconfigured web firewall application.

That's not to say trust in the cloud hasn't improved. "The cloud's become trusted," Brook said, "to the point that if you haven't made that digital transformation yet, your board is probably asking, 'Why not'?"

He notes that even the U.S. intelligence community now has a cloud. The challenge today is how to handle third- and fourth-party risks as CSPs broaden their offerings through partnerships to meet customer demands.

"If you start doing stupid things, or your supply chain does stupid things, you are at risk," he said. "As far as the third- and fourth-party vendors are concerned, you need to have vendor management. That's tough to do."

Such a program requires data flows to track where all information and particularly sensitive data goes, even to the point of planting fake data to see if it ends up on the dark web. It also requires close scrutiny of service level agreements to make sure they remain realistic and compensate fairly for any losses due to a breach. And, of course, there needs to be a solid incident response plan for if or when there's a service failure.

"With people going into the cloud, the biggest thing as a consultant that I keep seeing is this 'good enough' mentality," said Brook, who also serves as a research fellow for the Cloud Security Alliance. "They take a monolithic VM that they put together 10 years ago and just stuff it directly into the cloud. … It ends up costing more money to not use any of those cloud-native, auto-scale options and it's less resilient."

SHARED RESPONSIBILITY MODELS

Cloud providers have long touted a shared responsibility model when it comes to securing their infrastructure, platform and services.

"Statements pertaining to shared responsibility models that all the major CSPs have published have become a lot more concise and focused on what they provide and what the limitations are in securing services," explained cloud security architect Richard Tychansky, CISSP-ISSEP, CSSLP, CCSP, CAP, CIPP/US and CIPP/G. "They are actually putting in writing what they expect customers to do to secure their environments and protect their data."

This includes where service providers' responsibilities end. "I know the CSP is protecting its physical assets, the servers and network infrastructure, for free. But what they've now made clear is if my organization is offering a multi-tenant application environment [multiple customers using the same application], then I'm responsible for making sure every one of my clients has their data logically

"We need to see more CSPs putting the encryption keys in the customers' hands by default. If that can happen, then I think we'll have better cloud security in the future because customers won't have that question: 'Well who at the cloud service has access to my data?'"

—RICHARD TYCHANSKY, CISSP-ISSEP, CSSLP, CCSP, CAP, CIPP/US, CIPP/G, cloud security architect

separated," and that is a big responsibility, he said.

Tychansky sees more attention now on cloud-based data processing and data storage—and the role of encryption in reducing data exposure. Expect cloud customers to request management of their own encryption keys to minimize risks of data loss, data sharing and subpoena requests.

"We need to see more CSPs putting the encryption keys in the customers' hands by default. If that can happen, then I think we'll have better cloud security in the future because customers won't have that question: 'Well, who at the cloud service has access to my data?'"

CLOUD SECURITY POSTURE MANAGEMENT

Just as cloud usage has exploded, so have security tools to reduce the risks from faulty cloud configuration and administration.

In 2019, Gartner coined the term cloud security posture management (CSPM) to describe a new category of cybersecurity solutions that find and resolve customer-driven cloud misconfigurations. Analysts claim such errors are responsible for almost every attack on cloud services. And, they predict that within the next four years, those that adopt these products will see up to an 80% reduction in cloud security incidents due to misconfigurations.

Gartner analysts also warn that CSPM requires continuous assessments as both cloud infrastructures and applications continually evolve.

In a January 2019 Gartner white paper, *Innovation Insight for Cloud Security Posture Management*, author and analyst Neil MacDonald writes: "As enterprises place more services in public cloud and as the public cloud providers introduce more infrastructure and platform services directly into the hands of developers, it is becoming increasingly complex and time-consuming to answer the seemingly straightforward question: 'Are we using these services securely?' and 'Does the configuration of my cloud services represent excessive risk?'"

Among the paper's recommendations:

- Consider short-term contracts with CSPM vendors until the market is more mature.
- Take advantage of a CSP's internal CSPM capabilities if that cloud use is limited in scope and usage.
- Look to see what CSPM capabilities a cloud security access broker (CASB) might provide.
- Include everyone within a cloud operations team, so everyone has a firm handle on everything being accessed, stored or processed within a cloud management platform.
- Make sure any CSPM strategy includes locating all sensitive data stored in a cloud repository.

While the term may be relatively new, the concept of creating checks on configuration and compliance best practices and industry standards is not. But what a CSPM solution can do is provide that nudge to beef up requirements and elevate individual accountability.

"I think it's got potential," Brook said. "It's something where I expect the AWSes, Microsofts and Googles will come out with their '80% is good' version. They're already doing it from the perspective that they're already telling you, 'You have auditing capabilities out there.' AWS has their inspector products, and Microsoft and Google offer something similar that tells you what the found issues are, but they don't yet clean them up.

"I think we may get to that point where they do provide this by buying a CSPM provider. Or maybe they don't because it's too complicated, or they don't want to go down that multi-cloud route and just leave it to other people," he continued. "I don't think the big guys are going to get to the point of not allowing the company to have the machete on the table and if you hack your fingers off, it's your fault. At some point they will make you put the machete in the closet and lock the door."

Tychansky's view of the CSPM term is that it is more "fast fashion" and in response to a marketing trend than anything, but the concept—to instrument security controls into cloud-native applications in order to better measure cloud security posture over time—is important and will persist in one form or another based upon demand.

"If we have instrumentation built into applications and [micro]services, then we can better manage and monitor

application security controls in the cloud. Security instrumentation is where I'm predicting the technology will evolve," he said.

He likens these instruments to nano agents built into applications that then act as sensors. "In the future, when organizations deploy to the cloud, security architects will specify the placement of sensors throughout the environment, including within cloud-native applications and storage. Everyone from system reliability engineers, to auditors, to incident responders will have the telemetry data that they need to measure the security posture of the cloud configuration and the health of the services. Sensors will facilitate alerting in real time based upon anomalous behavior and well-understood application threat models defined in code."

"Cars and airplanes are built to safety standards, but we haven't built the cloud to a single safety standard that we all agree on despite the work of several standards-setting organizations," he continued. "Right now it's a shared responsibility model, and CSPs have limited their liability." For small, medium and large organizations that means they need qualified security personnel even more than they did for their on-premises solutions.

He continued: "We don't do a good enough job of creating security architectures with this notion of building in by default sensor instrumentation into cloud deployments. Many years ago we started to do with that with intrusion detection and prevention systems, but many cloud-native services today lack any form of automated instrumentation. And that's something we can do at very low cost. We can re-architect to build in these sensors into cloud-native applications…that's where hopefully we can see some change."

And for those very early in their digital transformation? Brook recommends starting small. That oil and gas company mentioned earlier first moved a lunchtime application into the cloud. It let employees know what was being served in the cafeteria that day. "It's low risk, so they had time to get it right," he said. "These are still greenfield opportunities." ■

ANNE SAITA *is editor-in-chief of* InfoSecurity Professional.

BUILDING A HARDENED CONTAINER INFRASTRUCTURE

Has your security posture adapted to containerization?

BY MATT GILLESPIE

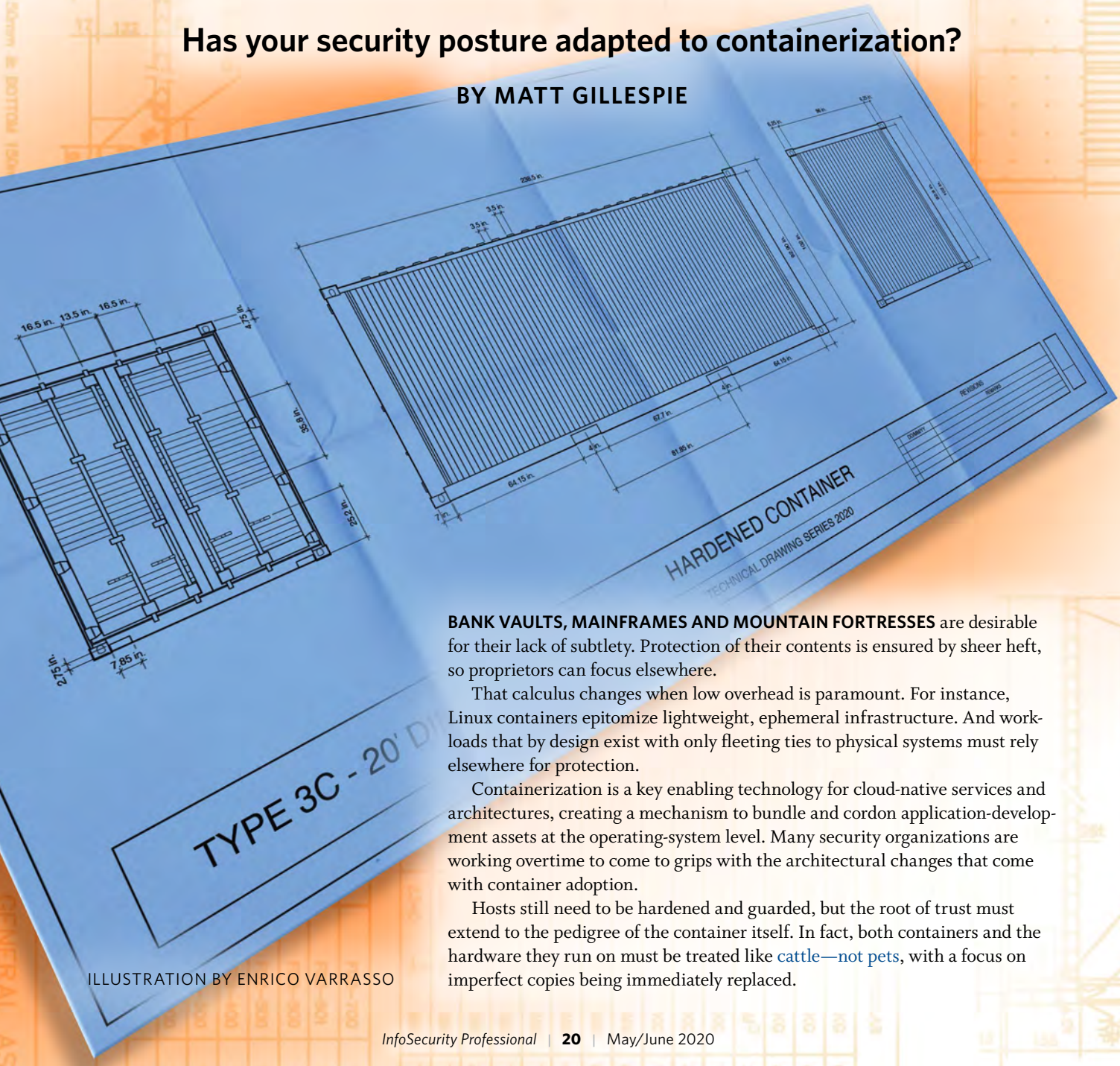


ILLUSTRATION BY ENRICO VARRASSO

BANK VAULTS, MAINFRAMES AND MOUNTAIN FORTRESSES are desirable for their lack of subtlety. Protection of their contents is ensured by sheer heft, so proprietors can focus elsewhere.

That calculus changes when low overhead is paramount. For instance, Linux containers epitomize lightweight, ephemeral infrastructure. And workloads that by design exist with only fleeting ties to physical systems must rely elsewhere for protection.

Containerization is a key enabling technology for cloud-native services and architectures, creating a mechanism to bundle and cordon application-development assets at the operating-system level. Many security organizations are working overtime to come to grips with the architectural changes that come with container adoption.

Hosts still need to be hardened and guarded, but the root of trust must extend to the pedigree of the container itself. In fact, both containers and the hardware they run on must be treated like cattle—not pets, with a focus on imperfect copies being immediately replaced.

At the host level, visibility and scanning monitor ongoing health of the physical system, the virtualization layer (if any) and the base layer of the container infrastructure. By running containers only on infrastructure that is verified to be in a known good state, you can preclude uncontrolled code beneath the level of the containers themselves.

Likewise, the only containers allowed to run must be those verified to be in a known good state. Because they are built to be spun up and down in seconds, very little overhead comes from destroying and replacing an imperfect container.

DEFINE THE EMERGING PRESENT WITH AN IMMUTABLE, GOLD-STANDARD CONTAINER IMAGE

Maintaining a trusted operating state for containers requires the perspective of the container's full lifecycle. The trustworthiness of every container in the environment is based on comparison to its corresponding certified container image.

Base images are built to meet gating criteria such as being limited to specific versions of specific software packages, with measures such as security scans and vulnerability analysis also performed at build time. Once the container image has been verified to be safe and meet the applicable criteria, it is certified as trusted and then cryptographically signed.

Signed images are used as the basis against which to measure containers in production. At deployment time, mechanisms such as The Update Framework (TUF) and Notary can authenticate and verify each individual container.

Travis Jeppson, engineering site lead at Kasten, which provides application backup and recovery for Kubernetes, notes how that approach protects the environment. "Once you get to your production system, that image has been scanned, it's been signed, and you can actually tell your servers to only accept signed images. That enables you to only run software that you trust."

Assurance that containers in deployment continue to conform to the corresponding trusted images must be passed to the runtime environment. Tools such as Falco enable runtime threat detection by monitoring container operating state and detecting unauthorized changes.

"If that state does change," Jeppson explains, "you can remove that container and replace it with a new container from the same image that you've signed and verified, to remove that risk out of your infrastructure."

This model represents a shift from the traditional focus of protecting workloads by identifying malware or other attacks to one that identifies abnormalities as quickly as possible and eliminates them by replacing them with trusted equivalents based on verified images.

In environments where code commits and container deployments occur continually—perhaps as frequently as hourly—registry visibility and hygiene are also critical. Security organizations must be able to track the contents of the registries, as well as the age and vulnerabilities associated with each.

"If that state does change, you can remove that container and replace it with a new container from the same image that you've signed and verified, to remove that risk out of your infrastructure."

—TRAVIS JEPPSON, engineering site lead, Kasten

For example, if a particular container image hasn't been updated in six months, the security team can work with application owners and development teams to determine whether the image should be removed from the registry or perhaps updated in the next sprint cycle.

Notably, these same principles apply both to on-prem and public cloud infrastructure. For example, cloud service providers can provide trusted infrastructure and services, including verification for regulatory frameworks such as PCI, but customers are responsible for protecting the software layers they run on top of that.

Thus, content trust based on signed images is equally important, regardless of where the containers are deployed.

TAILOR THE ARCHITECTURE TO THE DEGREE OF CONTROL NEEDED

The early iterations of container deployment by many organizations use hypervisor-based virtual machines. That approach is familiar and well adapted to the public cloud environment, where it bolsters data isolation beyond what's possible with containers alone.

Jeppson explains the appeal of this approach to many customers in the public cloud, "where the physical hardware is still going to be shared, but you can leverage the properties of the virtual machine to [help] prevent break-ins and break-outs."

Notwithstanding the advantages of that protection, the quest for cost efficiency motivates many organizations away from the overhead of hypervisor-based virtualization. Security solutions architect Sean Nicholson reports that

as customers develop further along their containerization journeys, "they're removing that hypervisor layer altogether, and they're running [containers] directly on bare metal in their data centers or a managed environment such as Amazon ECS or Azure Container Service or Google Container Service."

In particular, managed container orchestration services let customers abstract away management of the container environment, at the cost of ceding control of where specific workloads run. That type of control can allow an organization, for example, to run sensitive or regulated workloads only on a specified, segregated set of servers.

Nicholson likens the adoption of managed Docker and Kubernetes services to what we have seen over the past decade or so with public cloud. Organizations were originally cautious about moving production to the cloud, but "five years later, it's like, 'Oh, I don't need a data center; let them worry about the hardware.' I think the same thing is going to happen with [managed] containers."

Managed container environments vary in terms of what they allow the customer to retain responsibility for, but typically, the control plane is the province of the service provider, giving the customer limited or no control over the container environment as a whole.

> **"We need to foster an atmosphere of working together, starting as early in the process as possible."**
>
> *—SEAN NICHOLSON, security solutions architect*

Conversely, managing your own container infrastructure enables nodes to restrict which containers can be scheduled to run on them. A container can also specify that it will only run on a specific sub-population of nodes.

Together with runtime scanning that allows only containers based on trusted images to run, these measures provide significant protection against malicious containers.

Independent of core architecture considerations such as hypervisor-based virtualization and managed container services, tactical considerations at the per-container level play key roles in protecting workloads. A few representative issues include the following:

- **Embrace automation to protect containers in action.** Because changes in container environments happen at superhuman speeds, humans can't keep up with them. Pinpointing problems automatically enables pulling containers or hosts out of service and replacing them almost instantaneously.
- **Run containers with least privilege.** The common practice of running as root inside of a container can expose not only the container itself, but potentially the host as well, if control breaks out of the container. Mechanisms such as Docker's *user* instruction and Kubernetes' *runAsUser* field help mitigate this danger.
- **Use protection mechanisms built into the container platform.** For example, Kubernetes admission controllers can verify that every request coming into the API is from an authentic, authorized user. Anything else can be blocked, whether it's a nosy neighbor or a cavalcade of crypto-miners.

ESTABLISH A COLLABORATIVE VISION ACROSS SECURITY, DEVELOPMENT AND OPERATIONS

As ever, security teams must navigate carefully to avoid being perceived as roadblocks.

"Developers can tend not to interface with security teams until an application is ready to go into production, and by that time, it's too late. We need to foster an atmosphere of working together, starting as early in the process as possible," Nicholson notes.

Full visibility into development, staging and orchestration pipelines by all concerned parties helps build that spirit of collaboration as security tasks shift left in the development and deployment process, with the emergence of DevOps and DevSecOps approaches in mainstream organizations.

Operationally, the gating factors for what's allowed to run within containers are based on standards established jointly by development and security teams. Those gates provide critical guardrails for what's allowed in the container environment.

To meet business and technical needs, these standards must optimize flexibility, and their enforcement needs to be automated with an eye toward minimizing overhead. Such factors are vital to positioning security teams as enabling container adoption, rather than interfering with it.

Security organizations are well advised to foster partnership with the development organizations and business units responsible for containers and the workloads that operate in them. By building security into every phase of software development and deployment, the organization can be guided by mutual interests at the operational level.

It's possible for everyone to win. Nicholson calls for "agreement between the dev team building images and the security organization that's giving them the thumbs-up to go as fast as they want, as long as they do so within the bounds of these established gates." ■

MATT GILLESPIE *is a technology writer based in Chicago. He can be found at www.linkedin.com/in/mgillespie1.*

OH NO, HE DIDN'T?!

Follow along as a fictitious company faces a cybersecurity professional's worst nightmare. **BY PERRY CARPENTER**

TUESDAY. 3:43 P.M.
ACME CORPORATE HEADQUARTERS

"*Jerry!!!! God, no!* Why'd it have to be *JERRY??!!!*" Mike said to himself as he slammed his laptop shut and took off down the hallway in a dead sprint. Panting as he entered the war room, he said, "We've got another problem."

"Can it get any worse?" Jim, Acme Corp.'s CISO, asked, rather rhetorically. "Frankly, I'm hangry and really need to use the restroom. I don't think I can be held accountable for my actions if you give me more bad news."

"Well, you're *reeeally* not gonna like this," Mike replied. "We tracked it back to Jerry. He was phished."

"Crap!!!" Jim yelled, lightly pounding the desk with his fist. "Why'd it have to be JERRY??!!!"

"*Crap* is right. He got tricked into giving his login info," Mike said as he opened his laptop and pointed to the evidence, suddenly clear as day.

"See *here?* This is where they first logged in using his account and started doing their thing. We're just now getting a better idea of the full extent of what they took, but it looks like the customer info was just the tip of the iceberg."

"Have you talked to him yet?"

"No. I came straight to you. I don't do politics. That's all you, boss," Mike said with a smile and wink.

"Ugh!" Jim sighed, dramatically placing his head in his hands. Then, thinking better of the gesture, he lifted his head, looked off in the distance and began rubbing his temples to mitigate the migraine-like headache unfolding.

"Can I interest you in a battlefield promotion?"

"Nope!"

"Well, ... Crap!" Jim said as he stood and slowly made his way to the office door, first for a pitstop at the restroom before heading to tell Jerry what had happened.

He momentarily stopped before breaching the door's threshold and turned to Mike, his words laden with dread. "How am I going to tell our CEO that he's the source of the biggest security incident we've ever had?"

ILLUSTRATION BY TAYLOR CALLERY

HI! Welcome to a new series on security awareness. My name is Perry Carpenter, and I'll be your commentator as we follow the story of Acme Corporation's woes and revelations. You see, as company personnel continue to evaluate the root causes of the security incident, Mike, Jim, Jerry, and the rest of Acme Corp. are about to realize that simply talking about security isn't enough; they need to build a program that will intentionally shape security-related behaviors and help their employees—from the CEO down—make smarter security decisions every day.

Acme Corp. is like a lot of organizations around the world. Both executives and employees want to follow good security practices and Acme did, indeed, put a security awareness program in place several years ago. In fact, for the last two years they specifically talked about phishing.

So, what happened? What went wrong? The problem was that their awareness program, while well-intended, wasn't well-designed. Acme's program consisted of employee onboarding, yearly training, Cybersecurity Awareness Month activities, policy notifications, breakroom posters, newsletters and more. All good stuff … but not enough and not deployed effectively.

THE ROOT CAUSE OF INEFFECTIVE AWARENESS PROGRAMS

In my time running awareness programs, leading Gartner's research area for security awareness, and helping security leaders around the world debug their own programs, I've come to realize that there a number of factors that most traditional security awareness programs don't account for, and which ultimately limit their effectiveness.

Many traditional security awareness programs fail to account for what I call the *knowledge-intention-behavior gap*. Let me break that down for you:

- **There is a gap between knowledge and behavior:** Having information about something doesn't mean that you'll act on that knowledge.
- **There is a gap between knowledge and even the *intention* to act:** Information alone doesn't lead to caring or the intent to act on the information.
- **And there is a gap between intention and action:** Even when someone cares and intends to act on the information they've received, there is no guarantee that they will act on that information at the moment of behavior.

These gaps exist because there are so many things that compete for our attention and behavioral direction at the exact second that someone needs to *do* the behavior. And

PREVIEWS OF WHAT'S COMING

Over the next few issues, I'm going to take you on a tour of the components of a transformational security awareness program, one that is focused on moving past compliance checkboxes and simple information sharing to practices that are dynamic, learner centric, and will work with human nature rather than against it.

My hope is that you feel equipped, empowered, encouraged, and maybe even entertained by each installment.

Each segment of the series will open with a brief, fictional episode following the adventures of Acme Corporation as it responds to a security incident and begins working through its security awareness and human behavior-related issues.

After the story section, I'll give a breakdown and follow-up to help tease-out any details of the situation and remediation steps and principles. And lastly, I'll leave you with a bit of homework so that you can move from reading to doing.

Here's what's planned for future issues of *InfoSecurity Professional*:

TROJAN HORSES FOR THE MIND

We'll dive deeper into the *knowledge-intention-behavior gap* and the three realities of security awareness and the specific implications that they have on how people learn. I'll get into the specifics of what makes good content and I'll introduce you to four Trojan Horses for the Mind that you can use to subtly influence hearts, minds and behaviors.

BEHAVIORALLY SPEAKING

An introduction to the world of behavior science and behavior design. I'll introduce you to a few behavior models, including the Fogg Behavior Model and Nudge Theory; and I will show you specifically how to use those models to work *with* human nature rather than *against* it.

THE GAME IS ON

We'll cover what we mean by creating a "security culture," including the use of social structures, social pressures, game theory and more to influence the behaviors of diverse groups. ■

—P. Carpenter

so, we may act in ways that completely negate our knowledge and/or intentions.

Don't believe me? Just think about the last time you tried to keep a set of New Year's resolutions for the entire year.

You had things that you knew were important. You may have promised yourself that you were going to exercise more, save more money, eat healthier, have a better work/life balance, or similar goals. You knew the benefits of doing these things and fully intended to act differently based on that knowledge.

WE ALL MAKE IN-THE-MOMENT BEHAVIORAL DECISIONS THAT WORK AGAINST OUR KNOWLEDGE AND/OR INTENTIONS.

But, if you are like most people, it's very likely that the behavior didn't follow! I'm not trying to be harsh or to shame you. I'm merely pointing to a reality; We all make in-the-moment behavioral decisions that work against our knowledge and/or intentions.

Out of the *knowledge-intention-behavior gap* flow three realities of security awareness. They are:

1. Just because I'm *aware* doesn't mean that I *care*.
2. If you try to work *against* human nature, you will *fail*.
3. What your employees do is way more important than what they *know*.

We'll explore these realities, as well as their implications and resolutions, a few different times as they present themselves in the next installments of this series. These three realities impact everything from the way that you choose or create information-based content, to the security- and non-security-related technologies that you purchase, to the policies you create, the behaviors you reasonably expect, and the metrics you value.

Ultimately, I'll show you how to build a program that accounts for human nature, helps to shape behavior (even when the user is unaware), and also has the potential to drive greater engagement with your users. Maybe the best level of engagement you've ever seen. ■

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

YOUR HOMEWORK

OK. Now that you have a sense of the root cause of most ineffective awareness programs and you know where we are going, I've got some homework for you.

1. Evaluate your current security awareness program. Does it account for the *knowledge-intention-behavior gap* and the *three realities of security awareness*? Identify what your program currently does well and what it does not do well.
2. Take a good hard look at the policies and technologies that your end users are expected to interact with. Do these account for the *knowledge-intention-behavior gap* and the *three realities of security awareness*? Note your findings and thoughts.
3. Review the content (videos, newsletters, posters, learning modules, etc.) that your program uses. Is your content interesting? Does it feel current and relevant? Is it targeted to different roles and user populations? Be gut-level honest with yourself about their quality and ability to engage your end users.
4. Begin identifying three to five end-user behaviors that can, if adopted, have the greatest security benefit to your organization.
5. Start thinking about how your organization as a whole values security. What basic attitudes, perceptions and behavior patterns do you note? What variances (positive and negative) do you see between different departments, regions, etc.? Record your thoughts. ■

—*P. Carpenter*

HAVE A QUESTION FOR PERRY?

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

(ISC)²

Build Skills and Earn CPEs

Seeking more ways to keep cybersecurity skills sharp and knowledge fresh? (ISC)² Professional Development Institute (PDI) has you covered with the flexibility of online, self-paced courses. Dive into our portfolio of over 30 online courses – **free for (ISC)² members** and available for purchase by non-members. Build skills and earn 100+ CPEs, no travel required.

Stay on top of your craft with…

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

Start FREE Courses

To receive communications when new courses are released, add Continuing Education and Professional Development to your preferred communications at isc2.org/connect.

THE INTERPLAY OF SECURITY + PRIVACY

To comply with data privacy laws around the globe, the two disciplines must work together, even when their work conflicts

BY JUSSI LEPPÄLÄ, CISSP

THERE'S A GLOBAL MOVEMENT to improve consumer and other data privacy through legislation. In the two years since the EU General Data Protection Regulation (GDPR) went into effect, tens of information privacy laws have been debated and/or adopted around the world. The challenge now is for cybersecurity and privacy professionals to keep up with expectations around the world.

ILLUSTRATION BY ROBERT NEUBECKER

A 'FINE' EXAMPLE OF ENFORCEMENT

More than 170 EU General Data Protection Regulation (GDPR) fines were publicly known by the end of 2019. A substantial number were related to security breaches: 45 of the fines explicitly mentioned Article 32 of the GDPR, Security of Processing, while eight mentioned Articles 33 or 34, which set requirements about handling data breaches.

Often, a data breach will lead to a closer inspection of the organization's privacy and security practices. While the enforcement practices are still developing, we have already seen substantial announcements. The British Information Commissioner's Office announced its intention to fine British Airways £183.39m (about US$240 million) for the data breach the airlines suffered in September 2018.

Corporate information security and data privacy functions are natural allies. There is no privacy without security. Sometimes, security and privacy even fall under the responsibility of the same organizational unit.

Several data privacy laws set direct requirements on security measures for protecting personal data. There may also be sanctions for personal data breaches or failures to implement proper security controls.

However, security and privacy are only partially overlapping. Data privacy covers the handling of personal data, while security controls are used to protect all kinds of data.

Privacy laws define principles and rules, often including individual rights and processing fairness that go beyond security measures. Therefore, there is an inherent tension between privacy and security: some security controls may be considered too intrusive or even unlawful in some privacy jurisdictions.

This makes it a challenge for security and privacy professionals in a global organization to implement security measures and remain compliant with all relevant privacy laws yet remain efficient and effective in terms of security.

INFLUENTIAL PRIVACY LAWS

More than 130 countries had information privacy laws in force in 2019. This number has grown rapidly during recent years. There are also several other nations with newly proposed privacy bills still in the legislative process. Most of these laws are comprehensive; they affect every sector of society.

Some countries, like the United States, have enacted only limited sectoral laws, with no federal legislation for everyone to follow. While protecting consumer information is considered important, most comprehensive privacy laws apply equally to other types of personal data as well, including employee data and business-to-business contact information. Therefore, it is common to see a privacy program and a full-time data protection officer in an organization without consumer customers.

One of the most influential laws to date has been the GDPR, which directly applies in all 27 EU member states. GDPR's reach, however, extends well beyond EU borders. Consider the following:

- The Brazilian General Data Protection Law, LGPD, and Thailand's Personal Data Protection Act are examples of upcoming data protection laws that read similarly to GDPR.
- The Japanese Act on the Protection of Personal Information, APPI, was supplemented to offer "essentially equivalent" protection for personal data as GDPR, therefore allowing unhindered personal data flows between Japan and the EU.
- Australia and Canada amended their data protection laws with GDPR-like data breach notification requirements in 2018.
- New Zealand's Privacy Bill is expected to add a similar requirement.
- While in many respects different, the California Consumer Privacy Act, CCPA, shares some GDPR concepts including a broad definition of personal data.
- India's proposed Data Protection Bill also includes elements from the GDPR.

WHAT ARE THE MAIN SYNERGIES?

Privacy laws require good data management practices. In order to be compliant, an organization must know and document what personal information it has. Personal information that is no longer needed needs to be deleted.

These practices also help security: Knowing and documenting your data assets is fundamental for both security and privacy. It is easier to protect information if you don't store information unnecessarily; you cannot lose what you don't have.

Operational requirements for security and privacy are often similar. Responding to a data breach is not fundamentally different whether the breach affects personal data or not. Organizations sometimes define two separate breach processes: (a) by privacy program as required by relevant privacy laws and (b) by security organization.

It is more efficient to have these processes closely aligned or even merged. Right after the detection of the breach, it may not even be clear whether personal data was included or not.

Vendor management is another area where coordination is necessary; many security and privacy requirements for suppliers are the same.

NON-PERSONALLY IDENTIFIABLE INFORMATION CAN BE PERSONAL DATA

One of the difficulties in following global privacy laws is that the definitions related to privacy and personal data vary.

The security community is accustomed to paying special attention to "personally identifiable information" or PII. PII is often limited to information containing direct identifiers like given names, social security numbers or address information. Non-PII data then broadens this narrow definition to device identifiers, IP addresses and cookies. However, GDPR and many other privacy laws explicitly include online identifiers to their definition of "personal data." Therefore, obligations from these privacy laws would still apply.

Similarly, even if a de-identification process is approved in some jurisdiction, it does not necessarily qualify as anonymization in another. GDPR makes several references to pseudonymization as a recommended security measure. Security techniques like tokenization are used for similar purposes, but they do not always fulfill the legal definition of pseudonymization.

SECURITY REQUIREMENTS WITHIN PRIVACY LAWS

Privacy laws include several requirements related to data security.

As previously noted, GDPR's Article 32 is setting requirements about the "security of processing." The article is far less prescriptive than similar requirements in standards like the Payment Card Industry Data Security Standard (PCI DSS). GDPR requires the data controller and processors to implement "appropriate" security measures in relation to the risks of personal data processing. Article 32 lists some measures as examples of good practices including pseudonymization and encryption of data along with the regular testing and evaluation of the security measures.

This is typical for privacy laws across the board: The goal is to create technology-agnostic regulation that applies to vastly different processing scenarios and remains relevant for years. This in turn prevents the drafters from including specific requirements. More detailed requirements exist in the areas of data breach notifications, security documentation, security-related assessments and vendor management.

There are numerous vendors offering privacy manage-

Indicative Data Breach Requirements in International Privacy Laws

Area	Privacy law defining the breach obligations	Separate logging requirement	Notification to authorities	Notification to individuals	Note
EU	GDPR	Yes, all breaches	Within 72 hours when there is a risk to individuals	When there is a high risk to individuals	High sanctions
Brazil	LGPD	No	Within a reasonable time period	Within a reasonable time period	Relatively high sanctions
Thailand	PDPA	No	Within 72 hours when there is a risk to individuals	When there is high risk to individuals	GDPR-like
Canada	PIPEDA	Yes, all breaches	ASAP when there is a real risk of significant harm	When there is a real risk of significant harm	Adds third-party notifications
Australia	Privacy Amendment Act	No	Promptly when there is a risk of serious harm	Promptly when there is a risk of serious harm	Applies only to "covered entities"
Japan	APPI	No	Not a legal requirement but recommended	Not a legal requirement but recommended	Least prescriptive

ment tools that can help in complying with these specific requirements. Before deploying such tools, a proper analysis of the match to the organization's requirements is needed. No tool will remove the responsibility of the organization to understand and implement the requirements.

DATA BREACH NOTIFICATIONS

A personal data breach is a security breach resulting in the accidental or unlawful loss, alteration, disclosure or access to personal data. GDPR and many other international privacy laws have at least three different requirements related to data breaches:

- The organization needs to maintain an internal log of all data breaches.
- If there is a risk to the individuals, the data protection authorities need to be notified.
- If there is a high risk to individuals, the individuals need to be informed as well. Notification time limits vary, with GDPR's 72-hour limit to notify authorities particularly challenging for some organizations.

DOCUMENTATION REQUIREMENTS AND ASSESSMENTS

GDPR requires organizations to maintain records of processing activities. These records must also include a general description of related security measures. Similar requirements can also be found in Thailand's PDPA. The Brazilian LGPD also has a recordkeeping obligation, but it is less prescriptive than the other two.

GDPR also compels data controllers to conduct a data protection impact assessment when a planned processing activity is likely to result in high risk to the individuals. The assessment should include the measures to address the risks, including "safeguards, security measures and mechanisms to ensure the protection of personal data" (GDPR's Article 35). This kind of assessment is likely to require contributions by security staff. Other privacy laws, including Brazilian LGPD, also have similar requirements.

EMPLOYEE MONITORING

Protecting an organization often includes monitoring employees to mitigate insider threats. Sometimes monitoring may be targeted to external threats but affects employees as well. This kind of monitoring can take various forms, such as workplace entrance CCTV or automatic scanning of outgoing email messages. The privacy legislation in an employment context can be very different in different jurisdictions.

Even the more prescriptive GDPR leaves this area open for member states' own provisions. Sometimes employee monitoring is possible only when the employees are properly informed; sometimes work councils need to be consulted.

In Germany, some monitoring activities may trigger works council co-determination rights and the monitoring cannot be implemented without works council approval. Message confidentiality legislation in Finland may prevent the organization from implementing some data loss prevention tools consistently throughout the whole organization. The organization needs to decide on its approach, whether it applies the same process globally or accepts some national variation.

DATA LOCALIZATION REQUIREMENTS AND BUSINESS CONTINUITY

It is not unusual for privacy laws to introduce restrictions or conditions for cross-border data transfers. This is likely to have an influence on data flows and fail-over architectures. Russia's privacy law is one of the strictest in this respect.

Russian data localization law requires covered entities to use databases physically located in Russia to process the personal data of Russian citizens. However, transferring a data copy of such data outside of Russia is typically allowed. GDPR, on the other hand, generally requires a separate mechanism for transferring a copy outside of the EU or countries with "adequate data protection," but it does not include a requirement for a local copy.

These transfer mechanisms include appropriate safeguards like binding corporate rules and standard contractual clauses by the European Commission. The EU-U.S. Privacy Shield self-certification mechanism creates an "adequacy status" for the participating organizations. APEC Cross-Border Privacy Rules facilitate the data transfers within APEC countries. Data architects and business continuity planners must be careful to maintain compliance for all data transfers, also for fail-over sites and backup locations.

PREPARE NOW FOR THE DATA PRIVACY SWEEP AHEAD

Privacy laws are quickly developing around the world, as was predicted when GDPR took effect in May 2018. Wherever you do business, information privacy and security are more essential than ever. Close cooperation between privacy and security teams will facilitate legal compliance and build consumer and employee trust. ■

JUSSI LEPPÄLÄ, *CISSP, works as a data privacy officer for a Finland-based manufacturer. He also is a Fellow of Information Privacy at the International Association of Privacy Professionals.*

A Year in a Day

by Pat Craven

JUST FIVE YEARS AGO, the Center for Cyber Safety and Education (then called the (ISC)² Foundation) was proudly providing about 10,000 cyber safety lessons to children and parents around the world *annually*. On January 28, 2020, we provided our multi-award-winning Garfield cyber safety lessons to more than 10,500 Tampa Bay third-grade students in 106 elementary schools in *one day!*

The Cyber Safety Day Tampa Bay was the third of the Center's Cyber Safety events. The first was in New Orleans, LA, in 2018, where we reached 2,308 students at 17 elementary schools. In 2019, we provided 6,572 third-graders at 56 schools in Orlando, FL, with their first Garfield's Cyber Safety Adventures program. And later this year, 20,000 students in Toronto, Canada, will receive the program thanks to the efforts of the Toronto (ISC)² Chapter.

But there's much more to come. I am thrilled to announce a new partnership with Amazon Web Services (AWS), which has agreed to help bring Cyber Safety Days to cities across the country. Target communities already include Pittsburgh, PA; Orlando and Miami, FL; and New York City, with more being added. You can track where we are going at https://iamcybersafe.org/s/cyber-safety-days. If you don't see your city on the list, please help us get a Cyber Safety Day started there by emailing us at center@isc2.org.

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

The Center's educational reach just keeps on growing! If you add up all the educational programs the Center now offers—in addition to the Garfield program, we also serve teens, parents and senior citizens—last year we provided 143,000 safety lessons around the world. More than 42,000 of those came from our "traditional" Safe and Secure Online presentations that are now available in 24 languages. These are available right now for you to download at www.IAmCyberSafe.org and use for free. Your local library, school or community center would love to have a cyber expert like you to present a training session. Let us know when you do so we can recognize your contribution to next year's totals.

As more people learn about our mission, they want their company, community and family to be a part of it.

The pace of growth we are experiencing with all our programs is exciting. We are essentially doubling our impact every year with no signs of stopping. As more people learn about our mission, they want their company, community and family to be a part of it. We are even exploring how to reduce the cost of deploying the Garfield program in other countries so children everywhere can take advantage of our program.

The best way to keep up with new programs and changes is to follow us on social media, subscribe to our newsletter, and, if you are an (ISC)² member, be sure to opt-in for communications from the Center in your member profile. There has never been a more exciting time to join us! ■

Certification Testing, Risk Assessment How-to's, BYOD Security

The (ISC)² Community has more than 26,000 cybersecurity professionals connecting, sharing knowledge and offering solutions in the online forum. Note that the questions and responses may have been edited for clarity and brevity.

QUESTION:

Is it ethical for training institutions to focus solely on passing the CISSP exam? If a training institution is highly focused *only* on passing the exam, can we be sure that they deliver sufficient knowledge?

—*Posted by Kaveh*

SELECTED REPLIES:

As long as the institution is using the official training curriculum or providing tips and skills to help pass the exam, I do not have a problem. If the training institute is providing "brain dumps" and basically trying to help people memorize the answers, then I do not think that is ethical. And I think that anyone that passes the exam using that method is being unethical and should not be able to earn the certification. Unfortunately, that is a hard thing to police and monitor.

—*Posted by Brewdawg*

Morally questionable forms of educational opportunists are always going to exist, but we can slow them down a bit by taking a cue from the Project Management Institute by requiring a more stringent vetting process along with certified instruction and materials. To do less has only hurt the reputation of the certification in general.

—*Posted by Beads*

I think a training provider's main aim is to get as many people attending their training sessions as possible, as that is how they make their money. How they achieve that is either training people well, which you would think would translate into high pass rates, or training people to pass the exam, which again should result in high pass rates.

Over time, people will learn the style of training the providers offer and choose the provider that suits their objectives.

—*Posted by AlecTrevelyan*

Find this complete thread here.

QUESTION:

I have recently been tasked to perform risk assessment of our organization's data center. How and where to start?

—*Posted by Steve-Wilme*

SELECTED REPLIES:

I suggest you investigate NIST Special Publication (SP) 800-30 Rev. 1 Guide for Conducting Risk Assessments, and SP 800-37, Risk Management Framework for Information Systems and Organizations.

SP 800-30 and 800-37, like all NIST publications, are free. You will have to invest some money for some of the resources, and time in studying them. Although a few ISO/IEC standards are free, many are not.

—*Posted by CraginS*

You can use COBIT 5. Start from asset identification, identifying key business processes, threat modeling and estimating the likelihood and impact, then building risk scenarios. Finally, those risk scenarios will go to the risk register. COBIT 5 is from ISACA but if you Google COBIT 5 risk scenarios and COBIT 5 risk register, there are many samples on the internet.

—*Posted by csjohnng*

Find this complete thread here.

QUESTION:

We have users that visit a lot of external locations and take photos of sensitive data. This is against policy but makes their lives a million times easier. It's so hard to enforce.

I would like to find a solution that ensures the photos are properly encrypted and not uploaded to the cloud—ideally a corporate solution.

—*Posted by GinGa*

SELECTED REPLIES:

My stance has always been, if the company wants you to access the company's IT stuff on a phone, we will give you a phone (or another mobile device).

—*Posted by CISOScott*

How about examining the current policy and modifying it with meaningful and easy-to-use procedures? Policies that interfere with a worker's primary duties guarantee workarounds and subversion.

—*Posted by CraginS*

Does you organization have a corporate security policy that requires Mobile Device Management (MDM), which encrypts all data including photographs? If not, as in our case, you would not be permitted on the corporate network or even the guest internet via Wi-Fi.

—*Posted by Caute_cautim*

Find the complete thread here.

MAKE A REAL IMPACT: VOLUNTEER

Free resources - Over 23 languages available
Parents, senior citizens and youth programs - Earn CPEs

IAmCyberSafe.org

"As (ISC)² members, it is within our responsibilities to increase awareness about cybersecurity in our communities."

- Center Volunteer

CENTER FOR
CYBER SAFETY AND EDUCATION