CCSP AMONG FASTEST GROWING IN APAC

# InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

JANUARY/FEBRUARY 2020

# AI's Next Move

## Elevating the battle between attackers and defenders

PLUS

**CYBER INSURANCE**
What's your policy?

**BRINGING BALANCE**
Leveraging Lean and Agile

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

# LEARN AS AN (ISC)² MEMBER. AND SAVE AS ONE, TOO.

(ISC)²® is committed to providing the information, resources and connections that will empower you in the battle against cyberthreats, which is why members can take advantage of an exclusive $250 discount on a Full Conference Pass for RSAC 2020. Join a dedicated global community for a content-packed week that will deepen your understanding of cybersecurity best practices and emerging trends. Learn from industry experts and thought leaders, discover up-and-coming solutions, and collaborate and network with peers. Register for a Full Conference Pass before January 24 using **code 10UISC2FD** and you'll get your $250 (ISC)² discount PLUS an additional $900 savings off the onsite price—that's $1,150 in total savings!

Get the most out of your membership benefits.

Register today at rsaconference.com/isc2-us20

#RSAC

FOLLOW US

*$900 discount applies to the onsite price.

# contents

VOLUME 13 • ISSUE 1


PAGE 19

## features



Cover image: JOHN KUCZALA  Illustration above: ENRICO VARRASSO

## departments



*InfoSecurity Professional* is produced by Twirling Tiger® Media, 7 Jeffrey Road, Franklin, MA 02038. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)²® on the issues discussed as of the date of publication. 

# The Interesting Origin of CCPA

**ONE OF THE MOST** interesting side conversations I had at October's (ISC)² Security Congress involved the California Consumer Privacy Act (CCPA), which organizations must be in compliance with by this month. If you sell or gather data on Californians, then this new law is likely of interest to you. As the U.S. state with the most residents (almost 40 million) and largest economy (fifth in the world), California tends to be both an economic behemoth and cultural bellwether.

We've written about CCPA in past issues, particularly how it compares to the EU's General Data Protection Regulation (GDPR). Both provide consumers more control over the use of their data and remain a major headache for IT professionals who must re-architect systems and adapt new practices to come into compliance.

Coming on the heels of GDPR, I assumed California legislators wanted their own version to kick off a new wave of data privacy laws. But the act actually began as a way to blunt a ballot initiative floated by a San Francisco developer, a former CIA analyst and a financier. The trio wanted voters, not lawmakers, to force companies to be more transparent and better protect the consumer data they collected or sold as part of their monetization models. Support for the proposed initiative grew after the Cambridge Analytica scandal provided proof that companies like Facebook were surreptitiously exploiting their users.

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

Politicians believed the ballot initiative was seriously flawed and would create chaos instead of clarity around consumer data protections. So, lawmakers and the initiative backers worked together and came up with CCPA—which was drafted and enacted into law in seven days (compared to four years for GDPR).

CCPA is likely to disrupt larger organizations reliant on data brokers and data miners as part of their business models. But even smaller companies may want to reconsider how they treat their data since other states have or will follow suit. ■



## ADVERTISER INDEX

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



InfoSecurity PROFESSIONAL

**(ISC)² MANAGEMENT TEAM**

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

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

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

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

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

**TWIRLING TIGER MEDIA MAGAZINE TEAM**

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

**EDITORIAL ADVISORY BOARD**

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

**SALES**

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

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

# WHAT'S YOUR NEXT CAREER MOVE?


## GET CERTIFIED.

Join (ISC)² at Cloud & Cyber Security Expo
11-12 March 2020 Excel London

(ISC)² members can claim CPEs for attending workshops or educational talks taking place at Cloud & Cyber Security Expo.

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

Register Here

(ISC)²

www.isc2.org

# New Transformative Technologies Only Increase the Need for Cybersecurity Professionals

*by Clayton Jones*

**WHILE APAC CONTINUES** to be one of the fastest growing regions for cybersecurity certifications, the 2019 (ISC)² Cybersecurity Workforce Study also showed that it has the largest skills shortage and the most ground to make up in terms of recruiting new professionals into the field.

Many Asian economies have been investing in the development of IoT platforms, as they are seen as economic drivers. But with this interconnected technology, interwoven into consumer lives, comes concerns about data protection and residency laws. Government and industry in the region have increasingly recognized the important role that cybersecurity plays in the overall success of these initiatives.

Most recently I had the opportunity to visit the Information Security Cluster, a program initiated by the Korea Internet & Security Agency (KISA). The objective of the program is to support startups in the development of information security products and services. The facility also provides an IoT testing and certification environment. The cluster includes security education and competency building as one of its key services. There are similar programs in Singapore, China, India, Australia and Japan, to name just a few.

**Clayton Jones** is managing director for (ISC)² Asia-Pacific. He can be reached at cjones@isc2.org.

The increased volume of devices and solutions in the IoT space is also influencing the development of cybersecurity and data privacy legislation. Laws around data residency and breach notification have been among the first passed, and new ones are currently under review in many economies. The combination of legislative compliance requirements and technology needs has been a key driver for the increased demand for cybersecurity professionals. We crossed the 20,000-member milestone in APAC in 2019, with more than 2,000 members in the economies of Australia, Korea, China, Japan, India and Singapore, and most recently, the Hong Kong SAR (Special Administrative Region).

While the CISSP continues to be the dominant certification, the CCSP has the highest growth rate across regions. This maps directly to the increased adoption of cloud. Regulators have promoted the adoption of cloud even within the critical national infrastructure sectors (which tend to be the most conservative). (ISC)² partnered with NTT to offer the CCSP CBK review seminar in Japanese in 2019 and the CCSP exam will be available in Japanese in the April 2020 timeframe. This will help with the adoption of the certification in the Japanese market as well.

**While the CISSP continues to be the dominant certification, the CCSP has the highest growth rate across regions. This maps directly to the increased adoption of cloud.**

The transformational impact of IoT, along with the spread of 5G, will continue to influence legislation and the cybersecurity space. These developments broaden the threat surface area. And, while the use of AI and security automation increases, the need for well-rounded cybersecurity professionals and specialists will also increase. We will need to constantly upgrade our skills—moving up the food chain. This is why the (ISC)² Professional Development Institute, launched last year, is such a great resource for our members and others to take advantage of. I highly recommend you do. ■

# field notes

EDITED BY DEBORAH JOHNSON

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

## New Offerings from the (ISC)² Professional Development Institute

**FULFILLING ITS COMMITMENT** to bring new courses to the Professional Development Institute in its first year, (ISC)² has recently added another 12 offerings covering a wide arrange of topics, including cloud, pen testing, forensics and much more.

The new courses are valued at $2,850 in training and represent a total of 29 continuing professional education (CPE) credits.

"This broad new set of courses reflects the current training needs of our members based on continued feedback we're getting on the kinds of challenges they face every day in their roles," (ISC)² Education Director Mirtha Collin said.

The new offerings are:

**Immersive Courses**

- Incident Management: Preparation and Response
- Moving to the Cloud

**Express Learning Courses**

- Web Application Penetration Testing
- Practical Intrusion Analysis Using the Diamond Model
- Strengthening Presentation Skills
- Purple Team Playbook
- Techniques for Malware Analysis
- A Security Professional's Guide to AI

**Lab Courses**

- Introductory File System Forensics
- Live Forensics Using GRR
- Introduction to Memory Analysis with Rekall
- Introduction to Memory Analysis with Volatility

For full descriptions and enrollment information, go to https://www.isc2.org/Development.

### Have you updated your contact information?

WHEN YOU BECAME A MEMBER OF (ISC)², you agreed to keep your contact information and other relevant data current. Some of you have moved on to different places and positions, but forgot to reflect those changes in your account. Please take a moment to make sure your contact information—email, phone, etc.—is up to date.

## Spanish-language Webinar a First for (ISC)²

**From left, Wilson España, Jefferson Gutierrez and Richardo Céspedes recording the LATAM Spanish language webinar.**

To make the message and the mission of (ISC)² available to more cybersecurity professionals, the Latin American (LATAM) regional office has produced its first Spanish-language webinar.

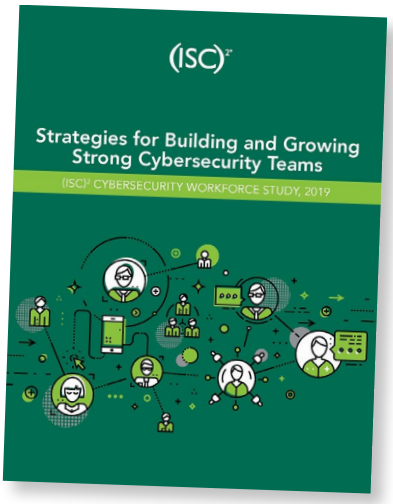
"Un día en la vida de un CISSP" ("A day in the life of a CISSP") is moderated by Ricardo Céspedes, a CISSP instructor. He is joined by Wilson España and Jefferson Gutierrez, members of the (ISC)² Advisory Council for Latin America. In an informal discussion, the three offer insights about their careers, the daily challenges of the profession, and the importance and value of the CISSP certification.

The shortage of cybersecurity professionals in countries such as Chile, Colombia, Mexico and Brazil is also discussed, emphasizing the importance of certifications as a competitive advantage for practitioners and companies around the world.

The LATAM office is very excited to offer webinars in Spanish and looks to expand the offerings in the future. To check out the full webinar, click here.

# Highlights from the Most Recent (ISC)² Cybersecurity Workforce Study

The talent gap is widening, and certain certifications are gaining ground. Here are some of the key findings in the latest workforce study released in November 2019.




## TOTAL CURRENT CYBERSECURITY WORKFORCE (EST.)

| | |
|---|---|
| Worldwide | **2.8 million** |
| U.S. | **805,000** |

## THE CYBERSECURITY GAP BY REGION

| | |
|---|---|
| APAC | **2.6 million** |
| LATAM | **600,000** |
| North America | **561,000** |
| Europe | **291,000** |

## TOP FIVE SECURITY CERTIFICATIONS HELD

1. **CISSP**
2. **CISSP with concentration**
3. **CCNA Security**
4. **CCSP**
5. **CCNP Security**

## IMPACT OF CERTIFICATIONS ON SALARIES

| | |
|---|---|
| Average salary **with** certification | **$71,000** |
| Average salary **without** certification | **$55,000** |

## THE CYBERSECURITY GAP (EST.)

| | |
|---|---|
| Worldwide | **4.07 million*** |
| U.S. | **500,000** |

**39% increase from last year*

## TOP JOB CONCERNS AMONG CYBERSECURITY PROFESSIONALS

| | |
|---|---|
| Lack of skilled/ experienced cybersecurity security personnel | **36%** |
| Lack of standard terminology for effective communication | **28%** |
| Lack of resources to do my job effectively | **27%** |
| Lack of work-life balance | **24%** |
| Inadequate budget for key security initiatives | **24%** |

## CYBERSECURITY PROFESSIONAL'S EDUCATION LEVEL

| | |
|---|---|
| High school diploma | **12%** |
| Associate's degree | **11%** |
| Bachelor's degree | **38%** |
| Master's degree | **28%** |
| Doctorate/post-doctoral | **10%** |

## A YOUNGER WORKFORCE

*Cybersecurity professionals by age*

| | |
|---|---|
| Gen Z (under 25) | **5%** |
| Millennials (25-34) | **32%** |
| Gen X (35-54) | **52%** |
| Baby Boomers (over 55) | **10%** |

The global cybersecurity workforce will need to grow by **145%** to meet the demand for cybersecurity professionals. The U.S. workforce alone will need to grow by **62%**.

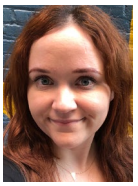
# (ISC)² Salutes the 2019 Information Security Leadership Awards (ISLA) Winners

## (ISC)² ISLA AMERICAS AWARDS

*Up-and-Coming Information Security Professional*
**Tomiko K. Evans**
Awarded to a "rising star" in information security based on performance in current position or educational work.

*Community Awareness*
**Andrés Velázquez, CISSP**
Awarded for a "significant contribution" to building or broadening security awareness.

*Information Security Practitioner*
**Anna Harrison, CISSP**
Awarded for implementing or managing a component of a security program.



*Senior Information Security Professional*
**Cassio Goldschmidt, CSSLP, CCSP**
Awarded for "significantly contributing" to the information security workforce through leadership.

## (ISC)² CHAPTER RECOGNITION AWARDS

Awarded to the regional chapter that best promotes the vision of (ISC)² by inspiring a safe and secure cyber work through the core focus areas of the (ISC)² Chapter Program of Connect, Educate, Inspire and Secure.

*Asia-Pacific (APAC): Singapore Chapter – Chapter President*
**Matthias Yeo, CISSP**

*Europe, Middle East, Africa (EMEA): North East England Chapter – Chapter President*
**Robin Fewster**

*North America (NAR): Central Florida Chapter – Chapter President*
**James McQuiggan, CISSP**


*Latin America (LATAM): Chile Chapter – Chapter President*
**Felipe A. Castro, CISSP**

## (ISC)² BOARD AWARDS

Awarded to honor and distinguish a select number of elite security professionals who have made outstanding contributions throughout their careers.

*Fellow of (ISC)²*

*Fellow #1*
**Ezequiel M. Sallis, CISSP**

*Fellow #2* *(Given posthumously)*
**Michael Assante**

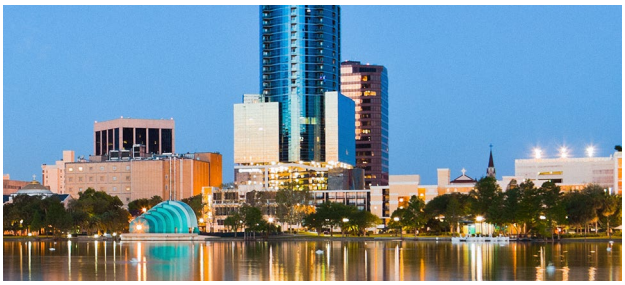
*(ISC)² Harold F. Tipton Award*
**John Sherwood**
A lifetime achievement award to recognize the lifelong contributions to the advancement of information security.

*James R. Wade Service Award*
**Felipe A. Castro, CISSP**
Awarded to acknowledge the involvement of volunteers for their sustained and valuable service to (ISC)².

*(ISC)² Diversity Award*
**Mari Galloway, CISSP**
Awarded to recognize the significant contributions in driving a more diverse workforce in the cybersecurity community.

# (ISC)² Security Congress Moves to November in Orlando

**THIS YEAR'S** (ISC)² Security Congress will again be held in Orlando, Florida, but a little later in the year. Mark your calendars now for November 16 through 18 at the Hyatt Regency. Registration opens this spring. For now, here are some highlights of the most recent global conference held last October at Walt Disney World's Swan & Dolphin Resort. A big thank you to everyone who attended, presented and volunteered to make this one of the best cybersecurity conferences to date.



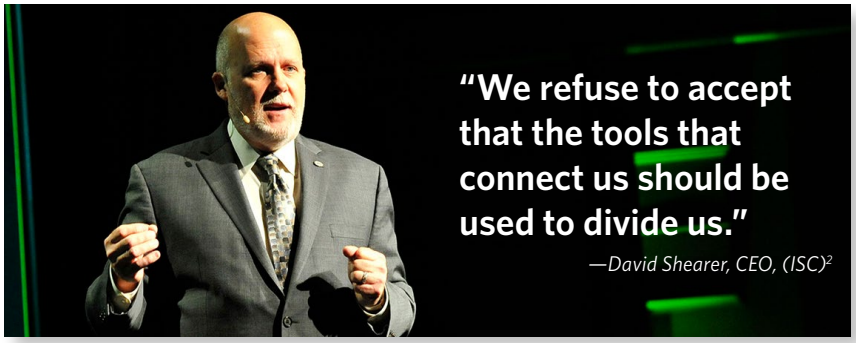


Photographs by David Joel

# (ISC)² Security Congress 2019 – Memorable People with Memorable Words

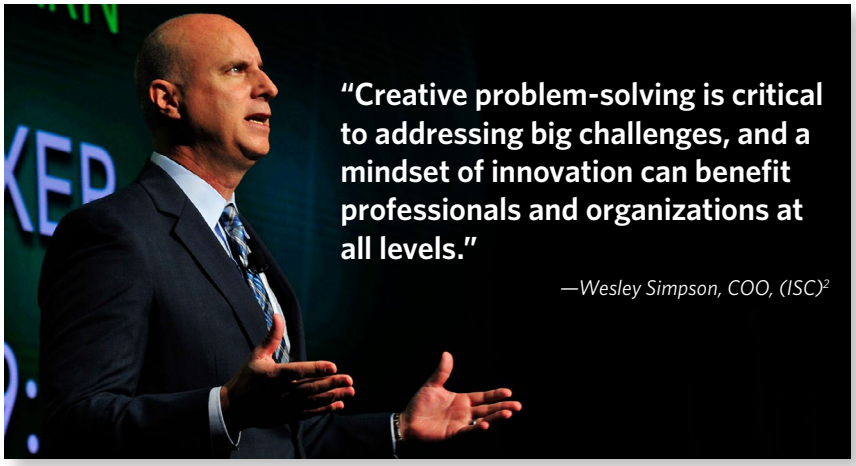
**William H. McRaven**, a retired U.S. Navy four-star admiral, a former SEAL and the commander of the operation that killed Osama bin Laden. In a blow-by-blow description of the rigors of SEAL training, Adm. McRaven stressed teamwork. When it comes to taking a small boat out into the ocean over the pounding surf, he said you learn one thing very quickly:

## "You can't paddle that boat by yourself."

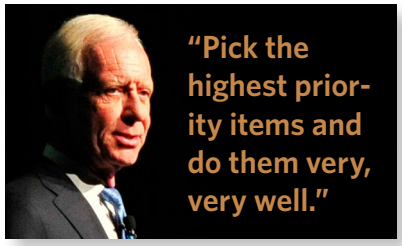



Author **Catherine Price** believes that we are "addicted" to our phones and that our phones have "taken over." They reduce our productivity, increase stress and negatively impact our enjoyment of our lives. Distancing yourself from your phone isn't easy, she said in her keynote. "Cold turkey doesn't work." Here are five steps she recommends to "break up with your phone."

1. **Have fewer apps on your home screen.**
2. **Use bland wallpaper instead of family photos for background images.**
3. **Get rid of addicting practices, such as constantly checking email or social media.**
4. **Eliminate notifications and badges.**
5. **Reduce FOMO (Fear of Missing Out).**




**Capt. "Sully" Sullenberger**, the first keynoter of Congress, shared the ordeal of landing his disabled commercial airplane on the Hudson River. He said that success in crisis requires discipline and clear thinking.



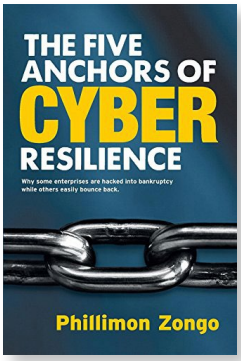

Photographs by David Joel

## RECOMMENDED READING

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

# *The Five Anchors of Cyber Resilience*

**BY PHILLIMON ZONGO**
(CISO Advisory, 2018)




**THE SUBTITLE** to this book captures the theme: Why some enterprises are hacked into bankruptcy while others easily bounce back. Author Phillimon Zongo, an award-winning cybersecurity expert, focuses on the need for resilience and offers advice on how organizations can recover from a breach.

Zongo looks at security as a strategy, not a tool or technique, and zeroes in on five key elements that he believes are required to mitigate a threat. For success, he emphasizes that all five must be present:

- Cost-effective strategies
- Cyber-savvy workforce
- Digital trust in new products
- Effective risk-assurance programs
- Effective governance structures

Guiding the reader to the latest technologies as well as strategies and models to secure and monitor access to data, the author focuses on the business at hand, discussing the impact of a data breach from the points of view of financial markets, customers and the "bottom line." It is a strategy that will cover new technologies and is applicable to all types of firms: large, medium and small.

"Cyber risk is a business risk, not a technology problem," Zongo asserts. There is no "magic bullet," he reminds us. *The Five Anchors of Cyber Resilience* is a user-friendly reference and will prompt the reader to ask pointed questions to strengthen access controls throughout their organization. ■

*The author of Recommended Reading did not receive financial compensation from the book publisher, nor a free copy of this book. All opinions are his alone.*

READ.
QUIZ.
EARN.

### Earn Two CPEs for Reading This Issue

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

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

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&P-CAT=7777&ACTION=SI&CatRedirect=10835|10835


## Cybersecurity Issues Facing Us

Cybersecurity is complex; so are the issues its practitioners anticipate as most important in the coming year. We asked attendees at the 2019 (ISC)² Security Congress in late October what most concerned them going into the new year. Here's a sampling.

The ever-expanding world of IoT and the lack of controls:

**"There will be regulation eventually. It will be the government or a large commercial entity that drives it. If you're writing the standards, you're in charge."**

*—Brent Kelley, VMware*

The need for better communication between technology practitioners and their management:

**"People in the [cybersecurity] profession struggle with relating to business. They're too involved with technology. We need more communication with business leaders on their terms."**

*—Bill Campbell, Predictable Solutions*

The dangerous lack of basic skills of data safety:

**"The fact is people are doing things that are 'unclean' and that were instinctive 10 years ago. I go into shops and find people are no longer using antivirus software! We've forgotten the little stuff."**

*—Michael Weisberg, Garnet River*

To read more predictions, visit the December 2019 issue of *Insights*, our companion e-newsletter. ■

# Signal to Noise Ratio: Machine Learning's Impact on the SOC

*by Brandon Dunlap*

**WITH THE RAPID ADVANCES** being made in machine learning and artificial intelligence (AI) and the democratization of these capabilities through cloud providers, it is easier than ever for anybody to build and run their own models at great scale. This is becoming increasingly evident in the security space as we are seeing escalated use of these terms in marketing materials and new product launches. However, this comes with some risk.

Earlier this year, I was having lunch with a colleague who said they were working on eliminating the need for Tier 1 security analysts through machine learning. This thought came back to me during an (ISC)² 2019 Security Congress preview webinar on security automation when Winn Schwartau said, "Data is everything when it comes to AI. Absolutely everything. When you train a machine, you're training with a dataset, and the question comes up: How valid is that dataset? How neutral is that dataset?"

The problem with replacing Tier 1 analysts with machine learning models is that the models themselves are only as good as the training data. What is missing is context. On that same webinar, Dr. Chuck Easttom said, "Machine learning does not give you definitive answers. It gives you probabilities." It is these probabilities and the possible bias that they hold that needs to be checked by real people, people with the context of your business.

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

Imagine a user that suddenly starts coming in three hours early. They are hitting internal file shares they have never used before and downloading and printing massive quantities of information. Is this a legitimate threat? Are they a corporate spy? Maybe, just maybe, they actually have been reassigned to a new project and are being a good employee by putting in the extra time to ramp up on the project they just joined. Relying solely on the data you are feeding your models, you may not be sure. Are you pulling internal transfer data from human resources? Are you tracking user activity as it relates to projects spinning up? Are you just profiling your users and handing them up to Tier 2 analysts without first contextualizing the situation?

**It is these probabilities and the possible bias that they hold that needs to be checked by real people, people with the context of your business.**

Without properly vetting your models, ensuring useful and accurate datasets during their training and continuing to follow up on those probabilities, security professionals run the very real risk of focusing on the behaviors and users who pose little or no threat. This could create a very hostile user environment if these false positives start triggering HR events.

Make sure that your training data offers a holistic view of the environment, including the human factors, and be aware of the biases that may exist. Context is everything. ■

Image: Grady Reese / Getty Images


# *Achieve More in **2020** as a* CLOUD SECURITY EXPERT

## Take Advantage of Official CCSP Self-Paced Training for ***$749***

It's no secret. The CCSP is the world's premier cloud security certification, consistently topping Certification Magazine's Next Big Thing list as the #1 credential annual salary survey respondents plan to earn.

If CCSP is your goal, now is your time. Prepare for your exam anytime, anywhere – without sacrificing quality for convenience. CCSP Online Self-Paced Training is now only $749. Get:

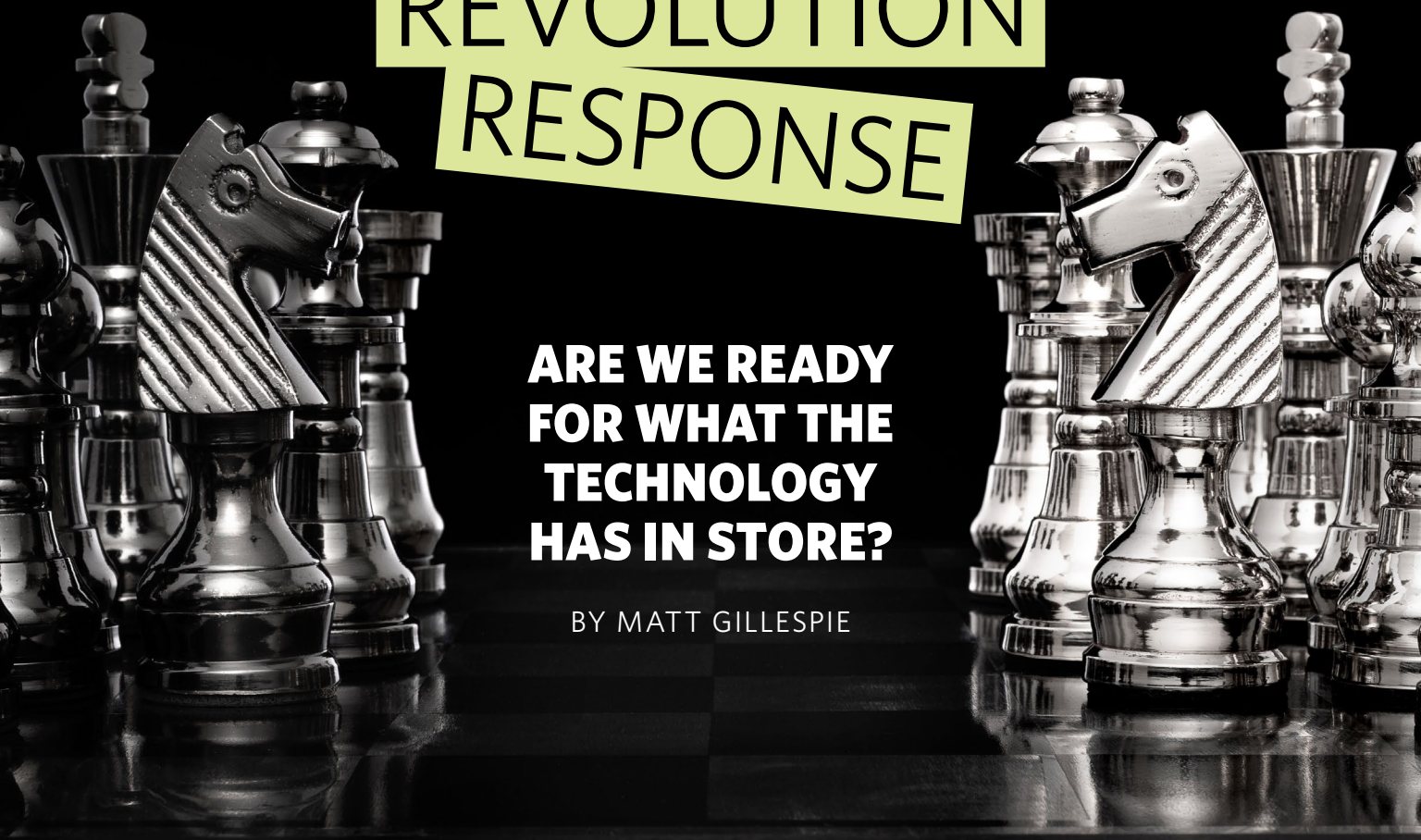
- Access to course content and recordings for 120 days from time of purchase
- More than 100 pre-recorded videos totaling over 10 hours of expert instruction
- Official (ISC)² Student Guide (electronic format)

**GET STARTED**

**STAY MOTIVATED. COMMIT TO YOUR EXAM DATE TODAY.**

# NEXT MOVES FOR AI

## EVOLUTION
## REVOLUTION
## RESPONSE



### ARE WE READY FOR WHAT THE TECHNOLOGY HAS IN STORE?

BY MATT GILLESPIE

**WE ARE IN A PROTRACTED MOMENT** when artificial intelligence (AI) is everywhere, without having yet truly emerged. No discussion of security is complete without mentioning it, but it's always dominated by the future tense.

For the moment, machine learning has improved mainstream defensive solutions, and this one time, the upright citizens have gotten out ahead of the criminal horde.

Beyond those first steps, hype cycles and marketing promises, the era of AI in cybersecurity has not yet arrived. But it's unmistakably on the horizon, and it promises to completely redefine both attacks and defenses in the next several years.

IMAGE BY JOHN KUCZALA

John Dickson, a principal at Denim Group, regards the current crop of breathless claims about AI in security to be something of an irrelevant distraction. "The promise right now outweighs the delivery, but stay tuned," he says. "The promise is too compelling to ignore."

Of course, the shadow side of that promise is that malicious use of AI will develop on a parallel track to its application in defenses. The game is about to change.

## EVOLUTION

### Stronger and sharper, but also the same

Alex Holden, the founder and CISO of Hold Security, likens the present state of machine learning and AI in cyber defense to that of a calculator in a calculus class: it doesn't do the work for you, but you couldn't do the work without it.

He points out that we are just getting started, and that will not always be the case. "We want AI to be significantly smarter, where it can understand the [figurative] calculus problem and solve it before we actually think about it, based on the instruction 'any time you see a calculus problem, go solve it.'"

Much of the value of computers is based on deftly manipulating data at scale, beyond what is possible by humans. Getting the full value out of log data, for example, requires automated sifting through massive amounts of mostly worthless information to find relevant security insights.

Machine learning and AI enable the next iteration of that ability, by handling uncertainty and novelty. For example, humans easily get bogged down in even moderate bodies of data. Comparing two 20-digit numbers is easily in our range of capability (although it takes some time); however, comparing two 1,000-digit numbers is untenable.

For a simple computer algorithm, there is little difference between the two tasks, and with the addition of AI, it can also discern significance in those numbers that it hasn't been explicitly programmed to look for.

In the context of cyber defense, adversaries may use crypters to obfuscate malware and hide it from signature-based antivirus systems. Machine learning algorithms can correlate these variations with the known signature to discover disguised malware. On the other hand, their ability to detect truly novel attacks is limited.

Emerging generations of AI will more effectively generalize the behaviors of malware and other attacks to make better inferences about potential danger. Rather than looking for variations on what it already knows—such as a signature—defensive measures are on the cusp of making logical decisions based on recognizing the danger itself, without depending on direct comparison to previous attacks.

Of course, that adaptation is just one side of the familiar escalation of tactics exercised by both sides. Holden explains, "It's not a static adversary. Every time we teach our AI systems something new, the bad guys teach their systems—either using AI or manually—something else."

In fact, we are at the very beginnings of a time when adversaries will commonly use machine learning to search networks for weaknesses. Time is a major hurdle for humans doing this type of analysis; carrying out even rudimentary surveys of many networks and endpoints is prohibitive. Machine learning does not suffer from that limitation.

Likewise, machine learning is well suited to tuning malware abilities to exploit those weaknesses. And well-proven techniques for establishing botnets provide a ready source of distributed computing power that can be applied to run algorithms and train AI networks to do their masters' illicit bidding.

## REVOLUTION

### The silent and instantaneous wars to come

It is a sign of our times that the images of killer robots evoked by AI-powered cyberattacks seem simultaneously absurd and yet vaguely reasonable.

Machine-based attacks and defenses are already commonplace, of course, and with the addition of advanced machine learning and AI, both will become self-directed.

"The good news is that we haven't seen full-blown weaponization yet, but the bad news is that I'm certain we will in the next two to three years," Derek Manky, chief of security insights and global threat alliances at Fortinet, says. That weaponization will dramatically extend the power of attacks.

Today's arms race involves continual updating of code by both attackers and defenders to manually respond to changes made by the other side. With advanced machine learning and AI, manual processes will eventually be replaced. On the attack side, for example, those models will be able to quickly find vulnerabilities that would take humans years to detect.

That adaptability will accelerate the attack and kill chains, and years in the future, their speed and variability will be beyond human comprehensibility, leading to so-called flash wars.

Manky explains: "The idea of a flash war is … two AI systems battling it out—over milliseconds or nanoseconds, everything's over and one side wins." Along with that increased velocity, hundreds or thousands of attacks could be leveled at a single target at once.

The high stakes and unimaginably short time windows of these conflicts make it imperative to change how we

respond to them. Taking advantage of the fact that with intelligence comes deception, AI will enable cyber defenses to wield misdirection as a force.

Evoking the classic movie trope, Manky suggests a "house of a thousand mirrors" approach to slow down these future attack chains and cause attackers to reveal themselves. The idea is for AI-driven defense measures to dynamically generate illusory honeypots that are tailored to the needs of the moment.

This active misdirection could keep attackers boxing with shadows instead of attacking actual targets, making them less stealthy by revealing their intentions, as well as slowing them down by making them less efficient. Because defenders know that no one would legitimately try to access these resources, the attacker tips its hand, which enables the attack to be isolated in the segment of the network where it is located.

Another familiar movie element also plays into the scene: keeping the conversation going with the bad guys in the hostage situation or kidnapping, so you can draw out information and get the upper hand. Specifically, while an attacker is occupied striking out at false targets, defenses gain time to analyze and respond.

## RESPONSE

### The path to adoption passes through your current location

For most security organizations, implementing machine learning and AI measures won't mean in-house expertise at the level of building algorithms or bringing data scientists on board. By analogy, a system administrator doesn't need to be able to write an operating system, although it behooves her to know something of its inner workings.

Continuing the trend of bringing AI and machine learning into the environment as an ingredient in defensive solutions, these technologies for most businesses will simply be aspects to consider when keeping their security postures up to date. "I see that as a viable strategy. AI will be a service or function to be consumed, and less an internal competency to be built," Dickson contends.

The sweet spot in terms of how deeply security teams need to understand the mechanics of AI may be defined in many cases by what's needed to evaluate vendor solutions and claims. It's clearly necessary to vet the claims made by solution providers, and a lack of background can open you up to being taken advantage of. In particular, there is an alarming number of ostensible experts in this field who in reality only have superficial knowledge.

A common danger of placing trust in unqualified parties is a false sense of security. It can be all too easy to believe in—and be placated by—an untested defense initiative, especially one that includes the apparent secret sauce of machine learning or AI.

The true test of the system can come too late, when a security team realizes after a breach that the ostensibly state-of-the-art system it had counted upon was in reality a set of low-end, off-the-shelf algorithms that were never very effective.

Less dramatically, machine learning is computationally intensive, and a poor implementation can drain network resources. To recognize either of these types of dangers and protect the organization from charlatans, there is no real substitute for a reasonable understanding of the technologies.

At the same time, it's not necessary to go head-to-head in a contest of intellect with solution providers. Chuck Easttom, a computer scientist and consultant, points out that, "You don't have to have a great deal of expertise to know if someone else has a great deal of expertise."

For example, the website of a security vendor offering solutions based on machine learning or AI should include papers published on the topics by some of their engineers, as well as biographies that showcase their qualifications.

True experts typically need little in the way of cross-

## AI AND PHRESH PHISH

**MANY** social engineering attacks are inherently low-yield activities. That's why emails promising to transfer vast sums of money from royal widows seem so absurd; the outrageousness immediately filters out the vast majority of targets, hopefully leaving only the most greedily gullible in play.

That smaller sample from the original horde is pared down to the point where the scammers can begin the resource-intensive stage of the process, where they exert psychological pressure through personalized contact.

As AI-driven chatbots become more sophisticated, they will be able to perform that personal contact at scale, addressing more potential victims at once and improving outcomes for the bad guys.

*—M. Gillespie*

examination.

"If somebody really has machine learning expertise and you invite them to tell you about it, they're going to want to talk about it in detail that you don't want to hear," Easttom suggests. "Three hours later, when they haven't stopped and you are ready to jump out a window to end the conversation, you know they're for real."

## PREPARE, PREPARE, FOR SOMETHING WICKED THIS WAY COMES

The details of weaponized AI are obscured in an uncertain future, but the general path is inevitable, just as with the generations of technology that came before. The first waves will be from rarified actors, such as nation-states, but simplification and commoditization will follow, making AI-driven attacks and defenses the new normal.

Easttom likens the proliferation of AI among bad actors to that of physical weapons, with a fundamental change in who wields these capabilities as they evolve from requiring a massive research effort to just a reasonable level of sophistication.

"There have been multiple instances of terrorist groups with anti-aircraft weaponry, because that's something that a single individual can operate," he notes. "A terrorist group can't very well get their hands on a battleship." But the resources to deploy AI aren't immutable like they are for a battleship, and the time will come when it is within reach for individual mainstream attackers.

Looking forward, Easttom says, "The impetus for criminals will be to circumvent machine learning defenses. So, if you're just doing the introductory stuff, you're going to have to go deeper." ■

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

# WHAT'S YOUR POLICY ON CYBER INSURANCE?

BY SHAWNA McALEARNEY


Spooked by the latest wave of cybersecurity breaches? It may be time for someone to underwrite your risks.

ILLUSTRATION BY ENRICO VARRASSO

**PICTURE IT:** Your organization is going about its everyday business and everything suddenly comes to a screeching halt. Frozen computers. No email. No access to files on the network. Nothing. For weeks. You've been hit by a NotPetya cyberattack and will later find that replacement equipment, lost orders and other costs total more than $100 million. Devastating, yes—but you have cyber insurance so it will be OK, right? Maybe not.

Mondelez International, manufacturer of snack brands like Tang, Oreo and Cadbury, filed this claim with its cyber insurance provider, Zurich Insurance, only to be told that it was denied. The reason: The U.S. government publicly attributed NotPetya to Russia, and that, in turn, activated a "war exclusion" in the policy. The case is now being challenged in a U.S. court, with a verdict likely to take years. Claims by other victims and their insurers are also making their way through the courts.

So, does that mean cyber insurance is a waste of money?

"'Cyber insurance doesn't pay claims' is to cyber insurance as 'my cybersecurity tool didn't work so none do' is to cybersecurity," Matt Prevost, the National Product Line Manager for Cyber Products at Chubb Insurance, said at last year's Black Hat conference in Las Vegas.

Industry experts say that many types of breaches have been covered, but it does serve as a cautionary tale to involve your security team early in the process when choosing a policy.

"While some people incorrectly believe that cyber insurance carriers do not pay claims, the truth is that several cyber insurance carriers have helped their clients by responding to and paying the costs for thousands of data breaches," says Jake Kouns, CISO of Risk Based Security, a provider of vulnerability intelligence, breach data and risk ratings. "Some of this misperception comes from cyber claims being reported under property or general liability policies, which were never intended to cover 'cyber' information security events."

At Black Hat, Kouns also spoke on how to integrate cyber insurance into a risk management program. He strongly suggested that security play a role in the process as early as the initial application because of technical language and potential exclusions that could negatively impact your organization if only the finance team is involved.

"Coverage limitations include policy exclusions but are also buried in conditions and definitions," said Jeffrey Smith, managing partner for Cyber Risk Underwriters and presenter on the cyber insurance basics for CISOs session at Black Hat.

**It's important not only for meeting the time-to-report obligations, but also to be sure the full benefits of the policy aren't jeopardized due to use of unapproved service providers."**

*—JAKE KOUNS, CISO, Risk Based Security*

The importance of security's input can't be underestimated in understanding a policy and its requirements, especially when making a claim for a security incident like a data breach. Often, the policy outlines timetables for incident reporting, as well as other specifics that must be followed to protect your coverage.

"The first thing that needs to be done is to contact the insurance company," Kouns says. "It's important not only for meeting the time-to-report obligations, but also to be sure the full benefits of the policy aren't jeopardized due to use of unapproved service providers. Many cyber insurance policies will dictate which IT or cybersecurity providers will be used in the incident process. If an organization has specific vendors they want to or must use, this needs to be investigated with the cyber insurance carrier prior to a claim event."

## REAPING THE BENEFITS

"No level of security can prevent a determined hacker or employee error," Smith says. "But, relative to other types of business insurance, coverage is inexpensive and offers value beyond simply paying claims."

Those benefits can be of tremendous help during a very stressful time. According to Smith, in addition to minimizing the potentially significant financial impact of a cyber event, cyber coverage often provides:

- Services, such as employee training and ongoing network monitoring, to help mitigate intrusions and, therefore, the cost of claims.
- Contact information for a "breach coach" who oversees the claims process.
- Immediate access to legal and technical resources otherwise unavailable to the insured.

Cyber insurance carriers typically run point on handling all aspects of the data breach through their claims process. "They will bring in the appropriate providers, whether it be legal or technical or other resources, as needed based on the type of breach," Kouns explains. "For small to medium businesses that [do not have] IT or cybersecurity experts, having the cyber insurance carrier be their partner guiding them through the event—and for the most part handling everything—is one of the most valuable aspects of having coverage."

## MOST STILL HESITANT

A surprisingly low number of organizations have yet to purchase cyber insurance policies. Cyber Risk Underwriters estimates that less than 50% of organizations carry standalone cyber insurance policies. PwC reports that only 30% of companies have cyber risk insurance or cyber liability insurance coverage, but it believes the current market of $2.5 to $3.5 billion annually will grow by another $2 billion over the next three years.

"Buyers not purchasing the product typically cite lack of exposure, an inability to understand coverage and/or the existence of security tools such as firewalls and antivirus,"

## NICE TO HAVE OR HAVE TO HAVE?

**IS IT TIME** to consider cyber insurance? Join three experts for a roundtable discussion on the topic by viewing the on-demand (ISC)² Think Tank "Nice to Have or Have to Have: The Case for Cyber Insurance."

The webcast, moderated by Brandon Dunlap, includes insights from John Smith, principal security engineer for ExtraHop; Sean Scranton, cyber liability national practice leader at RLI Corp.; and William Boeck, global cyber wordings and claims leader at Lockton Companies.

Learn more: https://www.brighttalk.com/webcast/5385/370761.

Smith says. "We see the uptake improving not only due to more public awareness of breach events, but as a result of the coverage being required by customers and business partners."

When you consider that a breach could affect not just trade secrets or customer or client data, but also employee information, business continuity and reputation, everyone has some level of exposure. Many years ago, a security guru once said a computer was only truly secure if the power and all connectivity were disconnected and that it was locked in a room to which no one had access—hardly a way to do business—so you balance your risks as part of an overall security strategy.

### THE NITTY GRITTY

Cyber insurance usually covers first- and third-party expenses resulting from a cyber event, which is typically defined as unauthorized system access or a privacy breach. "The most prevalent claims result from malware, phishing and unauthorized release of protected identity or health information of others," Smith says.

First-party policies cover the policyholder's expenses, such as legal counsel, computer forensics, lost income due to a business shutdown resulting from a cyber event, notifications, credit monitoring and crisis communication/public relations costs, Smith says. Cybercrime, including extortion consulting and ransom payments, phishing and funds transfer fraud is also often included, as are lost income relating to dependent system failures and brand damage.

Third-party coverage applies to legal actions from individuals, organizations or regulators and pays awards, fines and penalties on the policyholder's behalf, he continues. It also includes claims of defamation and intellectual property infringement arising out of the use of electronic or written media.

So let's talk about costs.

"Cyber insurance premiums vary by size and risk profile," Smith says. "Premiums typically start at $1,000 for a $1 million policy for small business to more than $100,000 for larger, more complicated risks."

Cited examples of pricing structures include a:

- Healthcare clinic with revenues of $75 million priced at $27,000 for a $5 million policy.
- Real estate management company with revenues of $4.5 million priced at $2,750 for a $1 million policy.
- Municipality with 75,000 residents priced at $14,500 for a $3 million policy.
- Hotel management company with revenues of $60 million priced at $16,500 for a $5 million policy.

### WHAT ABOUT RANSOMWARE?

"Ransomware is one of the worst types of events that organizations are facing currently," Kouns says. "While not all cyber insurance policies are the same, the good carriers typically handle the entire lifecycle of a ransomware event from the initial triage of the situation to negotiations to determine if payment is the appropriate action, convert the funds to cryptocurrency and ultimately recover the systems."

Think it won't happen to you? You might be surprised.

"Eighty-five percent of the claims we see involve ransomware or social engineering attacks," Smith says. "The policies provide expert extortion consulting services and pay ransom amounts as decided and directed by the insured and counsel."

Still on the fence about buying a policy? The seemingly ever-increasing costs might warrant a discussion with your C-suite or board of directors.

Companies prefer not to share sensitive information about their breach experiences, and no one publicly states that if they didn't have cyber insurance they would have gone out of business, as that would rattle customer confidence. But, Kouns says, "we are aware of situations where the company has gone out of business due to a data breach. American Medical Collection Agency is a prime example of this unfortunate situation. The response costs alone forced the CEO to take out a personal loan. And by the time the full extent of the event became clear, the company was forced to file for bankruptcy protection." ■

SHAWNA McALEARNEY *is a regular contributor to* InfoSecurity Professional. *She lives and works in Las Vegas.*

HOW TO

Hint: Learn to leverage Lean and Agile

# BRING MORE BALANCE TO YOUR 2020 CYBERSECURITY PROGRAM

BY MICHEL TEUWEN, CISSP


**HERE'S A PREDICTION FOR 2020** that is likely to be proven true any day now, if it hasn't already: Somewhere in the world we're just now learning about a serious DDoS attack, successful phishing campaign, disruptive ransomware attack or reputation-damaging data breach.

If we allow this kind of disturbing news to determine our immediate actions, we are at high risk of being led by day-to-day affairs rather than taking the long view. To prevent that and to ensure we spend our valuable resources on doing the right things correctly and at the right moment, there is a strong need for balance in information security. This can be achieved by incorporating the best of Lean and Agile methodologies.

This approach will result in comprehensive strategic and tactical plans that are practically feasible and have wide support within all layers of an organization. That includes raising security awareness at all levels; providing efficient incident responses; and visible compliance contributing to an optimized audit process.

ILLUSTRATION BY JONATHAN REINFURT

It will facilitate a close relationship with those working at strategic and tactical levels because it enables us to speak "their" business language. This will provide real management commitment as well as easier access to budget and resources. Additionally, it will enable us to clearly explain to line managers, team leaders, developers and engineers at tactical and operational levels, and even end users, why implementing certain controls, processes or functionality makes sense for the business.

When executed and communicated properly, this approach imbues a mind shift for traditional technical-oriented staff. Where they are naturally inclined to set everything in stone, they will now realize that with the business taking ownership, they need to be more flexible and allow for calculated risks.

In essence: Using common best practices from two popular and proven methodologies will bring more balance to your information security program.

## WHY WORRY?

Of course, every organization has its specific security challenges and requirements. Still, there are common issues we encounter at some point in many, if not all, organizations.

*End-of-support/end-of-life systems:* Some systems just cannot be upgraded right now for valid reasons. Sometimes for budgetary reasons, but often because of some kind of dependency on components that will not (yet) run on a new platform. Certified stacks, only supported with a specific combination of software versions among the different components, are another challenge.

*Insecure systems and processes:* At the time of implementation, systems and processes are usually safe and in control. But over time, control is often lessened or lost completely.

*Too many privileged accounts:* Not only the physical administrators, but also service accounts necessary for applications, or system accounts are necessary for an OS to work correctly. When, for the latter, a reduction of privileges is usually hard—if not impossible—to accomplish, the privileges for service accounts are definitely worth investigating. To ensure an application will function correctly, the principle of least privilege may not be strictly adhered to.

*Technical vulnerabilities:* Even if you don't have any technical vulnerabilities today, you will have them tomorrow. Actually, you do have technical vulnerabilities today; you just may be unaware of them.

In many cases technical vulnerabilities have been identified but have not been patched yet. The reason is that a proper patch management process also takes time. Unless a patch is critical enough to warrant immediate action in a production environment, it should follow the regular develop-test-acceptation-production path.

*Insecure user behavior:* This is most likely the biggest threat of all. In most cases it's not malicious, but a user will do just about anything to get a job done. Regardless of the advanced technical solutions and strict approval processes we implement, users *will* find a creative way to bypass these controls just to get that order out the door.

A closely related issue is *insecure passwords*. This is something we almost force on our users. Because who, in

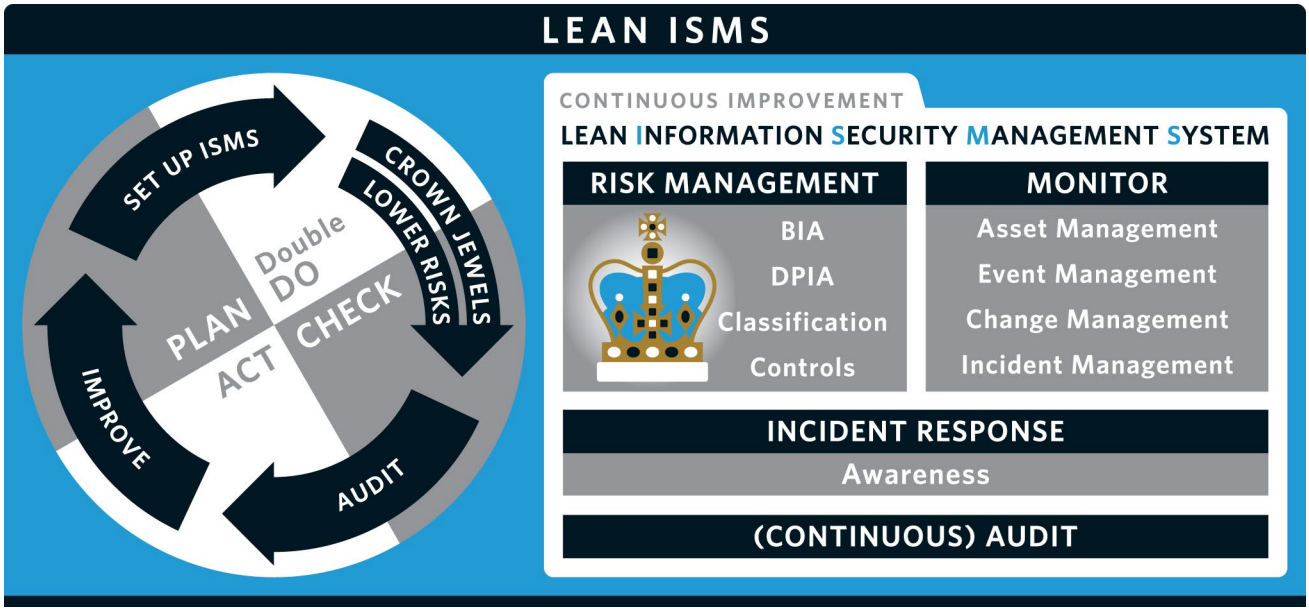
## WHAT OTHERS SAY

**"At Jumbo, the No. 2 food retailer in the Netherlands, the security backlog has proven to be a valuable tool in the information security program for determining and balancing risk and setting priorities for all security-related items. The security backlog has proven to be useful in putting things into perspective and/or to create a sense of urgency when necessary, internally and with our IT suppliers. In addition, it demonstrates a solid level of control to internal and external auditors."**

*—Marianne Schinkel, CISSP, manager information security (CISO), Jumbo Supermarkten*

**"Working with Interface, the world's largest designer and maker of carpet tile, we proved that the Lean and crown jewel approach was very effective in getting the board of directors on board. In a single session with the board, awareness regarding information security was turned a full 180 degrees, resulting in the board commitment, attention and budget required to implement security management and start the improvement cycle."**

*—Johan D. Bakker, MSc, CISSP, ISSAP, founder and CEO, Unified Vision*




Source: Unified Vision (http://www.leansecurity.nl)

his/her right mind, can expect a user to produce a strong password every 60, 90, xx days? The result is that the average password can be cracked within seconds. In the rare case these cracked passwords don't contain any privileged (user/service) accounts, the obtained credentials are an excellent starting point for a hacker to elevate privileges.

*Incident response:* Even when managed properly, incident response is reactive by nature, where proactive measures might be more appropriate, especially if it concerns our crown jewels.

*Fading borders:* In the past, all of our users worked together in office buildings, with very clear borders. At a certain point, users demanded remote access. Although this did require some effort, we granted them access by connecting their outside devices to our internal network.

We also started moving our server environments to specialized data centers. A smart move, since data centers are better equipped than we are, but a challenge because they added complexity in our networks. Still, the borders were pretty clear.

Now there's a worldwide mass migration to the cloud underway, as well as users that now expect nothing less than having access from anywhere, at any time, from any device. Borders are dissolving, and quickly.

The move to the cloud has also enhanced the use of shadow IT—employees using unauthorized applications to get work done. Or, as Gartner defines it: "IT devices, software and services outside the ownership or control of IT organizations." In 2018, Gartner estimated that by 2020, a third of successful attacks experienced by enterprises will be on data located in shadow IT resources.

Add to that the often uncontrolled use of social media, and the chaos is complete.

*Legislation:* Keeping up with legislation is another big challenge, where reputational damage is perhaps a bigger risk than potential fines. A good example is the European Union's General Data Protection Regulation (GDPR), which came into force in May 2018. The GDPR requires substantial effort to protect personally identifiable information, or PII. However, as of now, there remains uncertainty on the actual rules that need to be adhered to. For instance, Article 32 requires implementation of "appropriate technical and organisational measures to ensure a level of security appropriate to the risk." A privacy certification scheme as described in Article 42, such as ISO/IEC 27701, would contribute to alleviating the uncertainties. However, with constantly evolving legislation this will remain an issue.

## BRING ON THE BALANCE

The most obvious way to address all the above issues is by a traditional implementation of an information security management system based on the international ISO/IEC 27001 standard, given ISO/IEC 27001:2015 is the de facto standard for information security. The opinions on the effectiveness of certification to the ISO standard are divided, but if performed well, this definitely offers added value. Moreover, a certification is often the only way to demonstrate or gain reasonable assurance on the appropriateness of security measures in an organization. Other approaches may include implementation of frameworks such as COBIT (Control Objectives for Information and Related Technology).

What these standards and frameworks have in common is that they are solid and complete. But a traditional implementation adds a lot of complexity and paperwork. Following a Lean and Agile risk-based approach, when handled properly, will result in a well-balanced information security program.

Infographic: Robert Pizzo

## HOW TO IMPLEMENT A PROCESS FOR CONTINUOUS IMPROVEMENT

**Step 1: Establish strategic goals**
The first step is the most important one, because this will ensure commitment from the business. In this step senior executives are asked to determine the strategic business objectives for information security. They should answer the question: "What can information security do to help the business? How can we add value?"

This should ideally result in three, four, or a maximum of five business goals for information security, each with its own weight percentage to indicate the priority.

The only non-negotiable goal is "protecting the crown jewels," since that is a required part to reach balance in information security. The goals may be broad, from "prevent reputational damage and fines" and "control risks in the supply chain" to "make information available from anywhere, any device and anytime in a secure way." We definitely require more specific goals than "implement secure policies and procedures."

**Step 2: Develop tactical plans**
In the next step we move down from the strategic to the tactical level, where we make plans to reach the objectives. Each of these plans can then be directly linked to one or more of the set objectives.

Some examples of plans created in this stage of the process are implementation of key-ITIL processes (asset, configuration, event, change and incident management as a minimum), risk management, business continuity, awareness, data classification, BIAs/PIAs, etc.

**Step 3: Create operational/tactical controls and processes**
We now look at a tactical/operational level at the processes and technical controls necessary to accomplish our plans.

A good starting point is the CIS Top 20, which will cover most, if not all, cybersecurity requirements. To properly protect the crown jewels, some additional custom controls will be necessary to cover human resources, facilities and procurement processes.

Each of the controls directly links to one or more plans and consequently to one or more business objectives. These links will enable us to explain at any given point in time, at every level, what we need to do now—and why.

Once we have defined the process and controls, we perform a gap analysis. For each goal and process, we need to determine the current and aspirational maturity levels and what is needed to get there.

The output of this step is a (probably large) number of work packages, which we take to the next step.

**Step 4: Fill the backlog**
The work packages we just formulated are now used to fill or supplement the backlog. (Remember, this is an iterative process.) In addition to these work packages, we fill the backlog with all information security-related items such as findings from external accountants, internal audits and (self-)assessments, pen testing, vulnerability scans, questions from the business, projects from (multi-)year plans, or disturbing news for which we want to determine the impact on our organization.

All these issues (some of which need to be taken into smaller increments) are assigned a dynamic priority. So, adding five high-priority items may totally mess up the original plans for the coming period. The priority is risk-based and determined on a number of variables:

- Type of issue (incident or finding will get a higher score than a project or RFI)
- Risk score (probability x impact)
- Severity for organization

This includes a "veto" to accommodate questions from high up the hierarchical ladder. If the veto does not make the concerning issue one of the top priorities, the score can be used to have a well-founded and solidly substantiated discussion with senior management. Consider the:

- Impact on user organization (lower impact results in higher score).
  *Note: This is unrelated to the impact used for the traditional risk calculation; it is looking at the impact a certain change will have on your user base.*
- Business value (to be determined by the business owner of the concerned process/system).
- Lead time (quick win gets a higher score than a long-running project).
- Number of weeks open (to ensure that at some point a low-priority item will get attention).

**Step 5: Handle any outstanding issues**
Having completed all input for the process, we can start working with the backlog. Starting with the highest priority item, we work our way down. In a stand-up, for every predefined period of one or two weeks we look at what we have accomplished in the previous period and if any planned issues remain open. For finalized issues, we determine the residual risk (if any) and get formal approval to accept the risk. Should the residual risk not be accepted, it is added to the backlog as a separate entry so it will get the appropriate priority.

Then we determine which items we will work on in the coming period and what we need to accomplish.

Once an issue is closed, the priority score is set to zero. If it is closed as an accepted risk, the same

happens, until the end date of the risk acceptance is reached (maximum of one year after acceptance).

This way we have brought more balance in our information security program as soon as we have the basics covered and the Plan-Double Do-Check-Act process is running—even with a large number of open issues. After all, they are on our radar, and it is a deliberate business choice to temporarily acknowledge the risks until we have the resources to handle them, based on priority.

So how does this fit in a certification scheme such as ISO 27002?

Sure, we have outstanding issues (maybe even a lot of them), but since they are acknowledged by the business, and properly prioritized based on risk assessments, we are totally in control. Therefore, we don't need to reduce the scope, or exclude any of the controls in ISO 27002. The entries in our backlog can be looked at as CARs, as this is a clear overview of nonconformities and subsequent corrective actions.

With the CIS controls and the additional custom controls, we are nowhere near the 114 controls from the ISO 27002, but our picture is still complete. You can even break down all controls in smaller pieces and record where (in which policy, procedure, process or control) the evidence can be found. You will, in any case, need to extend the management process to a full ISMS that meets all mandatory elements from the norm. Then, perform a mapping to determine if any additional controls from Annex A are necessary to include.

*—M. Teuwen*

Will this work in every organization? Given it is based on consensus building, probably not. In strictly regulated organizations, where all boxes need to be ticked no matter what, it is probably not the optimal approach. Having said that, as soon as you draw a distinction between measures for the crown jewels and those for the less important assets, it is certainly an option.

## BALANCE IN INFORMATION SECURITY, IN THEORY

Starting with the theory, we follow six Lean principles and four Agile core values. These principles and values are slightly adjusted to fit in a model for information security but should be easily recognized by practitioners of Lean and Agile.

## LEAN

Lean originates from manufacturing environments where the goal is to eliminate or reduce waste, or any activity in the process that does not add value.

The concept of Lean Information Security was coined in 2012 by Unified Vision and its associates (www.leansecurity.nl). As of March 2019, I may also call myself a proud member of this reputable ensemble.

The Lean principles used to achieve balance in information security are the following:

- Visibly comply with business objectives and priorities.
- Prevent overhead and paperwork where possible by making improvements in small, pragmatic steps.
- Focus on the crown jewels for top threats.
- Rely on monitoring, detection and response for lower risks.
- Proven effectiveness of controls by measuring and monitoring.
- Realize continuous improvement based on measurements and facts.

## AGILE

Agile is found in almost every modern software development environment, where self-steering teams produce working functionality in pre-defined periods (sprints) of one or two weeks.

These are the core values in Agile used to accomplish balance in information security:

- We prefer working as a team over the use of pre-defined tools and processes.
- We prefer functioning controls over extensive documentation.
- We prefer working with the customer over strict following of rules.
- We prefer adapting to change over rigorously following a plan.

Of course, this cannot mean that we stop using proven tools and processes, that we stop documenting and that we don't follow rules and plans anymore. It *does* imply a fundamental shift, where we need to think about security, privacy and compliance by *design* from the start of each initiative. Because bolting on security at a later stage in the process will always result in a more expensive and less effective solution.

## BALANCE IN INFORMATION SECURITY, IN PRACTICE

In practice, balance in information security can be reached in five steps *(see sidebar on p. 25)*. An essential thing to

keep in mind is that information security is a continuous process. Remember the Deming cycle? For this occasion, the traditional PDCA process is supplemented with an extra Do, so we end up with a Plan-Double Do-Check-Act process.

In the Do phase, we make a clear distinction between the measures for our crown jewels and the measures for our lower risks. For the latter, we rely on our monitoring, detection and response capabilities, whereas for our crown jewels we implement proper controls, based on business impact analyses (BIA), and, if PII is involved, data protection impact assessments (PIA).

This does mean that we need to ensure that some key ITIL processes are running smoothly to support proper monitoring, detection and response. These processes are asset, event, change and incident management. That's because it all starts with knowing what we have (assets), what happens (event/change) and how to handle incidents.

For both crown jewels and the lower risks, we need to establish incident response procedures. Because at some point, an escalating incident will occur and all parties involved in this process need to be aware of what is expected of them. We also need to address awareness and (preferably continuous) auditing, so we can demonstrate that we are doing the right things in the right way at the right moment. And finally, we need to implement a process for continuous improvement.

## LEAN + AGILE = BALANCE

Pulling in best practices from the popular Lean and Agile methodologies enables us to create the best of both worlds tailored to an information security environment, clearly substantiating priorities based on established business objectives. This provides us with awareness and commitment from strategic to operational level but also increased visibility and thus improved awareness and involvement of the entire user base.

The ultimate goal is firmly embedding information security as a continuously improving process instead of fire-fighting and ad-hoc projects. By following the above suggestions and with the necessary persistence, patience and clear communication, it is no longer wishful thinking to get business owners to take responsibility. Embracing this approach will provide a feasible way to bring more balance to your information security program. ■

MICHEL TEUWEN, *CISSP, C|CISO, CISM, CISA, FIP, CIPP/E, CIPM, C|EH, is an information security and privacy consultant in The Netherlands.*

## BEWARE THESE POTENTIAL PITFALLS

**Insufficiently involved senior management**
A hard requirement for any information security program is active senior management commitment. They need to set the example as opposed to stating, "Do as I say, not as I do."

**Improper ownership**
Any employee may claim that they are "the business." However, it is crucial that decision makers are actually entitled to make decisions as formally delegated by senior management.

**Lack of resources**
Obviously, resolving many issues from a large security backlog will require proper resourcing, both in people and in budget. However, because the security backlog makes the (usually huge) amount of work packages very visible, resources are generally not the biggest challenge.

**Overcommitted management**
A large amount of open backlog items may make managers nervous. They may tend to start a project to eliminate the top items from the backlog. This may solve the resource challenge but will most likely increase the next pitfall: an organization that is unable to absorb all imposed changes.

**Overwhelmed organization**
Too many security controls with impact on the organization (i.e., impact on people) is a more serious risk compared to a lack of resources. Only a certain amount of changes can be unleashed on an organization. It's better to aim for slow-but-steady progress because haste trips up its own heels. Look in the backlog for lower priority items with less organizational impact to prevent underutilization of your resources.

**Non-functional requirements "offloaded" to the security backlog**
Non-functional requirements for any project need to remain must-haves for the project and should not be transferred to the backlog to handle later. Remember that it is always more expensive and less efficient to design bolted-on security measures.

**Security seen as a project, not process**
Probably the most important pitfall is that security is seen as a project instead of a process.

Of course, a project-based approach may be used for backlog items. For larger initiatives this may even be evident. However, always keep in mind that the project delivers a running process, not an end state.

*—M. Teuwen*

# Nothing Trivial About $1.5 Million in Scholarships

*by Pat Craven*

**SIXTY SCHOLARSHIPS.** Just a few years ago, that was the total number of applicants we would receive submissions from; now, we are awarding that many scholarships annually. Today, thanks to the growing interest and increased corporate investment in the cybersecurity profession, we can help more students and veterans pursue a career in this hot industry.

The (ISC)² scholarship program began in 2005, with scholarships awarded to four full-time, post-graduate students pursuing advanced degrees in information security. Each received one-year scholarships of $12,500. From 2005 through 2010, only three to six scholarships were awarded each year. In 2011, the (ISC)² Foundation (now the Center for Cyber Safety and Education) was formed as a separate 501(c)(3) charity and took over administering the scholarship program.

The scholarships were initially part of (ISC)²'s "Year of the Information Security Professional" program, designed to encourage new, high-quality entrants to join the profession. These early scholarships were focused on graduate students conducting research in the field.

In 2011, a separate women's category was created to help bridge the skills gap and improve diversity within the ranks of information security professionals. This past year, 58% of all scholarships were awarded to women. We also now provide more opportunities through a wider range of scholarship programs that focus on women, veterans, and undergraduate, graduate and secondary/high school students.

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

With the increase in applicants over the years (we had more than 1,100 in 2019), we began looking for additional partners to help us support more students. Booz Allen Hamilton was the first to come on board, followed by Raytheon, SAIC, and most recently, KnowBe4. To date, with our partners, we've provided more than US$1.5 million in financial aid to students in 40 countries.

**Since 2011, the number of applications has increased by 4,500%, which has led to some good challenges for us to overcome.**

Since 2011, the number of applications has increased by 4,500%, which has led to some good challenges for us to overcome. Keep in mind that each year we must now review and judge submissions from more than 1,000 wonderful candidates to select those scholarship recipients. All judging and scoring is done by active (ISC)² members. If you would like to help, please reach out to us at scholarships@isc2.org. It doesn't take a lot of time (you only have to review a small group of applications), and I guarantee that you will be inspired about the future of the industry when you read what these young people are doing today.

With the growing need, we are also looking for more companies and chapters to sponsor scholarships. We manage the entire process and can customize a program to fit your corporate goals. It is a proven win-win partnership.

Finally, if you are looking to advance your studies or have a friend, family member or coworker pursuing a degree or wanting to earn an (ISC)² certification, visit www.IAmCyberSafe.org/scholarships to learn more. ■

Image: Alex Doubovitsky / iStock

# Advice on GDPR Beyond the EU, CISSP Readiness, Access Reviews

The (ISC)² Community has more than 23,000 cybersecurity professionals connecting, sharing knowledge and offering solutions in the online forum. Note that the questions and responses may have been edited for clarity and brevity.

**QUESTION:**

**The company [in South Africa] I work for does not deal with the EU or any EU citizens officially, but the possibility is always there that this kind of data might make its way onto our systems.**

**How will the EU be able to enforce this regulation in South Africa? If a South African company hypothetically causes an EU citizen material or immaterial damage, how will the EU hold that company accountable? How will they impose the fine? If this South African company just says, "I'm not paying, to hell with the EU, this is Africa," how will the EU go about this? Is there an onus on the South African government to get involved?**

*—Submitted by Armandt_R*

**SELECTED REPLIES:**

Everything I have read would indicate that they cannot enforce the fines, and frankly, they have no right to in another sovereign nation. Privacy isn't covered (yet) in any international law that I am aware of, though I am not a lawyer. That said, they can take actions against any assets or business in the EU. If you are truly 100% not doing business in the EU, I would not be concerned with the specifics. I would also make sure to look through the privacy community in South Africa, as it seems more and more countries are putting in privacy laws [and] GDPR is the model many of them are using.

*—Submitted by mgorman*

Unless governments get together and form an alliance, I am not sure how the fines, etc., will or can be imposed. Of course, if you work for a global organization, one of your subsidiaries may bear the penalty for not complying with a law in a specific state or country.

*—Submitted by dcontesti*

**Find this complete thread here.**

**QUESTION:**

**I am a PMP-certified professional working with infrastructure projects for the last 15 years. I would like to make a career shift into security. Please suggest if CISSP is the right certification.**

*—Submitted by C_Shift*

**SELECTED REPLIES:**

Are you looking to get out of project management, or to move from infrastructure projects to infosec projects? I have seen folks who are infosec project managers, who almost all have both the CISSP and PMP. Which is a combo rarely found.

*—Submitted by emb021*

CISSP … is a cybersecurity leadership certification. Many of the students in my test preparation classes are C-suite executives and high-ranking military officers. If you feel that you are ready to step into, or are already in, a role like that, attaining the CISSP may be a good choice at this point in your career. If not, I recommend seeking a more "hands-on" position to gain experience and sit for the exam when you feel you're ready to lead a cybersecurity organization.

*—Submitted by CyberLead*

It really depends on several factors: your interest, your career path, and your experiences. Having both certifications certainly would help your career, but you will need experience to be fully qualified as a CISSP. Having obtained both myself, I find it is very beneficial to cross-reference your knowledge from either field. Exam-wise, CISSP is on par with PMP in terms of difficulty level.

*—Submitted by Chuxing*

**Find this complete thread here.**

**QUESTION:**

**I've recently started working at a new company that is trying to automate its access management as much as possible. What I'm wondering specifically pertains to access reviews. We're going to be putting in a lot of work to fully defining roles within the company and what permissions they have. We're using a human capital management system connected with AD to ensure that any hires, role changes and terminations flow through to the applications. What is the best way to simplify access reviews?**

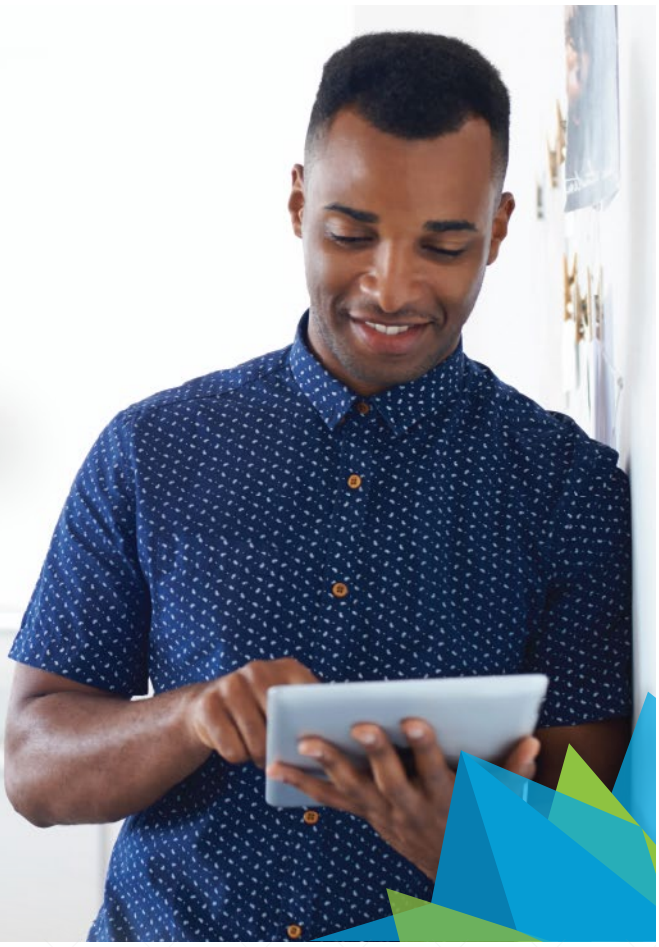
*—Submitted by Billygoat*

**SELECTED REPLY:**

If HR is initially assigning roles, then someone independent of HR should be reviewing access to said roles.

*—Submitted by Troy_Fine*

**Find this complete thread here.**



# Free Courses

## & CPEs for Members

The (ISC)² Professional Development Institute (PDI) takes you beyond your certification with a portfolio of FREE professional development courses and you earn **CPEs**.

### Course Types Include:

- Immersive – In-depth training on a variety of cybersecurity and IT security related topics.
- Lab – Hands-on courses that enable learners to practice specific technical skills.
- Express Learning – Short-format courses with on-the-go professionals in mind.

**Start FREE Courses**

To receive communications when new courses are released, log in to your (ISC)² account and update your communication preferences to include Continuing Education & Professional Development.