



InfoSecurity PROFESSIONAL

A Publication for the (ISC)2® Membership

MAY/JUNE 2018

“Management and leadership are not mutually exclusive.”

—KIMBERLY MAHAN, CISSP,
CEO and president, MAAX Potential

CERTIFICATION & ACCREDITATION

Can we trust the process used to determine the worthiness of a product or service?

PASSING ON PASSWORDS

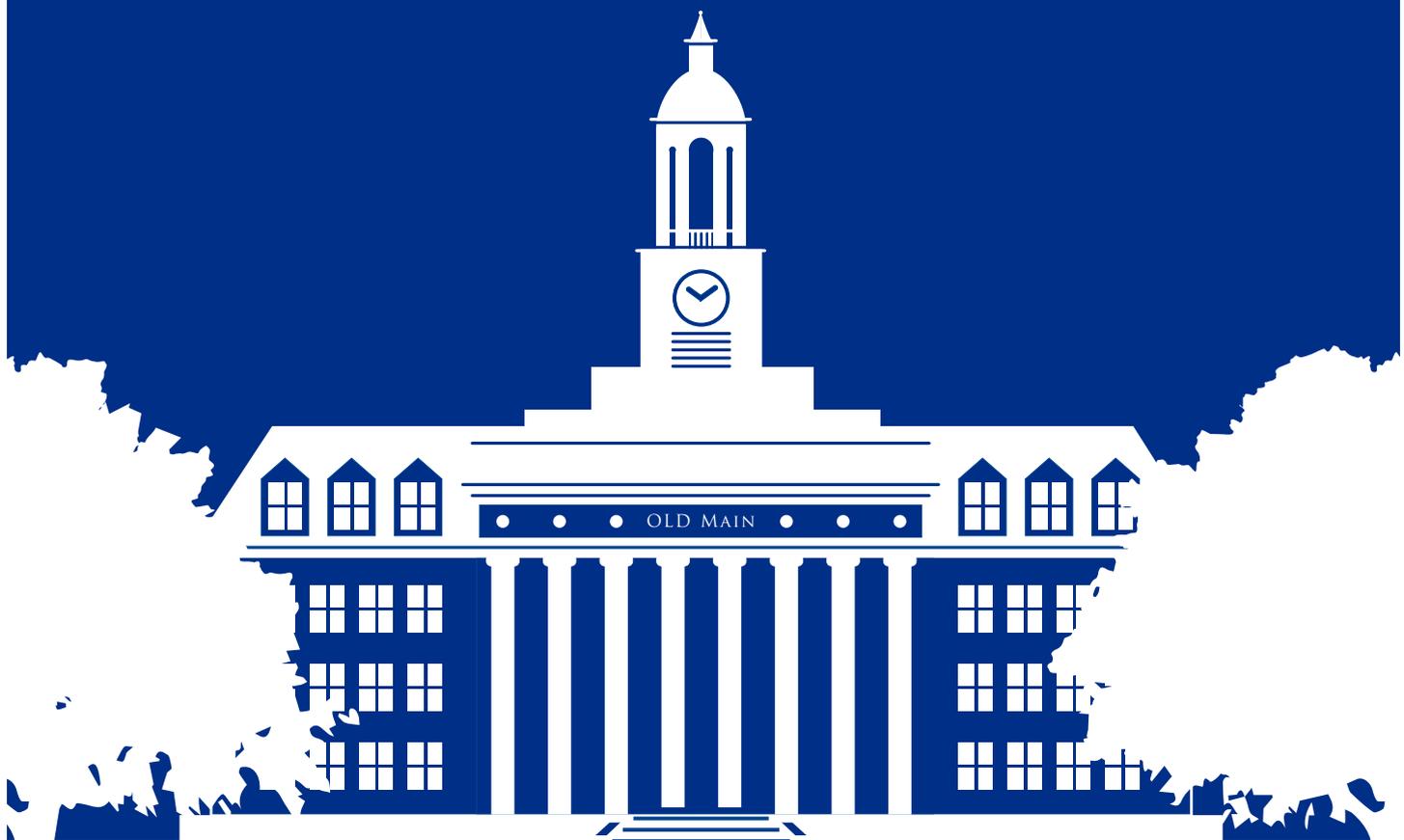
Some solutions to ease your pain

WHEN TO lead, when to FOLLOW

(AND WHY YOU SHOULD DO BOTH REGARDLESS OF YOUR JOB TITLE)

Cybersecurity degrees online from a recognized leader

Visit Penn State at RSA booth #4336



PennState
World Campus

worldcampus.psu.edu/isc2

A world of possibilities. Online.



A look at the replacements for passé passwords. PAGE 26

features

PROFESSIONAL DEVELOPMENT

- 16** **When to Lead, When to Manage...**
...and why you should do both, regardless of your job title.
BY CATHERINE KOZAK

IDENTITY/ACCESS CONTROL

- 22** **I_#@te_Us1ng_P@sswords!!**
Every organization has its own password rules—technology may soon eliminate the confusion and frustration.
BY SCOTT J. MILLER, CISSP

SWISS ARMY KNIFE

- 26** **Certification and Accreditation:
Beyond the Rubber Stamp**
How much should we trust the process used to determine the security-worthiness of a product or service?
BY JASON McDOWELL, CISSP

Cover photograph: JONATHAN TIMMES Illustration above: ENRICO VARRASSO

departments

4 EDITOR'S NOTE

Management is Tough; Leadership, No Less So

BY ANNE SAITA

6 EXECUTIVE LETTER

A Commitment to Upholding the Integrity of that Credential

BY DR. KEVIN CHAREST, CISSP

8 FIELD NOTES

Tips on vulnerability remediation; online SSCP® training; Center for Cyber Safety and Education a winner; primer on NIST guidelines; new regional director for EMEA and more.

12 #NEXTCHAPTER

(ISC)² Netherlands Chapter

14 ADVOCATE'S CORNER

It's Finally Spring— Let's Pick Up the Pace

BY JOHN McCUMBER

29 CENTER POINTS

It's Now Easier to be a Cyber Safety Ambassador

BY PAT CRAVEN

30 LEAD IN

Katsuhiko Nakanishi, CISSP

Preventing cyberattacks at the 2020 Tokyo Summer Olympics and Paralympics is Job One for this Asia-Pacific Information Security Leadership Achievements (ISLA™) honoree.

4 AD INDEX

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. No part of this document print or digital may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of (ISC)². (ISC)², the (ISC)² digital logo and all other product, service or certification names are registered marks or trademarks of the International Information Systems Security Certification Consortium, Incorporated, in the United States and/or other countries. The names of actual products and companies mentioned herein may be the trademarks of their respective owners. For subscription information, please visit www.isc2.org. To obtain permission to reprint materials, please email infosecproeditor@isc2.org. To request advertising information, please email tgaron@isc2.org. ©2018 (ISC)² Incorporated. All rights reserved.

editor's note

► BY ANNE SAITA

Management is Tough; Leadership, No Less So

I'M VENTURING OUT ON A LIMB, but I believe the majority of you reading this have worked for bad bosses. Maybe they lacked the empathy to handle people with care. Maybe they rose through the ranks quickly and didn't have the depth of knowledge or experience for their current title. Maybe they were the kind who throw shade to deflect attention, or throw others under the bus to avoid blame.

No one plans to be intentionally callous, incompetent or corrosive when they are starting a new career. And yet, too many managers and executives become that which they once detested. Why is that? For starters, managing others takes a set of skills far different from those that likely landed them their first job. Then, it was technical proficiency that topped the scorecard. Managing security software and systems, however, has little to do with managing people. And managing people is a far cry from leading business units or entire enterprises.

Last year, I devoted several of these columns (too many columns, some told me) to prime you for our cover story on the differences between leadership and management, and how to excel at both. I offered advice on time management, stress reduction and interpersonal communications—particularly active listening. Mastery of each is important to make the most of our personal and professional lives; we can't effectively manage others if we can't even manage ourselves.

Speaking of management, our other two features help members in different ways. One will help you evaluate security solutions by way of vendor certifications. The other offers practical pointers for those pesky passwords users keep forgetting or sharing.

As always, I welcome your feedback on this and other "issues." ■



Anne Saita, editor-in-chief, lives and works in Southern California. She can be reached at asaita@isc2.org.

advertiser index

For information about advertising in this publication, please contact Tim Garon at tgaron@isc2.org.

Penn State World Campus.....	2	Cofense.....	20
(ISC) ² Security Congress – APAC.....	5	(ISC) ² Security Congress – LATAM.....	21
(ISC) ² SecureSummitUK.....	7	(ISC) ² Ultimate Guides.....	25
Duo Security.....	13	(ISC) ² Community.....	31
(ISC) ² Security Congress – North America.....	15	(ISC) ² CPE Enhancement.....	32

(ISC)² MANAGEMENT TEAM

DIRECTOR, CUSTOMER EXPERIENCE
Jessica Hardy
727-493-3566 | jhardy@isc2.org

EXECUTIVE PUBLISHER
Timothy Garon
508-529-6103 | tgaron@isc2.org

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

MANAGER, CORPORATE COMMUNICATIONS
Amanda Tarantino
727-877-2230 | atarantino@isc2.org

COMMUNICATIONS SPECIALIST
Kaity Eagle
727-683-0146 | keagle@isc2.org

MANAGER, MEDIA SERVICES
Michelle Schweitz
727-201-5770 | mschweitz@isc2.org

EVENT PLANNER
Tammy Muhtadi
727-493-4481 | tmuhtadi@isc2.org

SALES TEAM

EVENTS SALES MANAGER
Jennifer Hunt
781-685-4667 | jhunt@isc2.org

REGIONAL SALES MANAGER
Lisa O'Connell
781-460-2105 | loconnell@isc2.org

EDITORIAL ADVISORY BOARD

Kaity Eagle, (ISC)²
Jarred LeFebvre, (ISC)²
Yves Le Roux, EMEA
Cesar Olivera, Brazil and Canada

TWIRLING TIGER MEDIA EDITORIAL TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

MANAGING EDITOR
Deborah Johnson

EDITOR
Paul South

PROOFREADER
Ken Krause



Twirling Tiger™ Media (www.twirlingtigermedia.com) is certified as a Women's Business Enterprise (WBE) by the Women's Business Enterprise National Council (WBENC). This partnership reflects (ISC)²'s commitment to supplier diversity.

(ISC)²



SECURITY
CONGRESS

APAC
2018

9-10 July
Conrad Hong Kong

ENRICH

ENABLE

EXCEL

REGISTER TODAY >>

Enjoy Member
Rate & Earn up
to 16 CPEs

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

At (ISC)² Security Congress APAC 2018, you'll get to engage with over 400 security-minded individuals, discover solutions to the latest cybersecurity threats and gain insight from international industry experts. Maximize your learning experience with our multi-subject sessions, panel discussions and networking opportunities designed to enrich and enable you to excel as a cybersecurity professional.

Have questions? Talk to us!

Sponsorship - Michaella Park (mpark@isc2.org) | Registration - Maggie Yuen (myuen@isc2.org)

In partnership with:

image
engine

Visit apaccongress.isc2.org

f t #isc2congressAPAC



A Commitment to Upholding the Integrity of that Credential

THROUGHOUT MY CAREER, I've been fortunate to have proudly worked in many capacities for a wide variety of organizations. I'm a military veteran who served in both the United States Marine Corps and Army. I've worked in several entrepreneurial and senior executive positions in the private sector and have been CISO for the U.S. Department of Health and Human Services. I've led global cyberdefense operations for the largest healthcare company in the world and currently serve as the divisional senior vice president and CISO for Health Care Service Corporation, where I'm responsible for all facets of IT security.

In January, I added to that leadership list, being elected chairperson of the (ISC)² Board of Directors. As such, I intend to make sure that we, as representatives of the membership, continue to challenge management to serve

members in everything they do and to maintain the integrity of the credentials you have worked hard to earn.

This is my third year on the board, and I continue to be excited by the consistent, tremendous growth (ISC)² is experiencing, especially as old legacy systems are replaced through digital transformation into new, far more robust capabilities. This transformation helps to ensure an (ISC)² credential continues to bring value to both our global members and the organizations they serve.

One such example is the new online Community (<https://community.isc2.org>) for mem-

bers to connect, collectively problem-solve and exchange employment opportunities. We've also replaced the paper-based version of the CISSP exam with a modern, computer-adaptive testing (CAT) platform that cuts testing time significantly and provides us deeper analytics to ensure test questions remain valid.

What CAT and other updates won't do is reduce the rigor required to achieve an (ISC)² credential. The integrity of that credential and the Code of Ethics under which we operate are foundational linchpins to our organization. They are a major reason you initially sought to become part of our global membership.

The integrity of that credential and the Code of Ethics under which we operate are foundational linchpins to our organization.

Our board also encourages (ISC)² executives and management leaders to continually examine our credential offerings. Industries evolve over time and we need to ensure our members' breadth of knowledge does too.

As we ponder the digital transformations and cloud adoption rates currently sweeping the world, traditional compliance-based security will struggle to keep pace with such agile development cycles. That's why, as chairperson of the board, I am committed to providing the knowledge development and educational opportunities now required by you, our members, so that we maintain relevancy in today's ever-evolving technical and business landscapes. ■



Dr. Kevin Charest, CISSP, is the deputy senior vice president and CISO for the largest member-owned U.S. healthcare company and chairperson of the (ISC)² Board of Directors. He can be reached at kcharest@isc2.org.



(ISC)²

SECURE SUMMITS / UK

#ISC2Summits

ENRICH. ENABLE. EXCEL.



Join us at the (ISC)² Secure Summit UK
19 - 20 September | The Kia Oval, London

(ISC)² Secure Summit UK assembles the best minds in cybersecurity for two days of insightful discussions, workshops and best-practice sharing that will better equip you to tackle today's threats and advance your career in the ever dynamic workplace. Enrich your mind by learning from the most experienced and brightest in our profession. Their thought-provoking and fresh perspectives will enable you to achieve your career goals while strengthening your organisation's security posture. It's time for you to excel at everything you do. We can help.

Learn more at:

securesummits.isc2.org

Free for (ISC)² members and (ISC)² chapter members

field notes

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

EDITED BY DEBORAH JOHNSON

MEMBER ADVICE

Six Steps to Improving Vulnerability Remediation

BY WILLIAM NANA FABU, CISSP

GENERALLY, people are not that good at identifying their weaknesses because such flaws only arise when challenges are faced. Here are some tips based on my own experience in improving vulnerability remediation.

1. Complete management support.

Remediation involves all departments in the company, so it is imperative to have full support at the top. Without management's support, your crucial patching programs could take a back seat to business priorities. Note that in most institutions, the lower environment is not a replica of the production environment. Therefore, testing in the lower environment does not guarantee a "zero issue" state when you move the patches to production.

2. Educate the business on the importance of patching.

Patching and remediation are not just for information security, but cover the entire enterprise. You have to build awareness on the importance of patching. Use the examples of current ransomware and other cyberattacks to make your case, especially to the senior business (non-IT) managers, as they are the ones likely to push back the most. Have management send the message about patching activities to stress the importance and support.

3. Patch both new and historical vulnerabilities.

Do not limit your patching to the newly published patches and vulnerabilities. Make sure you also tackle the historical patches and vulnerabilities (backlog). Remember that bad actors generally use forgotten vulnerabilities to launch their attack campaigns. Also, pay attention to the new patching format introduced by Microsoft and adapt your patching program to it as soon as possible.

4. Work also on the non-patchable vulnerabilities.

It may take more time and effort to clear your non-patch-



able vulnerabilities, but you need to put in the effort and energy on this category, especially in your most critical network zones and applications. Build a strong relationship with the system administrator and propose clear remediation paths (upgrade, system configuration, end-of-life system and application replacement, etc.). This is where you need to put on your consultant hat and work with the application and system owners to translate the non-patchable vulnerability list into a list of actionable items that can be easily implemented. Do not forget to involve vendors at the beginning of this process. Generally, the solution or at least a key part of it would come from the vendor. Finally, insist on testing the system after remediation.

5. Build exception groups.

There will be times when systems crash after a patch despite the due diligence and testing. For these cases, build exception groups—have the business enter an exception with information security and clearly document the cases.

6. Move from volume to risk.

In most cases, start with a volume approach to reduce the vulnerability count. When the number has reached an accepted ratio (number of vulnerabilities compared to the number of endpoints) prescribed by management, then shift to a risk approach. At this point, build your targets based on the risk assessment carried out by the information security team. Do not only rely on the CVSS score to prioritize vulnerability remediation. ■

WILLIAM NANA FABU, CISSP, works in Atlanta. This is an excerpt of a feature he wrote for the February issue of Insights, a companion e-newsletter for the (ISC)² membership.

Online Training Now Available for SSCP Program

(ISC)² NOW HAS ONLINE TRAINING when you want it. In partnership with Coursera, the online provider of higher education, (ISC)² is offering its Systems Security Certified Practitioner (SSCP) training in a self-paced environment. “Making security training easily attainable to those who might not otherwise have access allows them to proactively build their professional careers and master the expertise employers most need to conquer today’s cybersecurity challenges,” said (ISC)² CEO David Shearer.



The SSCP program is designed for IT professionals responsible for the hands-on operations of securing their organizations and covers security operations and administration; risk identification, monitoring and analysis; incident response and recovery; network and communications security; system and application security; and cryptography—skills most often required by IT employers.

Certification courses can be found by visiting <https://www.coursera.org/specializations/sscp-training>. ■

How We Work: More Findings from the Global Information Security Workforce Study

IT professionals are a critically underutilized resource for cybersecurity, according to more than 3,000 IT professionals who participated in the 2017 (ISC)² Global Information Security Workforce Study. That broader biennial study’s results, based on opinions of almost 20,000 professionals from 170 countries, can be found at <https://iamcybersafe.org/gisws/>.

43% Say their organizations don’t provide adequate resources for IT security training and professional development

55% Say their organizations do not require IT staff to have a cybersecurity certification

63% Say their organizations have too few cybersecurity workers

Earn 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.

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&PCAT=7777&CAT=10757

KUDOS

Center for Cyber Safety and Education Named Local Chamber’s Nonprofit Organization of the Year

The Center for Cyber Safety and Education is the Clearwater (Fla.) Regional Chamber of Commerce’s 2018 Nonprofit Organization of the Year. The Center is the charitable trust of (ISC)² and learned of the award earlier this year.

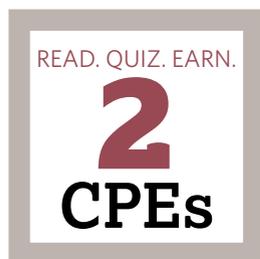
“We are deeply honored to receive this recognition, especially in our local community,” said Patrick Craven, director of the Center. “This award fuels our mission to ingrain cyber safety education into our culture so that everyone growing up or living in the digital world can protect themselves online. It also acknowledges the tireless work of the Center’s staff and volunteers around the world.”

Among the Center’s most popular programs:

- **Safe and Secure Online** (<https://safeandsecureonline.org/>), which offers interactive safety education materials for children, parents, educators and senior citizens. The children’s materials feature Garfield and friends tackling cybersecurity issues, including privacy, the dangers of posting online, online etiquette, cyberbullying and more.

- **Cybersecurity scholarships** (<https://www.iamcybersafe.org/scholarships/>), which to date have provided more than \$1 million to women, military veterans, and undergraduate and graduate students around the world.

- **Cybersecurity workforce research** (<https://www.iamcybersafe.org/gisws/>): The Center releases a biennial Global Information Security Workforce Study, which provides one of the most comprehensive views on the current state of the cybersecurity workforce worldwide. ■



DESHINI NEWMAN NAMED EMEA REGIONAL MANAGING DIRECTOR

Deshini Newman is the new regional managing director for EMEA. She will take over for Dr. Adrian Davis, CISSP, who recently became the region's new cybersecurity advocate.

Newman comes to (ISC)² from Cambridge Assessment, part of Cambridge University (U.K.), where for more than a decade she held leadership roles in global development of its English language examinations that are recognized by more than 20,000 universities, employers and governments globally. She also brings 15 years' experience in examination publishing.

"Deshini is a strong addition to our effort to develop skilled talent in the face of a well-acknowledged skills shortage in cybersecurity," said (ISC)² COO Wesley Simpson. "The need to enhance cybersecurity and access to relevant talent is an increasingly top priority at the highest level of government and business thinking in more countries around the world. Deshini brings valuable experience working across varied geographies, addressing both mature and emerging economies, and will enhance the support we offer with certification and membership."

You can learn more on our website (<https://www.isc2.org/News-and-Events/Press-Room/Posts/2018/02/01/ISC2-Names-Deshini-Newman-as-Managing-Director-for-EMEA>). ■



Deshini Newman

Securing Digital Identity

NIST guidelines hope to clarify the meaning of 'identity.' BY LARRY MARKS, CISSP

AS PART OF EFFORTS by the National Institute of Standards and Technology (NIST) to clarify and enhance implementation of the cybersecurity framework, NIST recently released guidance on "digital identity" definitions and authentication. Here's a quick primer on what it advises.

DEFINING DIGITAL IDENTITY

NIST defines a digital identity as "...the unique representation of a subject that is engaged in an online transaction." NIST focuses on the components of digital identity—identity proofing, authentication and federation—and explains how these can be used to protect the digital identities of their employees. Though this guidance is directed toward federal networked systems, it can be adapted to non-federal systems.

Identity proofing – The process used to verify a subject's association with their real-world identity, establishing that a subject is who they claim to be.

Authenticator – Something the subject possesses and controls (typically, a cryptographic module or password) that is used to authenticate the subject's identity.

Digital authentication – The process of determining the validity of one or more authenticators used to claim a digital identity. Authentication establishes that a subject attempting to access a digital service is in control of the technologies used to authenticate. Successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same one that previously accessed the service.

Federation – When the relying party and identity provider are not a single entity or not under common administration, federation enables an identity provider to prove and authenticate an individual and provide identity assertions that a relying party can accept and trust.

IMPACT ON USERS

The impact of the process of verifying digital identity can be measured using the following four factors:

Identity proofing: Identity proofing is described in general as the most difficult to implement because the proofing goes to the heart of authentication and leaves the discretion to the identity reviewer. The identity reviewer must review the process used to verify the evidence for identity, authentication and federation. Identifying attributes must be verified by an authorized and trained representative.

Authentication: NIST provides recommendations on the types of allowable authenticators such as tokens, captchas, etc., that may be used, the controls over the authenticator, best practices for account recovery and when it is necessary to reauthenticate an individual.

Continued on next page

field notes

From previous page

Federation: NIST mentions federation and provides best practices for asserting a user's identity in order to deflect an attacker and includes a host of privacy-enhancing requirements that can make federation appealing to users.

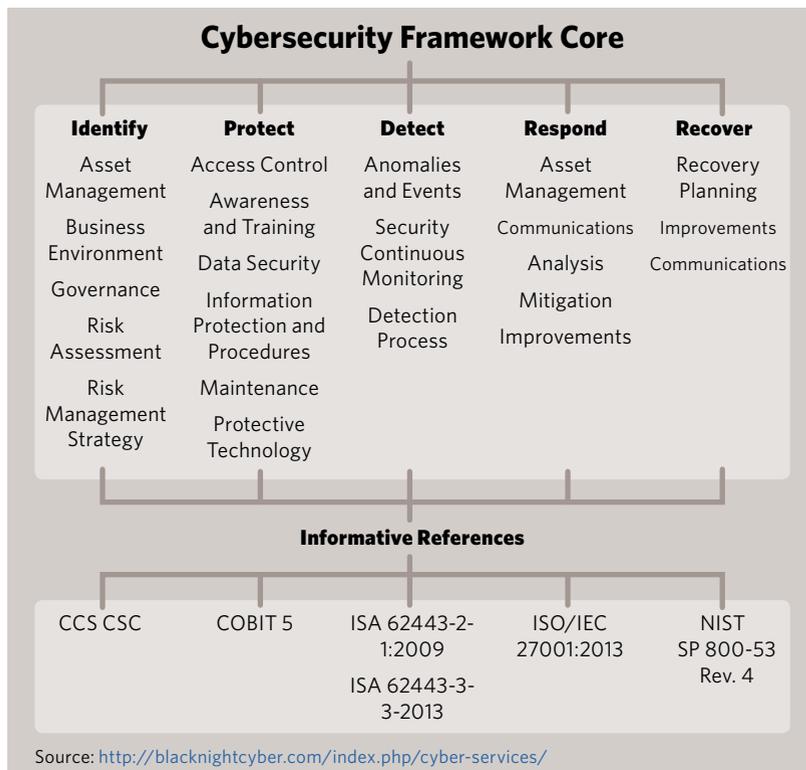
STRENGTHENING PROTECTION

NIST 800-63 recommends the following changes to strengthen identity and protection controls as they relate to the NIST Cybersecurity Framework. They are a departure from the past, and firms will have to evaluate their impact on their internal applications, databases, vendor applications, etc.

- Maximum length increased to 64 characters or more
- All printable characters allowed, including spaces
- Fewer complexity rules enforced ("Must include one uppercase/number/symbol/etc.")
- Expiration of passwords no longer based on a time schedule
- SMS as a two-factor authentication method removed
- Passwords should be compared to dictionaries and lists of common, easily guessed passwords

NIST continues to provide guidance to help users implement NIST 800-63. As feedback is received from customers on the implementation of these guidelines, NIST will be revising or enhancing this guidance. ■

LARRY MARKS is a veteran infosecurity professional and a freelance writer and blogger. He regularly contributes to the Recommended Reading section of InfoSecurity Professional.



CLARIFICATION ON GDPR PENALTIES

Shortly after our March/April issue was published, we heard from U.K. member Elizabeth Pryce, who let us know the EU General Data Privacy Regulation actually has a two-tiered penalty system.

For infringements of the organization's obligations, including data security breaches, fines can be up to €10 million, or 2 percent of annual global turnover (whichever is higher).

When there's a determined infringement of an individual's privacy rights, a higher penalty of up to €20 million, or 4 percent annual global turnover (whichever is higher) applies. ■



45
PERCENT
of organizations
perceive their own
employees to be the
biggest security risk

Source: Cloud Security Risks and Concerns in 2018 - Netwrix.com

<https://blog.netwrix.com/2018/01/23/cloud-security-risks-and-concerns-in-2018/>

Photograph: gradyreese/Stock

#nextchapter

EDITED BY DEBORAH JOHNSON

GOING DUTCH

Growth is the Goal for the (ISC)² Netherlands Chapter



WITH 533 CURRENT MEMBERS, (ISC)² Netherlands Chapter, based in Slochteren, has a strong base, but chapter leadership is not resting there. They've set a goal to have 1,000 members by the end of the year. An ambitious goal, to be sure; it's part of a one-year plan to:

- increase the number of active volunteers to 25
- increase the number of sponsors to 10
- organize additional events, workshops and webinars
- cooperate with other chapters
- maintain and improve their relation with EMEA
- begin participating in the Center for Cyber Safety and Education's Safe and Secure Online[®] program

The key to engaging information security professionals, says chapter president Heinrich (Henk) Klöpping, CISSP, CCSP, is to focus on usable information. "We try to present actual, real-life examples and provide information that can be applied in real-life situations. For example, during our next event, we will have a young gentleman who has actually hacked the controlling units of solar panels—and of a type that is very common in my country."

In order to produce exciting events that would help grow the chapter and expand its impact, more active volunteers were needed. Chapter leadership reached out to membership with a survey that resulted in a list of people who had the time and interest to do the work. "Volunteer Days" are held to organize and motivate the "workforce" to help broaden the chapter's scope and activities.

(ISC)² NETHERLANDS CHAPTER CONTACT INFO

Contact:
Heinrich Wilhelm (Henk) Klöpping
Email: board@chapter.isc2.nl
Website: <http://chapter.isc2.nl>

With an active and engaged—and growing—membership, (ISC)² Netherlands looks to enhance its mission with Safe and Secure Online and to become a central point for sharing crucial updates on information security. ■

▼ Q&A

Heinrich (Henk) Klöpping, CISSP, CCSP, president, (ISC)² Netherlands Chapter

What are the greatest challenges the chapter faces in growing membership?

Ensuring that every person in the Netherlands that has an interest in information security knows our chapter exists and how to register as a member. This especially holds true for (ISC)² members. We know there are roughly 2,280 CISSPs in our country. It would be great to see them all register as members of our chapter and if possible, join our volunteer workforce. So, if any Dutch members of (ISC)² read this, who are not members of our chapter yet, go to <https://registry.chapter.isc2.nl> and register!



We know there are roughly 2,280 CISSPs in our country. It would be great to see them all register as members of our chapter and if possible, join our volunteer workforce.

What advice would you give to other chapter leaders who are looking to increase the membership?

In short: If you're not a legal entity, become one. Structure your organization, set up an online registry and proper website, ask the EMEA

#nextchapter

regional office and other chapters to help you and reach out to both members and non-members. And last, but certainly not least, organize good events.

In reaching out to the membership in general, what suggestions do you have for them to grow and strengthen their own chapters?

Visit our events, help organize them, become an active volunteer. You may think there is not much you can do; but, rest assured, there is! From writing articles, blogs or recording vlogs, to visiting schools, developing learning materials or translating existing materials, and much, much more.

What are some of the major issues your members are interested in?

Currently, IoT and GDPR are quite hot. The application of existing frameworks and standards to new technologies and situations is also a topic. Then international espionage, especially online attacks and interventions by foreign nations and what to do about it, are becoming of increasing importance. Privacy is a big theme for 2018.

On the subject of GDPR, any observations you'd like to share?

GDPR has at least one big advantage: It stimulates interest of many companies in information security and offers great opportunities for our workforce. Given the huge number of companies involved, there is an equally large need for information security and privacy specialists.

This is also a great opportunity for (ISC)² as we offer a long-standing, well-respected series of certifications, helping to ensure the quality of candidates for new positions like the DPO [data privacy officer]. It is also, as far as I know, the first time we will have something that may, in practice, work as a global data protection law, as almost every country in the world actively trades with EU countries and hence, is required to handle EU citizens' data according to the GDPR. The new regulations taking effect may initially result in problems, as we still struggle with a shortage of sufficiently skilled information security workers, but I'm sure that in the end, the GDPR will bring a positive change, worldwide. ■

Duo's Trusted Access solutions accelerate your IT modernization journey

- Easy and effective MFA
- Agentless device insight and trusted access policies
- Secure BYOD devices and GFE
- Cloud first with support for on-premises apps
- Helps to meet NIST 800-53/63/171
- Supports NIST SP-800-63-3 auth methods and secure (FIPS 140-2 validated) tokens



Sign up for a
free trial at duo.com



It's Finally Spring—Let's Pick Up the Pace

FINALLY, better weather. The temperature climbed sufficiently for me to drag my motorcycle out of the garage and blow some carbon out of the cylinders a few weeks ago.

Here's my third installment of the Advocate's Column, and I want to use this platform to welcome (ISC)²'s latest cybersecurity advocate for EMEA.

Let's give a warm welcome to Dr. Adrian Davis, CISSP, who enjoys all the benefits of being assigned to our office on the south side of the Thames in London. If you want to find our offices there, just go to the Traitors' Gate at the Tower of London, and gaze directly across the river. Yup, that's us. We're waving back.

In this edition, I want to bring you up to speed on our fast-paced activities. By the time you read this, our Lexicon Project will be a reality. I edited the next-to-final copy today before it goes for a read-through and layout for production. There's a link to it on our website, so you can see it there and download your copy.

We developed this project simply because we hear so many important people butchering terms used in cybersecurity and risk management. Many of these people are legislators, lawyers, journalists and others who really need to understand the basics. We wanted to provide a useful reference for laypersons to ensure that authors of new laws, regulations, articles, guidance, policies and standards use

these terms correctly. Feel free to make copies and distribute as needed.

In addition, we are working on a Cybersecurity 101 course you can use. We are going to make this available as a resource for similar audiences: those who may not have a career in cybersecurity, but need basic knowledge of key concepts, strategies and terms.

Many of you have seen me on the road at places like BSides Tampa, Secure Summit Phoenix, RSA Conference and

Secure Summit DC. It's been a singular pleasure to represent you and our profession. The rest of the year will be just as busy with chapter events, speaking and presentations. Please make it a point to stop and say hello. I hope we can meet this year.

We developed the project simply because we hear so many important people butchering terms used in cybersecurity and risk management. Many of these people are legislators, lawyers, journalists and others who really need to understand the basics.

I am going to ask something else. I'd like those of you who are not currently in a chapter or council to strongly consider joining your local chapter or starting one of your own. These local gatherings provide a perfect setting to network and keep current on the job market. You never know when that will come in handy. It's not a bad idea to also attend other local gatherings of your fellow practitioners in places like Baltimore, Chicago, New Orleans, Orlando, New York and Seattle. They're fun spots for fellowship among friends with knowledge, leads, stories and snacks. What's not to like?

Finally, be on the lookout for the new Advocate's section on our website (<https://www.isc2.org/cybersecurity-advocates>). Adrian and I will be posting updates and hosting Q&A sessions. You can also use this link to get access to white papers, the Lexicon Project and conversations with your advocates. Adrian and I look forward to hearing from you soon. ■



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



EARLY BIRD PRICING

— through July 31 —

Oct. 8 - 10 • New Orleans, LA • Marriott

(ISC)² Members
SAVE \$300

2000+ Attendees
& **100+** Sessions

Earn up to
46 CPEs

All Access Pass Benefits:

- Educational Sessions, Keynotes & Workshops
- Networking Luncheons
- Expo Hall
- Town Hall & Career Center
- Networking Night at Mardi Gras World
- Sunday Bonus: CSA Summit & Expo Hall Pub Crawl

ENRICH

ENABLE

EXCEL

SAVE \$50

Off All Access Pass
with code:

INFOSEC18

REGISTER TODAY!

congress.isc2.org

 [#ISC2Congress](https://twitter.com/ISC2Congress)

“You have to be confident enough to sometimes take hard steps, whether as a leader or manager.”

—KIMBERLY MAHAN, CISSP,
CEO and president, MAAX Potential

WHEN TO lead, when to FOLLOW

(AND WHY YOU SHOULD DO BOTH REGARDLESS OF YOUR JOB TITLE)

BY CATHERINE KOZAK | Charisma can only go so far in the business world. Even advanced degrees and experience have their limits, especially if they were gained in other industries.

For entry-level security professionals aspiring to be great leaders and managers, success more likely will be rooted in inherent and adaptive abilities, fueled by drive, vision and instinct.

PHOTOGRAPH BY JONATHAN TIMMES

THE BUILDING BLOCKS OF LEADERSHIP

Character is key, according to four top-level cybersecurity leaders interviewed. Trustworthiness, honesty and humility were cited as the infrastructure of effective management and leadership.

“You’ve got to really be totally honest with everybody on your team and everybody that you’re reporting to up the management chain and everybody under you,” advises Gordon Rudd, CISSP, vice president and CISO of RCB Bank in Tulsa, Okla.

“You have to be able to know your team well enough to know their strengths and weaknesses. You’re going to have to work with them individually enough that they’ll believe that you’re going to help them to correct their weaknesses and give them strengths and to further develop their strengths. You’ve got to, as a leader, have everybody on your team believing that you’ve got their best interests at heart every day, all day. Now, to make somebody believe that—that has to be true.”

Emotional intelligence comes into play in both managing and leading, says Emily Morgan, CISSP, of Western & Southern Financial Group in Cincinnati, Ohio.

A leader who steps on people is “not much of a leader,” she asserts. A manager, she adds, has to “care about his/her people” and protect them.

“There’s a lot wrapped up in emotional intelligence,” Morgan declares. “Respecting people, respecting where they are, what they’re doing and how they perceive the world—because everybody sees the world differently. Honesty—that’s one of those things that I think is a given. If you’re ever dishonest, then you’re not a good leader, manager, person.”

NOT ONE AND THE SAME

Managing and leading, to some extent, are different sides of the same coin. In fact, the terms are often used interchangeably, but there are distinctions in each role. A title should not serve as the defining quality.

“Management and leadership are not mutually exclusive,” says Kimberly Mahan, CISSP, CEO and president of MAAX Potential in Richmond, Va. As she explains it, leaders think about the “why”—they set a direction. Managers think more about the “what” and “how”—they follow up on goals and make sure things get done right and on time. “In fact, to be successful, you are going to need a little bit of both.” She cites her favorite quote on the subject, from the late leadership scholar Warren G. Bennis: “Managers are people who do things right and leaders are people who do the right thing.”

Gordon Rudd relies on the military example: You can’t manage troops to take a hill. You’ve got to lead them. And there has to be someone in the back who manages delivery of guns and bullets.

“Information security is one of those things that fits in

every organization, but size does matter,” he says. “The size of the organization is going to determine where you fit. So, if they’re large enough where they’re going to need supervisory personnel, I always look for people that have demonstrated the ability to do three things: plan, organize and control.”

KNOW WHAT MAKES THE BEST LEADERS

Narcissism and deep insecurity are traits that have no place in strong leadership, Rudd says. “You know, they’ll get there and then, all of a sudden, things begin to shake, rattle and roll and parts begin to fall off and things don’t look quite as rosy as they did when that person was promoted to that position,” Rudd warns. “It happens every time.”

Self-awareness sometimes can be obscured under the warm glow of power. The solution, according to Kimberly Mahan, is “coming to terms with your own ego—or else people are less likely to follow you. For me, the types of leaders I look to are people that I want to follow or tend to follow when I think they’re inspired—when I think they’re doing things for the right reason, as opposed to just for their own self-gain.”

In essence, the ability to manage and lead springs from confidence and reliability. Both roles share the ability to guide and mentor. Leaders excel in strategizing, inspiring and innovating. Managers excel at organizing, refining and planning. Typically, as leaders climb up the ranks, they manage less. On the flip side, lower-level managers lead less. Ideally, everyone in the chain is adding his or her strengths to the company ecosystem.

Leaders think creatively, says Mark Coderre, global director at TÜV Rheinland Group in Hartford, Conn. They have good vision and good energy. They’re approachable, open-minded, not easily threatened and welcome advice. They’re self-assured, a quality that he said helped him early in his career. He remembers his then-boss asking him where he saw himself going. “I said, ‘I want your job,’” he recounts. “She loved it and she supported that.”

Coderre also counts himself among those who believe managers should also be leaders in looking after their team. “You’ve got to manage things at your level, and that will open the door for them, and sometimes you’ve got to run cover for them,” he says. “Sometimes you or your team are going to ruffle some feathers for the right reason.”

LOOK INSIDE FOR YOUR NEXT LEADERS

With the growing demand for cybersecurity professionals in both the public and private sectors, it makes sense to foster leadership from within. The Center for Cyber Safety and Education predicts that by 2022 there will be a global shortage of 1.8 million cybersecurity professionals.

As explained in a November/December 2017 *Harvard Business Review* article, “Turning Potential Into Success,”

Continued on page 19



IT TAKES MORE THAN BRAINPOWER TO BE A GREAT LEADER

BY LISA PETEN | Good global cybersecurity leadership is the kind that motivates teams, inspires individuals and makes claim to successful win-win endeavors. The qualities that make for a strong leader are not always apparent; it isn't enough to "know your stuff." There are intangibles that can hamper a leader if she or he is not wise to them. The culprit is often within ambiguity of the definition of leadership. Understanding and mastering those intangibles can support and accelerate a leader's growth and efficiency in gaining knowledge and developing best practices.

NOT EVERYTHING IS LEARNED IN BOOKS

Author Robert Fulghum gained huge success 30 years ago when he proposed that we learn many lessons of leadership as children. *All I Really Need to Know I Learned in Kindergarten* (<http://www.peace.ca/kindergarten.htm>), still a best-seller, says that we'd improve our world if adults subscribed to lessons learned before age 6—lessons like generosity, honesty and integrity.

Cybersecurity leaders might want to consider an adapted version of Fulghum's philosophy: "Everything I Need to Be a Cybersecurity Leader I Learned in Social Settings."

The most charismatic people—that is, people that you want to know and to work both with and for—in social gatherings are persuasive, assertive, engaging, knowledgeable, perceptive, demonstrative and open to others. In other words, they embody many traits of great leaders. These qualities can convert the visibility and voice of cybersecurity industry leaders into value.

Some of these qualities are inherent, but most can be learned through personal interactions in a variety of social settings. Some of these might seem common sense, but to those who seek leadership positions, how you present yourself to others is important. Is it as important as imparting and gathering knowledge to do great work? No, but people intuitively decide who to engage with based in part on how we present ourselves at events, including meetings and networking functions.

DRESSING THE PART

We've all heard we should dress for the job we want, not necessarily the job we have. But what about events outside of work? What a leader

wears makes an impact, regardless of the setting. Dress is an unspoken code signaling lifestyle, significance and impact. Significant social invitations provide guidance for a reason. Terms like "semi-formal," "business casual," "cocktail attire" and "dressy casual" provide guidelines for what's appropriate given the social setting. When in doubt, ask the host or hostess for examples of appropriate attire.

A leader's style of dress can prompt opinions, criticisms and ideas about a leader's effectiveness at the helm of their enterprise. Leaders must be careful to avoid misrepresentations and misunderstandings of their intent based on how they're dressed. Feel free to develop your own personal style, but be sure such self-expression is appropriately displayed (including on news feeds and social media platforms). The effort it takes to correct missteps can be considerable. That's why prominent leaders take measures in order to protect their image.

GIVING OFF 'GOOD VIBRATIONS'

A leader's behavior is as visible as clothing. And as crucial, if not more so. Some say leaders give off a "vibe" that can repulse or attract others without saying a word. A "high vibe" emanating from leaders creates an immediate reaction and can immediately draw warmth toward the leader and a thirst to learn more about them and the work they do or support.

The converse can be dangerous. "Low vibes" tend to repel others, creating tension and friction for the leader. Some of the most awkward moments come when we witness a leader whose low energy during a presentation is being poorly received and people start to turn on them or walk

out of the room. Leaders need to be able to “read” an audience to gauge when the reactions are not what is expected and adjust accordingly.

This brings up the issue of alcohol at professional functions or after-hours parties. It’s fine to have a drink or two to relax and join in the fun. But don’t overindulge during such downtime, and don’t egg on non-drinkers to join you. Leaders are expected to stay mindful of their purpose and well within their wits during social functions and serve as role models. Aspiring leaders should model that behavior too.

MAKING CONVERSATION

Conversation topics during social settings are as diverse as snowflakes. The duration of the social engagement, familiarity with audience present, commonality and comfort zones factor into the variety of topics discussed. Those points of discussion will vary, but it’s best to avoid subjects that may unintentionally shame, anger or offend others. After all, when socializing, the mood is bent on being upbeat. Leaders, whether in social or professional settings, are presumed to know safe topics like weather, sports or pet talk. Discussing what everyone’s learned or loved about the conference or retreat (or whatever the business function is) also is a great conversation starter. Such topics are known to less likely cause

ill regard—just don’t monopolize conversations with the antics of your pet parrot or devote your turn to speaking ill of speakers and sessions.

LEADERS ARE LIKE US—JUST MORE SO

It comes as no surprise that the roots of leadership stem from observable social norms in words, deeds and actions. More than three decades ago, Fulghum foretold his view of leadership using examples cited from a kindergartener’s perspective. Sharing, caring and even rest were addressed. Providing safe spaces to be seen and heard is a best practice at the helm of good leadership. As cybersecurity leaders endure an ever-changing landscape, it’s important that their voices be heard and advice be taken, so that organizations become stronger and more secure. This takes social skills and grace that not many of us are born with. Social settings provide opportunities for each of us to show we are astute, smart and trusting in both professional and personal settings. How you present yourself—in dress, voice and mannerisms—speaks volumes. Keep this in mind and chances are people will speak well of you. ■

LISA PETEN, *CISSP*, is founder of *Cybersity Leaders*, an organization that mentors newcomers to cybersecurity so they can master the interpersonal side of a job as they grow into their new roles.

From page 17

it is worth cultivating good people in an organization so they move up, not out. Low engagement and high turnover are extremely costly for organizations,” the authors declared, “especially if the people jumping ship are high potentials in whom much has already been invested.”

Western & Southern’s Emily Morgan believes the elemental ingredients of solid leadership candidates should be evident just by observing how everyday work is tackled. “I think you grow in that leadership as you go along,” she says. “But when I’m looking at the people on my team and seeing who has the potential to really be a leader, and consequently a manager, are they able to manage themselves? Can they manage their workload? Are they able to schedule their work, and then manage to help others? If they’re working on a team, do they naturally step up to be that team leader?”

Sometimes a person can lead, she adds, but can’t keep up with details. That’s not to say that person couldn’t be a CISO, as long as there was a deputy dealing with the day-to-day execution. Some people are wonderful at leading, but struggle with keeping on top of paperwork.

At the same time, she warns, it is wrong to devalue man-

agement. “Every time someone says, ‘We should all be leaders, not managers,’ I cringe,” Morgan declares. “Because I think it’s a misrepresentation and a slap in the face to those people who are very good managers but not really very good leaders.... But you know what? I need people who can actually execute on vision, too.”

TEACHING LEADERSHIP BY EXAMPLE

Kimberly Mahan’s company, MAAX Potential, which she founded five years ago, is an apprenticeship program that helps entry-level talent gain experience so they can move into higher-level jobs. Rather than teach leadership, per se, the company allows apprentices to be exposed to a lot of areas within technology to encourage them to determine their personal strengths and interests.

“How to be a leader starts with the conversation you’re having with the person in the mirror,” Mahan explains. “In general, it gets back to that ‘Why do you want to lead?’ I feel like you have to develop on your own, which is listening to your own sense of conscience.... The first person you ought to be able to lead is yourself. And if you’re trying to lead

because of some need to be followed, chances are you're not ready to lead."

Great leaders, she states, are confident enough to welcome other ideas and admit when they're wrong. They're not concerned with being liked. "You have to be able to overcome your insecurities. There's a very fine line between cocky and confident. You have to be confident enough to sometimes take hard steps, whether as a leader or manager. Sometimes it means telling people, 'Hey, you're not getting the job done.'"

Even at higher rungs, people can benefit from mentoring, TÜV Rheinland's Mark Coderre says. He has seen too many instances of people working at lower levels in a company who care only about checking off the next box or who just keep their head down and toil away.

"You should be leading people through their career path," he advises. Coderre recalled asking one woman in an operational role in a company what she wanted for herself in three years. "She said, 'You know, no one ever asked me that.' She did her job so well for different managers, but people just kept her in a box."

Still, even if a company lacks effective managers and leaders, he says, it should be seen as an opportunity. "Hopefully, somebody will recognize that lapse and rise

above the ranks."

If managers and leaders don't know where their people are and what they're doing, RCB Bank's Rudd says, they're not doing a good job. But at the same time, leaders have to be willing to fail, so they can learn from their mistakes. And a smart organization will provide that latitude, and help them get back on track.

NEEDED: LEADERS WHO LEAD

The bottom line, according to Rudd, is that cybersecurity professionals must set the standard of great leadership. Information technology personnel have a serious fiduciary responsibility to an organization as stewards of its data, he says. But information security specialists have an even higher responsibility.

"We're watchers of the watchers—we're the guys that are going to make sure that your secrets stay safe," Rudd declares. "We absolutely have got to be the example of how that ought to be done." ■

CATHERINE KOZAK is a freelance writer based on the Outer Banks of North Carolina. This is her first article for InfoSecurity Professional.

COFENSE

FIGHT AS ONE.

COFENSE.COM | The Power of the Collective

PHISHME® is now COFENSE

Cofense™ delivers a collective defense enabling thousands of global organizations to stop phishing attacks in progress faster and prevent breaches. Learn more at www.cofense.com.



(ISC)²

SECURITY CONGRESS

LATIN AMERICA
2018

July 25 - 26 • Santiago, Chile

Sheraton Santiago Hotel and Convention Center

ENRICH ENABLE EXCEL

The conference of 2018 will offer educational sessions presented by international thought-leadership experts. As cyber threats and attacks continue to rise, the goal of the conference is to collaborate with the development of cybersecurity professionals, providing knowledge, tools, orientations and expertise to protect their organizations.



Cloud Security



Mobile Devices / Security and Management



Gov., Regulation & Compliance



Software Assurance, Application Security



Malware



Threats



Professional Development



Incident Response & Forensics



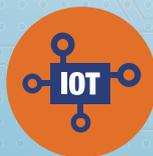
Healthcare Security



Privacy



Identity / Access Management



Internet of Things



Cybercrime

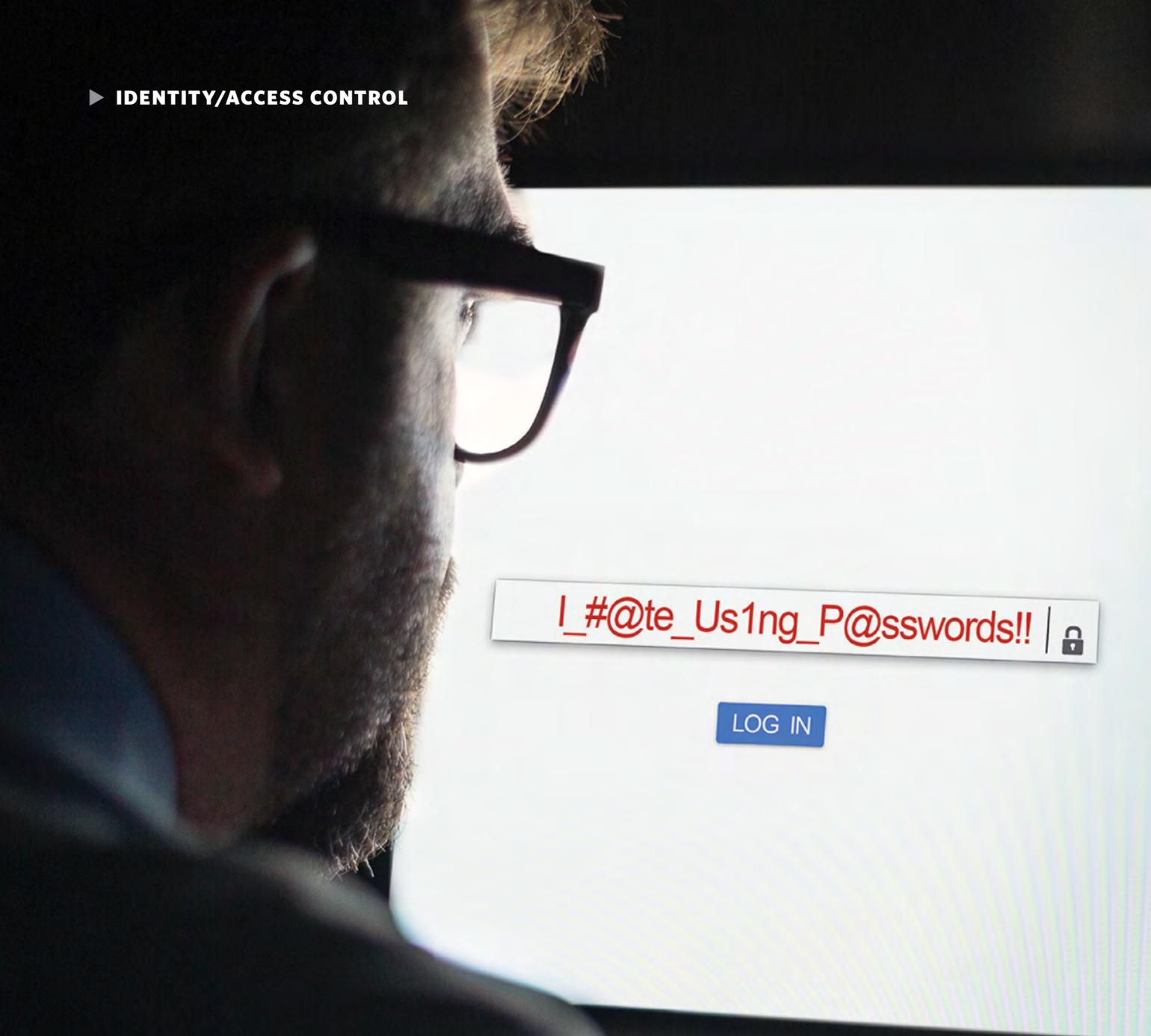


Critical Infrastructure



People & Security

(ISC)² members can earn up to 16 CPEs • latamcongress.isc2.org • [#ISC2CongressLATAM](https://twitter.com/ISC2CongressLATAM)



I_#@te_Us1ng_P@sswords!! | 

LOG IN

Every organization has its own password rules—technology may soon eliminate the confusion and frustration.

BY SCOTT J. MILLER, CISSP

AS HARD AS technology companies try to eliminate them, passwords just never seem to die. Adding functionality to help the user while still securing the targeted data becomes a complex balancing game between usability and friction. Usability should be the easy part. Friction is usually measured by the number of calls to the support line and the dreaded “failed login attempts” report. No project team wants these burdens. But absolutely no company wants to be in the latest breach headlines; securing the infrastructure and the precious data is imperative.

TOP TWO TREACHEROUS THREATS TO CLOUD COMPUTING

1. Data breaches
2. Insufficient identity, credentials and access management

Source: Cloud Security Alliance. (<https://cloudsecurityalliance.org/download/top-threats-cloud-computing-plus-industry-insights/>)

THE PASSWORD MAZE

The challenge begins with the user input screen. Properly handling the new user registration, password resets, user deletion and regulatory compliance about retaining personal information can be tricky. For the password field itself, there are the password restrictions. We are all too familiar with the rules: *No less than 8 characters. Must contain at least one of each of the following: one lowercase letter, one capital letter, one number, one symbol. It must not contain any part of your name, the name of the site, three or more consecutive numbers or letters. Must not be one of three previously used passwords.*

These rules alone confuse users and force them to either reuse passwords or create a base password with minor changes for each site and for password updates—P@ssWord1-1, P@ssWord1-2, etc. Again, weakening the process. According to the Digital Guardian (<https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic>), the average email address is associated with 130 online accounts.

Some sites are more restrictive, some less. The restrictions are usually an agreement among the company's UI team, sales team and legal department. Some companies also have a customer experience team.

HOW COMPLEX IS TOO COMPLEX?

To minimize the friction, it's important to keep the cycle time low and the identity challenges to a minimum. Exceeding an acceptable login time or presenting too many challenges or too difficult a challenge creates user frustration, failed logins and calls to first-line tech support.

Many companies use just the username and password for access, but others employ security questions, security images and even user history (credit data) to protect the logins. The effectiveness of these is highly debated. I had difficulty recently when I could not remember what year I refinanced my home, or what bank had my first car loan. If it's too complex or difficult, human nature will try to bypass it or simply won't do it.

The login sequence can touch several servers or several different product suites before routing the user to one of several applications depending on the company's investments and security architecture policies.

In one of my previous assignments, the sequence touched no fewer than seven server sets, each providing a different risk assessment of the attempted login. Various SAML and REST processes were used to pass this information between the disparate systems. All of this is outside of protecting the user pages themselves. The developers have the responsibility of the basic web security: input field

verification, injection attack prevention, cross-site scripting prevention, third-party library code reviews, bug testing, etc.

The entire login cycle could exceed three minutes. Totally unusable.

TECHNOLOGY TO THE RESCUE

Google and Microsoft are two of the tech leaders that have announced plans to do away with traditional passwords. Cutting-edge techniques for verifying the user's identity are now available: browser fingerprinting, device fingerprinting, geolocation, geo-fencing, login velocity, out-of-band verification, biometrics or behavioral analysis. Combining a few of these features can minimize the risk and more securely protect your users' data.

User history: Does the data presented match the data the user logged in with previously? If so, maybe we allow the user to log in. If, however, some of the key elements are different (reported IP, language pack loaded, browser, OS) we step up the authentication verification and query the user for more proof.

Location tracking: Geolocation can be one part of an overall login risk assessment, but by itself is not as reliable since IP address location indicates the internet jump-on point and not the user's true location. Cellphones rarely match the user's location as they report the location of the carrier's peering point. The use of VPNs also invalidates this test. Geo-fencing allows a broader test over user IP and combined with geolocation and log-in velocity (minimal time between login attempts) could track users with far more accuracy. For example: John Doe just logged in from Atlanta 30 seconds ago, but now he's in Germany? More



technical users may be deploying VPN jumping or using different VPN proxies' locations daily or several times per day.

Out-of-band authentication is typically your second factor—something that the user has: a token, a cellphone, a mobile app or access to an email address. This is typically considered the single best approach for stepped-up authentication. Adoption of two-factor authentication (2FA) is on a steady increase with the general population.

Biometrics are also increasing in popularity thanks to cellphone companies. Users are still skeptical, though: “If a breach occurs and you lose my password, I can just change it. However, if you lose my fingerprint now what?” The user doesn't know that a system will store a mathematical equivalent of the fingerprint and not the actual image of the print.

Behavioral analysis can add an additional identity test. Does the user's login attempt match his/her historical login schedule? Does the speed of the typing match? Are the mouse movements the same as previous visits?

LOOKING TO THE CLOUD

Creating an in-house solution can quickly overwhelm a project team, so some organizations turn to shared trust models like cloud providers.

A third party (relying partner [https://en.wikipedia.org/wiki/Relying_party]) is retained to vouch for the user's identity. Two examples: using your established LinkedIn identity to gain access to a career site, or using your stored fingerprint on your phone to gain access to your (401)k site. These use OpenID, OAuth, OpenID Connect (ODIC) and OAuth 2.0 bearer tokens to pass around the authentication or authorization token. Many users remain skeptical, wondering if their social media identity is compromised, are all their connected sites compromised as well.

There are numerous cloud providers lining up to offer these services from the powerhouses like Microsoft and Google to the social media platforms. There also are a growing number of companies that focus just on the authentication and authorization components of IAM, like Okta and InAuth. These are known as Identity as a Service (IDaaS) providers. [Note: (ISC)² just recently started using Okta for some of these services.]

A WORK IN PROGRESS

Some of the latest and greatest work is being done by the FIDO Alliance (<https://fidoalliance.org>). FIDO means Fast IDentity Online. Many of these previously mentioned providers are members. They are all working together to provide a simpler, password-free method of user identity

11 MOST COMMON PASSWORDS OF 2017

(compiled from 5 million leaked by hackers)

1. **123456** (Unchanged)
2. **Password** (Unchanged)
3. **12345678** (Up 1)
4. **qwerty** (Up 2)
5. **12345** (Down 2)
6. **123456789** (New)
7. **letmein** (New)
8. **1234567** (Unchanged)
9. **football** (Down 4)
10. **iloveyou** (New)
11. **admin** (Up 4)

Source: <http://fortune.com/2017/12/19/the-25-most-used-hackable-passwords-2017-star-wars-freedom/>

verification. Their initiative is stated as “simpler, stronger authentication.” For all our sanities, let's hope so. But until then, we all have to deal with these pesky passwords. ■

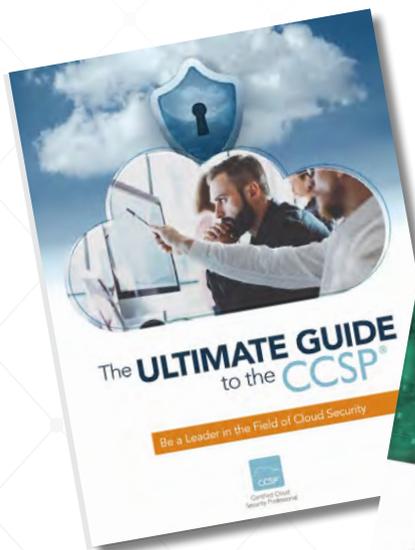
SCOTT J. MILLER, CISSP, is a certified cybersecurity professional with more than 25 years of experience. He is the owner of SMACC LLC: Analytical Certified Consulting, which provides CIO/CISO consulting services for enterprises of all sizes. Scott can be reached at sjmiller@smaccllc.com and [linkedin.com/in/scottjmiller](https://www.linkedin.com/in/scottjmiller).



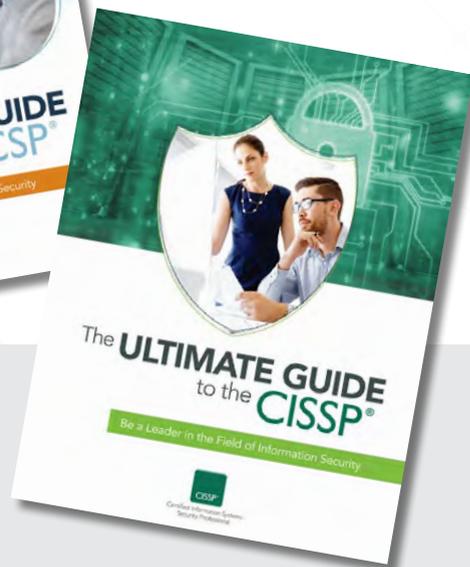
THE NEXT BIG THING



CCSP and CISSP top "The Next Big Thing" list as the #1 and #2 certifications that CertMag's Annual Salary Survey respondents plan to earn in 2018.



Is the CCSP or CISSP on Your 2018 To-Do List?



Get Your Free Ultimate Guide to Get Started.

[Get My CCSP Guide](#) 

[Get My CISSP Guide](#) 

CERTIFICATION AND ACCREDITATION:

Beyond the Rubber Stamp

How much should we trust the process used to determine the security-worthiness of a product or service? By Jason McDowell, CISSP



AS INFORMATION SECURITY PROFESSIONALS, we stand guard at the gates of nearly every enterprise in operation today. Stakes continue to rise for information breaches, with a seemingly never-ending list of compromised networks that publicly showcase outdated or neglected data security practices.

In an always-on, always-connected world where everything from refrigerators to enterprise-level routers serve as attack vectors, how do we secure such a broad landscape of products and services?

ILLUSTRATION BY ENRICO VARRASSO

We rely on tools and processes that provide some assurance that they align with our risk tolerance. Certification and Accreditation (C&A) is one such process.

C&A is used in various industries; in information security, we rely on the process by which independent testing facilities test and then certify products and services. Based on the level of assurance required, cybersecurity professionals can then make intelligent and informed decisions on what products and services are acceptable for their networks.

With such trust in—and reliance on—the C&A process, it is only prudent that (ISC)² members have a firm understanding of what comprises C&A, as well as the process's strengths and potential weaknesses. Additionally, as cybersecurity professionals, we must do our due diligence while sifting through the plethora of available certified products and services, and find those that best fit our needs.

C&A BASICS

Let's begin with the basics of proper terminology.

Most commonly, C&A refers to any process that vets a product or service based on a specific standard or set of requirements. Looking at the process a bit more granularly, the term "certification" generally applies to the product or service being vetted. Certification is also synonymous with other similar words, depending on the C&A program (e.g., validation for FIPS or authorization for RMF).

Products and services obtain certification, whereas independent testing facilities obtain accreditation.

Accreditation applies to the independent testing facility responsible for vetting the product or service in adherence with a specific standard or set of requirements set forth by the validating organization. In other words, products and services obtain certification, whereas independent testing facilities obtain accreditation.

Accreditation is usually provided to the testing facilities by the validating organization that specifies a standard or set of requirements against which the product or service is tested. The validating body, upon successful and acceptable testing by the independent testing facility, is usually the one who issues the certification for the tested product or service.

Fundamentally, C&A is not a hard concept to grasp;

however, it is surprising how interchangeable C&A terminology has become. When researching a product or service for your organization, it's always a good idea to understand the industry's vocabulary.

GOALS AND CHALLENGES

At its core, the C&A process is a means of assuring that the product or service works as intended and in the manner specified by the manufacturer. For example, an electrical circuit breaker rated for 15 amperes will, in fact, open the circuit at a current higher than 15 amps. Or, a cryptographic library will, in fact, use and generate only 2048-bit key pairs as specified in the documentation. Without C&A, our assurance of these kinds of operational details would be minimal at best, and would rely almost solely on the claims of the manufacturer or developer. Thus, we could easily end up with a 15 amp breaker that trips at 17.5 amps, and a cryptographic library that possibly uses 1024-bit keys. These examples demonstrate the primary intent and goal of nearly all C&A processes.

As with any human-made process, C&A is not without its challenges.

First, keep in mind that C&A is central to some business models, and as such, profit is a major driver. For instance, waning profits may translate into an internal push by the testing facility or the developer to accelerate certification efforts to make up for revenue shortfalls. For independent testing facilities, this may mean the inability to test with the level of scrutiny it did in the past. Although still meeting the minimum requirements of a specific standard, the level of assurance offered may not be of the same quality or completeness as it was when the project completion rate generated a healthy bottom line.

Second, an independent testing facility's primary purpose, which is the accurate and comprehensive vetting of a product or service, is many times in direct opposition to the goals of its customers. From the testing facility's perspective, each product or service being tested will require a specific amount of time based on the depth and breadth of the certification being accomplished. From the customer's perspective, time is money. A product or service sitting in a testing facility is money lost, and there is always the looming threat of another competitor getting their product or service certified and out in the marketplace sooner.

The opposing goals, and somewhat contentious relationship between the independent testing facilities and their customers, is not only required to enable the C&A process to work, but also a part of the natural beauty of what makes it effective.

Independent testing facilities work as a pseudo gatekeeper, with the intention of passing along only those

products and services that are deemed fit enough to endure and survive the final analysis by the validating organization. A breakdown in the chain could lead to products and services obtaining certification that do not meet the minimum requirements, or, worse yet, function in an insecure and unpredictable manner. Though not commonplace, this unfortunate scenario does happen; we see it in the form of product recalls, off-schedule firmware updates and certification revocations.

Implementing a security solution without understanding how it provides that security isn't really secure at all, so take the time to research and review all available documentation.

Although not the intent of the independent testing facilities or the customers of these facilities, sometimes profit-driven scheduling can push a certification effort toward speed at the expense of quality. When we're looking for a certified product to implement in our networks, we need to keep the above challenges in mind, and think beyond the rubber stamp of the C&A process. We need to do our due diligence and research what we're buying into.

Let's take a look at a few things we can do to safeguard ourselves from acquiring a less than quality certified product or service.

DUE DILIGENCE AND CERTIFICATION

Knowing the fundamental challenges of the C&A process, a thorough review of the certified product or service before purchase is key to acquiring something you can trust to be on your network.

Considering the assurance levels of the certification program is only the beginning. As security professionals who hold the keys to the doorway of our company's resources, we not only need to judge a product or service by its identified level of assurance, we need to be intimately familiar with what that level of assurance represents. For example, let us say your company's cryptographic equipment acquisition policy requires a certification of at least level two. Before purchasing any products or services that are certified to level two, do you understand what the requirements are for a level-two-certified product? Will a level-two product or service integrate well into your environment,

or would a level-three product complement your current processes better?

Implementing a security solution without understanding how it provides that security isn't really secure at all, so take the time to research and review all available documentation. Nearly all certified products or services have publicly available documentation available for analysis, and many times, obvious red flags can be found by a single read-through of the manufacturer's or developer's documentation.

Additionally, research current events related to the manufacturer or developer whose product or service you are considering. If there were any reported breaches or questionable business practices that have come to light in the last couple of years, it may be wise to look at competitors before making a final decision. It's also not far-fetched to contact a manufacturer or developer to obtain more detailed documentation on a certified product.

Lastly, consider the longevity of your investment; in other words, future-proof and keep abreast of changes to the standard or requirements upon which your potential product or service is certified. Standards and requirements evolve over time due to advancements in technology; thus, what is acceptable this year, may be less so the next. A little due diligence now could prevent substantial replacement and upgrade headaches in the future.

IN THE END, IT COMES DOWN TO TRUST

At the end of the day, it all comes down to trust. Whatever product or service you are looking to acquire, a security-minded individual will always ask him or herself if the product or service being introduced is trustworthy.

We can use C&A as a means of determining how much trust to provide for a product or service based on independent testing and subsequent certification. But, we must always keep in mind business pressures that may generate a higher risk of human error.

In truth, a certified product or service is only as trustworthy as the process that certified it; therefore, put your faith in not just an assurance level, certificate or stamp, but also in your own research and understanding of the rigors against which it was tested. An ounce of prevention is worth 10 pounds of cure in the security industry, so stay safe by reaping the benefits of C&A, while also being mindful of its limitations. ■

JASON McDOWELL, CISSP, is an (ISC)² member based in Santa Maria, Calif., where he works as an information systems security analyst for Orbital ATK. His last article for InfoSecurity Professional was on RMF.

It's Now Easier to be a Cyber Safety Ambassador

IF YOU HAVE BEEN a supporter of the Safe and Secure Online program or the old (ISC)² Foundation, you may have taken the time to jump through all the hoops we asked of you to become an authorized volunteer. If you happened to live in one of the approved countries, completed an application, submitted a background check (which the local school often made you do again anyway) and attended an orientation, we would give you the secret password to the secret website. Only then did you have the privilege of downloading PowerPoint presentations to show to your local schoolchildren, parents or senior citizens.

Could we have made it any harder to help spread the word and teach people how to be safe online?

Well, I am thrilled to announce that effective immediately, that cumbersome process is officially gone.

Now, it is easier than ever to become a volunteer ambassador and promote cybersafety in your community. All the materials you need to help make it a safer cyber world are available for free on our website, www.IAmCyberSafe.org. We have new presentations available for children, parents and senior citizens, with more to come throughout the next year.

Instead of all that old paperwork, now you simply register at the site, let us know what materials you need and then download them. It's that easy. You are free to use the branded and copyrighted materials at your convenience at your local school, community center, library, Scout group, church or even your own company. We only ask that you not change any of the slides without checking with us first, that you report back on what you did, how many people attended and share any feedback. (Note: Yes, as an (ISC)² member, you still get CPEs for volunteering.)

Volunteer ambassadors play an integral role in our mission

to change lives and shape our cyber community. Under the new process, you choose when, where and how to volunteer, and we provide the resources to help you make an impact in your community. You can even order event supplies on our website (<https://www.cybersafetykits.org/collections/ambassador-materials>), including materials to display at your company or in your community, that promote our cyber safety and scholarship programs. All you need to pay is the shipping cost.

Instead of all that old paperwork, now you simply register at the site, let us know what materials you need and then download them. It's that easy.

We are excited to work with you to organize a cyber-safety campaign that best suits you, your company and neighborhood. Whether it's a financial sponsorship, a "school takeover" or an educational event, we can work with you to make a real impact in your community.

Need materials in another language? Help us get all our programs—including the Garfield cartoons and comic workbooks—into your native tongue. We are ready to make this happen and need your help.

Your Center staff (all five of us) are doing everything we can to spread the word, but we can't cover the entire globe. We need your help reaching local schools, companies and libraries. Follow us and share your stories on Facebook (<https://www.facebook.com/IAmCyberSafe/>), Twitter (<https://twitter.com/ISC2Cares>), Instagram (<https://www.instagram.com/iamcybersafe/>) and LinkedIn (<https://www.linkedin.com/company/center-for-cyber-safety-and-education/>). If you have questions, suggestions or want to help in some other way, we'd love to hear from you. Please contact us anytime 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.

lead in

(ISC)² MEMBERS AND EXPERTS
FOCUSED ON LEADERSHIP
AND PROJECT MANAGEMENT

KATSUHIKO NAKANISHI



Katsuhiko Nakanishi, CISSP, works for NEC Corp. in Japan and currently is the manager in the Public Safety Business Promotion Office for the 2020 Tokyo Olympics and Paralympics Promotion Division. Last year, he was awarded an Asia-Pacific Information Security Leadership Achievement (ISLA™) for his contributions to cybersecurity human resource development for the 2020 summer games, including building a CSIRT, examining cyber exercises and collaborating with government organizations.

Nakanishi has experience in web application development and data center infrastructure building,

involvement in development and support of WAF, security diagnosis work, as well as incident response inside and outside the company. He has more than 10 years of experience in information security consulting services and incident response for various NEC Corp. customers in Japan.

At the Information Security Operation Providers Group JAPAN (ISOG-J) steering committee, he contributes to improving the status of security engineers and raising awareness of security operations services. Since 2012, he has engaged in building a cyber range for a “Hardening Project.” In addition, he was responsible for scenario creation and lectures of cyber exercises for ministries and important infrastructure.

How did you come to be part of the Tokyo Olympics?

Our company has been a gold sponsor of the Olympic and Paralympic Games since February 2015. Two months later, I began to work for the Tokyo Organizing Committee of the 2020 Olympic and Paralympic Games as a cybersecurity expert.

What are some unique cybersecurity issues in protecting the Olympics?

The Olympics are watched by more than 3.6 billion people (based on the

2016 Rio games).

Cyberattacks by hacktivists and criminal elements are a concern. In the event technological infrastructures like the energy grid, telecom and broadcast networks become a target, we will have to work in cooperation with government and private infrastructure providers.

Tell us what it was like to receive an (ISC)² leadership award.

I’m very grateful to receive such an honorable award. This is not a

personal award. I’m very grateful to project members and to my family, and will keep doing my best to uphold the honor that comes from receiving this award.

What is the best part of being a cybersecurity leader?

Operating under unambiguous policies with clear criteria that were formally approved by the organization enhances our ability to lead. An example of one such policy is the (ISC)² Code of Ethics.

What is the most challenging part of being a cybersecurity leader?

Selecting what is a priority among a vast array of information to protect the organization from new threats. It’s also important to explain the importance of measures to stakeholders, such as executives and users, and encourage them to act to protect themselves and the organization.

What advice do you have for others who want to become leaders in their respective fields?

Actively participating in community activities is important. Our community can provide us opportunities to communicate with other organizational leaders. Information about cybersecurity should be shared with other organizations, even if they are competitors.

Leaders from other organizations also provide us with a lot of insights. ■

An expanded version of this interview will appear in the June issue of *Insights*, a companion e-newsletter for the (ISC)² membership.

Join the new

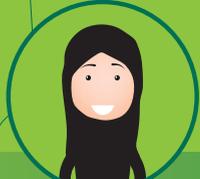
(ISC)² Community!



For cybersecurity and IT professionals

**CONNECT.
COLLABORATE.
SHARE.
DEVELOP.**

community.isc2.org





NEW WAYS TO EXCEL

Online Self-Paced Learning to Enrich Knowledge and Enable Success

Fuel your growth through online self-paced courses allowing you to learn at your own pace when it's most convenient for you. Keep your skills relevant and knowledge of evolving trends current.

Earn your CPEs through these available trainings:

- » MindEdge Self-Paced Cybersecurity Courses
– 15% Discount for (ISC)² members
- » Secure IoT Networks
– 50% Discount for (ISC)² members
- » UCF Compliance Mapping Certificate Course

GET FULL DETAILS AT:

www.isc2.org/CPE-Opportunities 



New immersive, self-paced learning opportunities coming soon from (ISC)², with topics on General Data Protection Regulation, Building a Strong Security Culture and Integrating Security into DevOps. It's all part of our mission to enrich and enable so you can excel.

