LISTEN UP, WILL YOU? • 5 MINUTES WITH JULIETTE KAYYEM

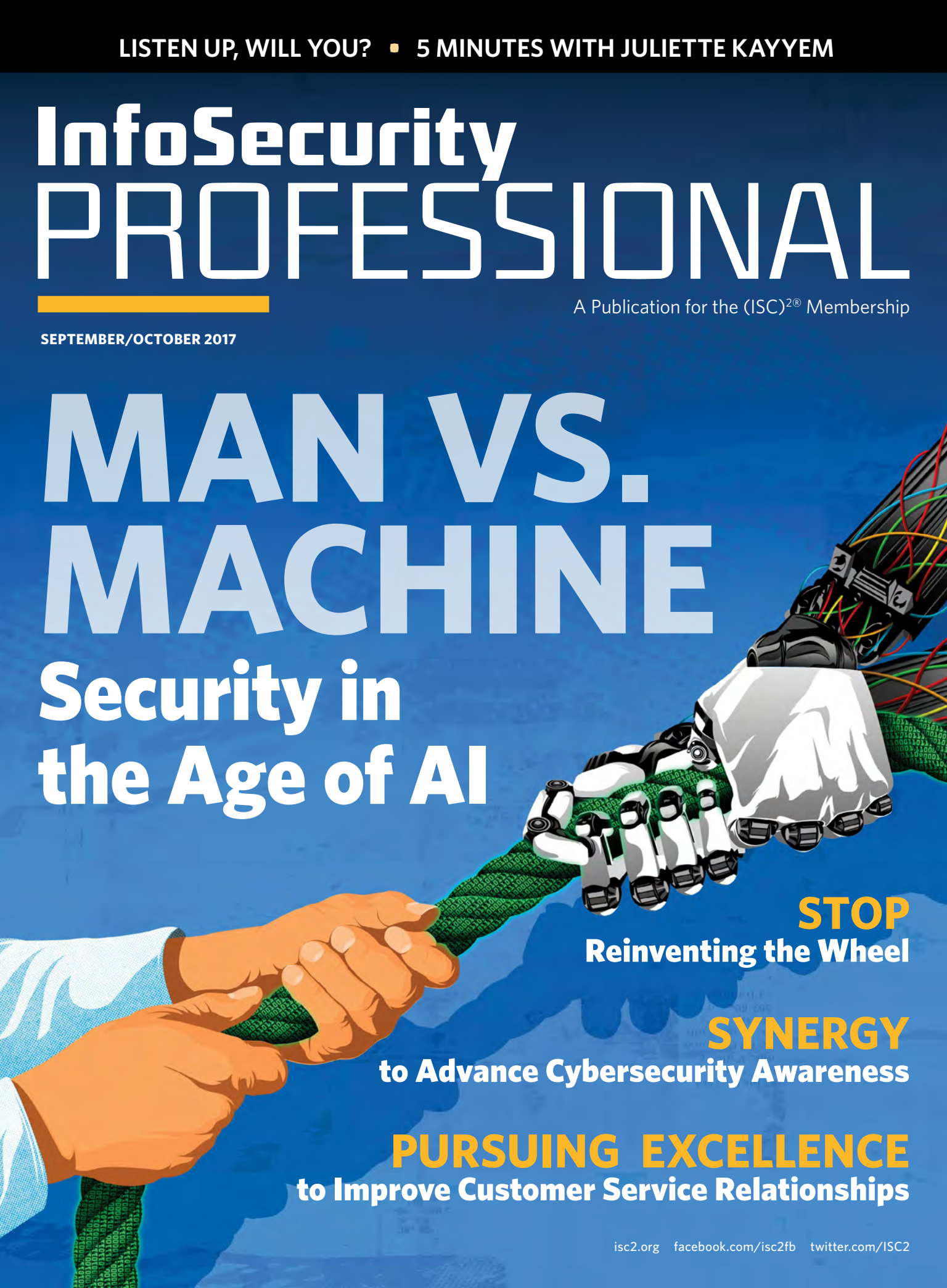
InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

SEPTEMBER/OCTOBER 2017

MAN VS. MACHINE

Security in the Age of AI

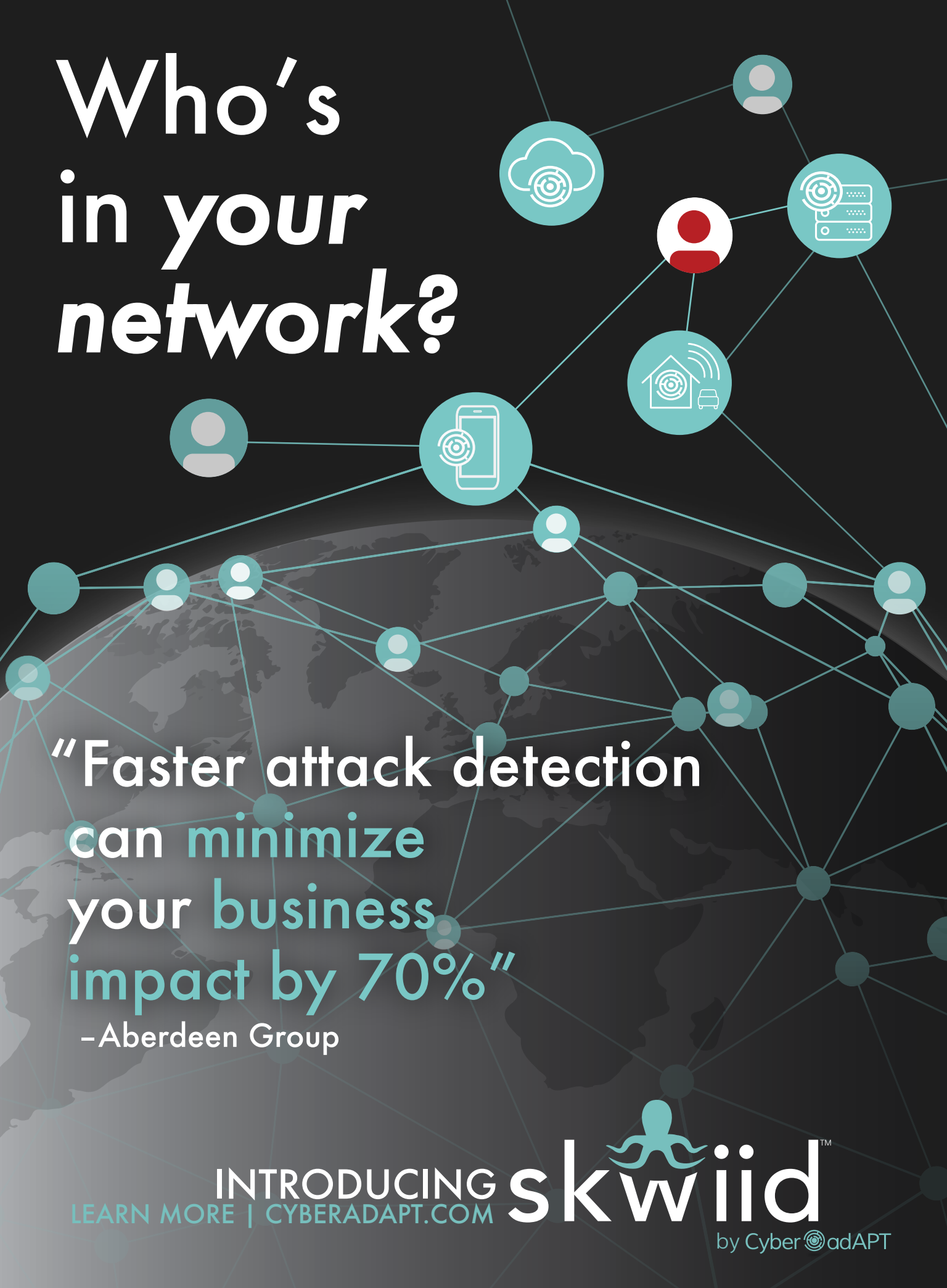


STOP
Reinventing the Wheel

SYNERGY
to Advance Cybersecurity Awareness

PURSUING EXCELLENCE
to Improve Customer Service Relationships

isc2.org facebook.com/isc2fb twitter.com/ISC2


Who's in your network?
"Faster attack detection can minimize your business impact by 70%"
-Aberdeen Group
INTRODUCING skwiid™
LEARN MORE | CYBERADAPT.COM
by CyberadAPT

contents

VOLUME 10 • ISSUE 5

Ways to generate greater security awareness without adding costs. PAGE 24

features

Cover illustration: TAYLOR CALLERY. Image *(above)*: JAMES KACZMAN

departments

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

editor's note

BY ANNE SAITA

Listen Up, Will You?

It takes skill to soak in what someone else is saying.

I'M A LONGTIME FAN of broadcast journalist Charlie Rose, whose late-night interview show has been a PBS staple for decades. His stellar reputation (backed by decades of awards) comes from asking tough questions of world leaders and celebrities, and keeping on-air talks, however uncomfortable, from sounding stilted. It takes great skill to artfully press people when they provide empty or erroneous responses or to let silence speak volumes instead of filling the void with useless chatter.

Mastering the art of active listening is critical to (ISC)² members who want to advance in their careers. At the entry level, you need to carefully consider others' words to respond appropriately during a job interview. Later, meetings provide a number of mines to avoid, from staying silent too long to avoiding rudely interjecting or talking over someone, especially if the gathering becomes heated. Even in our personal lives, we sometimes have trouble truly hearing what a friend or loved one is telling us before we make regretful mistakes.

Good listeners periodically ask questions that gently challenge or clarify assumptions on the speaker's part. They don't have to win an argument. And they don't have to monopolize the conversation (though they do have to contribute to it). They allow others to have their say and make someone feel supported, even if they disagree with them. They make suggestions that are constructive, not critical.

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

In other words, good listeners leave everyone feeling like they were truly heard and understood. This issue includes different ways we now interact, with machines and each other. Our cover story is about the melding of artificial intelligence and machine learning, both of which require human interaction to work. Two (ISC)² members suggest ways to collaborate for greater security awareness and to ensure executives actually hear what you communicate about cybersecurity.

We at the magazine listen to our members too. Right now, we're developing stories to cover in 2018, so if there's something within professional development you'd like us to cover, please send me an email at asaita@isc2.org. When it comes to hearing your ideas, I'm all ears. ■

advertiser index

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

InfoSecurity PROFESSIONAL

(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 D'Alessandro
727-877-2230
adalessandro@isc2.org

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

MEDIA SERVICES MANAGER
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 MANAGERS
Lisa O'Connell
781-460-2105
loconnell@isc2.org

Mike Magno
781-569-6630
mmagno@isc2.org

EDITORIAL ADVISORY BOARD

Carlos Cañoto, South America
Kaity Eagle, (ISC)²
Tushar Gokhale, U.S.A.
Jarred LeFebvre, (ISC)²
Javvad Malik, EMEA

TWIRLING TIGER MEDIA EDITORIAL TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

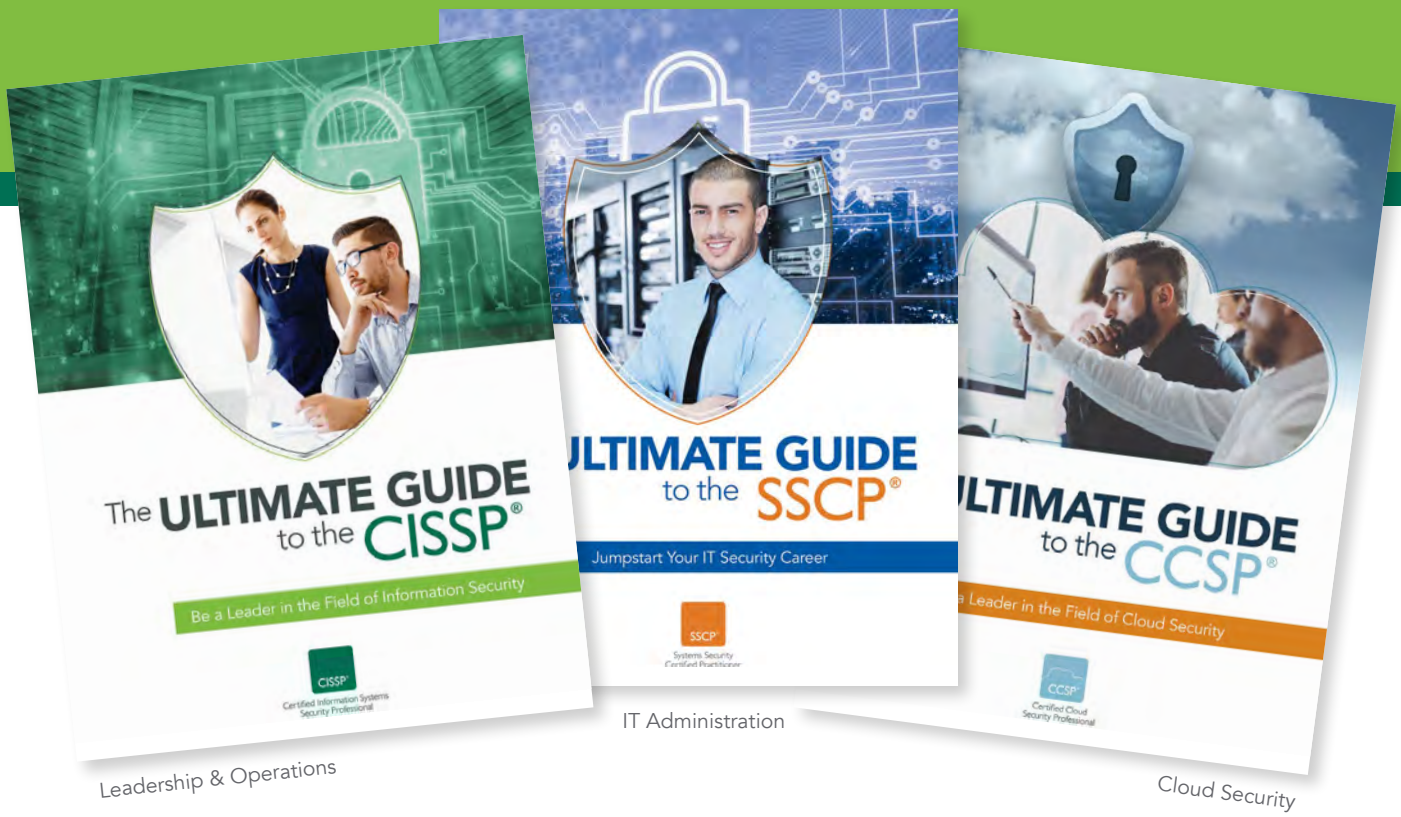
MANAGING EDITOR
Deborah Johnson

PROOFREADER
Ken Krause

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

RETURN TO CONTENTS

The ULTIMATE GUIDES *to the* Ultimate Cybersecurity CERTIFICATIONS



Leadership & Operations

IT Administration

Cloud Security

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

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

Get the ULTIMATE GUIDE today.

edu.isc2.org/ultimate-guides

These guides include:

- ✓ Fast facts of the certification
- ✓ An overview of the exam
- ✓ Benefits of the certification
- ✓ Setting yourself up for success
- ✓ Steps to getting certified

(ISC)²

THE LATEST FROM (ISC)²'S LEADERSHIP

letter to members

FROM THE PROFESSIONAL PRACTICES COMMITTEE

What to Consider When Filing an Ethics Complaint

Photograph: Thinkstock

(ISC)²'s Professional Practices (Ethics) Committee receives a significant number of "complaints" along the lines of "you have certified so-and-so who does not have the requisite experience." "Complaints" is in quotes for a number of reasons. The first is that many of these are really assertions rather than sworn complaints. Not having sufficient experience for certification is not, per se, an ethical violation. However, falsely claiming to have such experience is.

In order to protect (ISC)² members from frivolous complaints, the Committee requires an ethics complaint be based upon firsthand knowledge and sworn testimony of that knowledge. Further, it requires that complaints be sufficiently specific so that, if untrue, they can be rebutted. They require that the complainant have standing; that is, that there be injury to the complainant attributable to the acts or omissions specified. (Misrepresentation of qualifications is presumed to constitute injury to the profession, at a minimum.) These requirements place the burden of evidence on the complainant, while the benefit of any doubt goes to the accused. Finally, given that the Committee cannot compel evidence, these procedures mean the Committee must decide only on the evidence it is given.

It might seem as though an assertion that someone does not have the requisite experience would be simple enough to resolve. However, the accused has already provided evidence of experience. Specifically, applicants provide a resume, a brief written account of personal, educational and professional qualifications and experience, along with a signed attestation to the truthfulness of the documents provided. Moreover, the application, including the resume and statement, must be endorsed by a certified professional.

The Committee takes the qualifications for certification seriously: a candidate's experience is just as important as professional knowledge. While evidence of experience may not be as objective as that of the knowledge, we are satisfied that the procedures for testing it are adequate and serve us well. (ISC)² staff members do evaluate all claims of experience, test to ensure that only "professional" experience is counted and ask for corroboration of those claims in randomly selected samples of applications.

> **An assertion that someone is not qualified raises issues not only for the applicant, but also the endorser.**

These procedures rely heavily on an applicant's professional endorsement as well as experience claims. The professionals who endorse applications are responsible for the information within those documents. An assertion that someone is not qualified raises issues not only for the applicant, but also the endorser.

Often complaints are withdrawn once these procedures are explained. Perhaps, upon reflection, complainants realize that, whatever the facts may be, they are not able to provide sworn, first-person evidence.

That doesn't mean members shouldn't continue to bring suspected ethical violations to our attention. Just be sure when it comes to challenging someone's experiences, the complainant can provide proof. The integrity of the profession requires that we police one another. On the other hand, given that the Committee does not have the resources to investigate mere suspicions, nor the authority to compel testimony, members should only lodge complaints when they can provide evidence to support them. ■

APAC Secure Webinars

(ISC)² Security Briefings

Watch Free Webinars Live/On-Demand
Anytime, Anywhere

Subscribe Now!

Visit https://www.isc2.org/en/News-and-Events/Webinars/APAC-Webinars

1 cpe

Earn 1 CPE per Webinar*

*will automatically be added to the (ISC)² members' profiles.

To Speak. To Sponsor. Contact mpark@isc2.org

field notes

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

EDITED BY DEBORAH JOHNSON

(ISC)²® Congratulates the 2017 Asia-Pacific Information Security Leadership Achievements (ISLA®) Honorees

TWENTY-FOUR INFORMATION security professionals from the Asia-Pacific region were honored at the 11th annual ISLA presentation this summer during a gala at the Sheraton Hong Kong. The ceremony was held concurrently with (ISC)² Security Congress APAC.

Congratulations to the following 2017 honorees:

Information Security Educator

- Dr. Do Young Kim, CCFP-KR, professor, KwangWoon University (Korea)
- Prof. Pauline C. Reich, founder/director, Asia-Pacific Cyberlaw, Cybercrime and Internet Security Research Institute, Waseda University School of Law (Japan)
- Dr. Hidehiko Tanaka, life fellow of IEEE; professor emeritus, The University of Tokyo (Japan)

Managerial Professional for Information Security Project(s)

- Yoshiyuki Kuwahara, CISSP, chief of information strategy, Hiroshima Prefectural Government (Japan)

Information Security Practitioner

- Jae-hwan Baek, ENCE, CCFP, information security specialist, Ministry of Culture, Sports and Tourism, Republic of Korea (Information Security team) (Korea)
- Hoi Kit Martin Chan, program director, (ISC)² Hong Kong Chapter (Hong Kong)
- SangMyung Simon Choi, director, Hauri, Inc. (Korea)
- Wei Gu, CISSP, CCSP, CISM, AsiaPacific information security team leader, AstraZeneca (China)
- Po Lun Ho, OSCP, SANS GWAPT, SANS DFIR, researcher, VXRL (Hong Kong)
- Dr. Chih-Hung Hsieh, R&D manager, CyberTrust Technology Institute, Institute for Information Industry (Taiwan)
- Thanongsak Kijronee, assistant manager, Provincial Electricity Authority (PEA) (Thailand)
- Lan-Fen Lin, MBA, ISO 27001 LAC, head, Information Security Department, 104 Corp. (Job Bank) (Taiwan)
- Chia-Yi Wang, section head, National Center for Cyber Security Technology (Taiwan National Computer Emergency Response, TWNCERT) (Taiwan)

Senior Information Security Professional

- Dr. Joongsup Choi, CISO/head of information security department, NEOWIZ (Korea)
- Dr. Ricci S.C. Ieong, CISSP, CCFP-US, CCSP, principal consultant, eWalker Consulting (HK) Ltd. (Hong Kong)
- Kwok Wai Kin Ip, CISSP, CISM, CISA, manager, Risk Advisory, Deloitte China (Hong Kong)
- Dr. Xiapu Luo, research assistant professor, The Hong Kong Polytechnic University (Hong Kong)
- Dr. Jungchan Na, managing director, Electronics and Telecommunications Research Institute (Korea)
- Katsuhiko Nakanishi, CISSP, manager of Public Safety Business Promotion Office, Tokyo Olympics and Paralympics Promotion Division, NEC Corporation (Japan)
- Sarah Taylor, strategic management and quality manager, CyberSecurity Malaysia (Malaysia)
- Sen Ueno, president, Tricorder Co. Ltd. (Japan)
- Dr. Yu-Chih Wei, CISSP, CISM, CISA, researcher, Telecom Laboratories, Chunghwa Telecom Co., Ltd. (Taiwan)
- Xin Xu, CEO/president, Beijing secPoint Technology Co., Ltd. (China)
- Daisuke Yogi, CISSP, senior manager, Business Promotion Department, NRI SecureTechnologies, Ltd. (Japan)

(ISC)² EMEA Moving Forward with Members

Advisory Council driving influence and priorities since 2004.

ON MARCH 3, 2004, a group of 12 senior information and IT security professionals came together in Brussels, Belgium, for the first (ISC)² EMEA Advisory Board meeting. Their aim was to support (ISC)² development in the region.

At the time, there were about 3,000 certified members in Europe, with most in the United Kingdom and Benelux areas. The group of 12 hailed from six countries, bringing much-needed local insight; they also revealed developing attitudes toward (ISC)². This helped to tackle both misconceptions and relationships that would influence the (ISC)² mission to develop our profession in the region.

John Colley, CISSP, then chair of (ISC)²'s Board of Directors, summarized the challenge ahead for the volunteers: "The European Advisory Board is tasked with helping to elevate information security as a boardroom issue and, as a consequence, to promote professional security accreditation in Europe, where, historically, it has been poorly embraced."

The Brussels meeting was an important first step in what has become a long-standing commitment to work with members keen to take ownership in and help develop (ISC)². A lot has changed since. Now known as the EMEA Advisory Council (EAC), it supports development in the Middle East and Africa, as well as Europe, and can draw from the experience of the nearly 22,000 members in the region.

Members make their way onto the council today by making a project proposal or being invited to support work they are already doing. There are currently 10 members sitting on the EAC, many of whom are or have been chapter leaders or volunteers with (ISC)² in another capacity. All are highly motivated to champion efforts, and, over the


Yves Le Roux and Geoff Harris with David Shearer at the Dublin meeting, 2016.

years, a few have gone on to be elected for the (ISC)² Board of Directors.

"The EAC has always been a facility for understanding current concerns across the (ISC)² membership. As the membership grew, it also became a facility for members to get active and support each other, either as volunteers, or simply by reaching out to let us know the issues they would like us to tackle," describes EAC co-chair Yiannis Pavlosoglou.

Often the work has impact beyond the region's profession, including a significant effort to enhance cybersecurity content within computing science education and the European eCompetence Framework. The EAC's efforts were also instrumental in the development of the Chapter Mentorship program, which supports chapters around the world.

Another project, the EAC GDPR Taskforce, led by the EAC's other co-chair, Yves Le Roux, brings members together to compare experience in implementing Europe's new General Data Protection Regulation. Launched in late 2016, 12 volunteers meet monthly by conference call, and are running a series of workshops at (ISC)² Secure Summits, documenting the experience of hundreds of members who are grappling with GDPR, and regularly reporting insights through the *(ISC)² Blog*.

"GDPR is a subject that everyone is talking about, but few are focused on the details of what actually has to be done, understanding the workload and the people that have to be involved. In our first meeting, we learned that most projects struggled to get off the ground with very little time before the deadline and we had a mission in front of us," describes Le Roux.

"We also discovered that there is real value for members to help each other if you can bring them together around a common concern," he added.

All initiatives, including opportunities to get in involved, are regularly reported to chapters and in the member newsletter. Anyone interested should be sure to opt-in to the newsletters, join a chapter or contact the EAC directly at info-emea@isc2.org. ■

Now It's an Even Bigger Deal to be an (ISC)² Member

AN (ISC)² MEMBERSHIP provides great ways to stay current on industry news and trends along with high-level certification opportunities. Now it can also save you money on travel, entertainment and at a variety of retail outlets in the United States and Canada.

The list of places to save is long and varied, including:

- Hotels, including Sheraton, Doubletree, Hilton Garden Inn and many more
- Retail outlets like Amazon and Best Buy, to name a few
- Car rentals such as Avis and Budget
- Movie theaters, including AMC and Regal chains

And there are even more discounts for:

- Concerts and events
- Pharmacies
- Restaurants
- Spa and massage venues
- Car dealerships
- Local florists
- Gym and fitness studios
- Theme parks, attractions and tours

Look also for discounts from cybersecurity vendors in Member Perks.

Creating an account takes just minutes. Click https://isc2.abenity.com/. Complete the form and enter registration code MBRPKS. ■

(ISC)² PARTNERS WITH UNIFIED COMPLIANCE FOR NEW CERTIFICATE PROGRAM

Unified Compliance has partnered with (ISC)² to create the Compliance Mapping Certificate Program. The new program is designed to prepare compliance mappers for the responsibility of mapping multiple authority documents correctly and accurately in a way that will satisfy auditors and regulators, while simplifying governance for their organization or clients.

The UCF Mapper™ allows compliance teams to include any publicly available authority documents relevant to their organization, but not currently available in the Unified Compliance Framework. Compliance teams must be certified to use the UCF Mapper.

Training includes multimedia presentations, demonstrations and hands-on experience. (ISC)² will host the self-paced, seven-module online course; Unified Compliance will host practical-application modules. Students may take up to a year to complete the course, and must pass both the online quizzes and the practical-application projects.

For more information on the (ISC)² Compliance Mapping Certificate Program, go to http://www.ucfmapper.com/overview/isc2-compliance-mapping-certificate-program/. ■

READ. QUIZ. EARN.
2
CPEs

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=10696

Coming up in the next issue of *InfoSecurity Professional*

Highlights from (ISC)² Security Congress 2017 in Austin!

InfoSecurity Professional Wins Top Journalism Award in Technical Writing

KUDOS TO GERMAN (ISC)² member Manu Carus and the editorial and creative teams behind the (ISC)² membership magazine for winning a gold international magazine writing award from Trade, Association and Business Publications Inc.

The feature "An Exploit is Born" appeared in the January/February 2016 issue and focused on how a vulnerability in an out-of-circulation printer could be exploited. The second half of the feature focused on mitigations to prevent similar vulnerabilities from being compromised.

"This is absolutely very technical as the intro warns, but also very useful to the reader. Bravo!" wrote the judges in awarding the magazine the gold award in technical writing. The magazine won a bronze in the same category last year, along with a bronze design award.

To see other winners, go to http://www.tabpi.org/awards.htm. ■

FOUR RULES FOR SUCCESSFUL THREAT INTELLIGENCE TEAMS

1. Tailor your talent. Make sure you have the right people with complementary skills who can work together as well as with the company as a whole.

2. Architect your infrastructure. Build custom, in-house systems to collect, store and process internal and external data.

3. Enable business profitability. Understand larger threats and monitor industry trends to protect core business.

4. Communicate continuously. Keep executives updated in a thoughtful, practical manner, without spreading FUD (fear, uncertainty and doubt). ■

Source: *Recorded Future*, February 2016 https://www.recordedfuture.com/successful-threat-intelligence-teams/

Finalists announced for Americas ISLA

The following are finalists for this year's (ISC)² Information Security Leadership Awards, which will be handed out Sept. 26 at the JW Marriott in Austin as part of the 2017 Security Congress (http://congress.isc2.org/).

Community Awareness

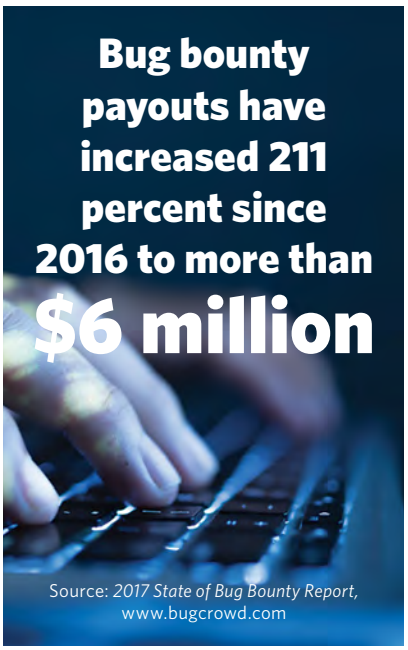
- Christopher Greco
  Silver Hats Founder
- Brian O'Hara
  Indiana Members Alliance Infragard
- Daniela Álvarez
  The Pawawar Project

Information Security Practitioner

- Oscar Monge
  Securing Company Assets
- Nghiem Nguyen
  Data Protection Program
- Jasmine Neal
  Cybersecurity Vulnerability Waiver

Senior Information Security Professional

- Mansur Hasib
  Cybersecurity Technology Degree Program
- Jorge Mario Ochoa
  Information Security Culture
- Jesse Varsalone
  Cyber Padawans
- Rahul Bhardwaj
  Information Security Management Framework



Photograph: Thinkstock

RETURN TO CONTENTS

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

Implementing the ISO/IEC 27001 ISMS Standard, 2nd Edition

By Edward Humphries
(Artech House Publishers, 2016)

International Standards Organization (ISO) standards are important toward helping firms do business online and respond to Internet of Things (IoT) technology. IS/IEC 27001, promulgated by ISO, describes the governance process for protection of information and its implementation.

Author Edward (Ted) Humphries convened the ISO/IEC JTC 27 work group responsible for the development and maintenance of the family of ISO/IEC 27001 ISMS standards and is often referred to as the "father of the ISO/IEC 27001 family of information security management systems standards." This edition provides the latest updates to the 27001 standard and discusses the critical information security management issues needed to help businesses protect their valuable assets.

This book is marvelous for the person who is seeking to implement a risk management process since it lays out an easy-to-understand, somewhat intuitive framework for evaluating the impact of risk that can be applied to any firm and any industry. On the other hand, the book does not provide the reader with technical checklists for performing risk.

The other challenge I have with the book is that, while the author indicates that there should be a firm-wide risk management and security policy, he does not clarify where the development of this responsibility lies, i.e., enterprise risk, senior manager, CIO, etc. Not addressing that is a major oversight, in my opinion.

The bottom line is that this is a very good reference book for those who are in the process of implementing an IT risk management framework, since it covers the required essentials. The author provides an inventory of procedures and policies that an organization requires for implementation to ensure coverage.

In clear, concise, non-technical language, the reader learns how to manage IT risk such as incident management and governance with a clear understanding of the ISO/IEC 27000 security standards and implementation of the recent ISO/IEC 27001. ■

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

The number of days to identify a data breach falls

2015	**201 days**
2016	**191 days**

Source: *2017 Cost of Data Breach Study* – Ponemon Institute, sponsored by IBM Security

PREDICTION

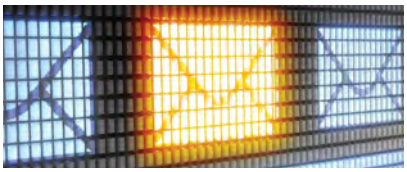
$4-$11 TRILLION

Potential economic value of the Internet of Things by 2025

Source: *McKinsey & Company Highlights, June 2017* - McKinsey Global Institute Analysis

IN 2016

1 in 131 emails sent were malicious



Source: *Internet Security Threat Report,* April 2016, Symantec, https://www.symantec.com/security-center/threat-report

73% of 1,735 CIOs, CISOs and other executives surveyed say they are concerned about poor user awareness and behavior around mobile devices

Source: *Path to Cyber Resilience: Sense, Resist, React,* EY's 19th Global Information Security Survey 2016-2017

Photograph: Thinkstock

RETURN TO CONTENTS

#nextchapter

EDITED BY DEBORAH JOHNSON

(ISC)² POLAND CHAPTER

Early Struggles Lead to Success

Poland Chapter meeting in Warsaw in June 2017

ONE OF THE OLDEST CHAPTERS in EMEA, the (ISC)² Poland Chapter was formed in 2013 with the mission to increase the awareness of IT security and importance of certifications in Poland. After struggling and ultimately succeeding to gain official registration of the chapter as an NGO (non-government organization) in Poland, the chapter began to build a professional community by inviting security experts from around the country to regular meetings with well-chosen topics presented by interesting speakers. From the original 15 members, the chapter has grown to about 60.

Based in Warsaw, the chapter presents regular monthly meetings. In 2016, it was one of the most active chapters in EMEA, holding 14 member meetings, including presentations on a wide variety of topics on technical and management themes, including identity management, vulnerabilities in IT security software, JavaScript engines and popular open source libraries. Since about 60 percent of chapter members are engaged in technical work, presenters are usually threat hunters or pen testers.

The chapter also has a mentor partnership with several industry conferences in Poland, keeping chapter members up-to-date on a variety of events and enabling members to get discounts on the conference fee. Chapter secretary Jacek Grymuza (CISSP, CEH, CIHE, OSCP) presented at the CONFidence conference in Krakow on detection and monitoring security incidents by security operations center analysts. He also talked about cyber threat intelligence at the Security BSides conference in Warsaw.

Here are links to both his presentations:

https://www.youtube.com/watch?v=PWUK8fYJ6JI

https://www.youtube.com/watch?v=u1GOqw-49Rk

(ISC)² POLAND CHAPTER CONTACT INFORMATION

Contact: Jacek Grymuza, Martin Simka

Email: kontakt@isc2chapter-poland.com

Website: http://isc2chapter-poland.com/

Going forward, the chapter would like to organize a security conference and start the Center for Cyber Safety and Education's Safe and Secure Online program in Polish schools. ■

Q&A ▼
MARTIN SIMKA, CISSP

Chapter President Talks Challenges

Martin Simka, CISSP, secretary, (ISC)² Poland (president, 2013-2017)

What were some of the challenges to starting up the chapter?

In our case, the most difficult was the process of establishing the chapter as an official NGO in Poland. Last year, we were finally able to register the organization, so we can now fully operate as an NGO. About two years ago, we reactivated the chapter to focus on the community first. Our regular meetings were organized with presentations on various topics.

Thanks to the enormous effort of Jacek Grymuza, our recently elected president, along with other members and the presenters, we've achieved our initial goal. I suggest that chapters start first with building the community, and later focus on formalities, like NGO registration.

What might make working in IT in Poland different from other countries?

The market in Poland is very dynamic and has changed significantly during the last decade. While most opportu-

nities are in Warsaw, Poland's capital, other cities like Krakow or Wroclaw have their places on the Polish IT map.

The high quality of IT university-level education is well known and Polish teams regularly win coding competitions worldwide. The combination of highly skilled staff and quick development of the country and the central Europe region makes the market very challenging and promising, so our approach is "nothing is impossible for us" or "if not us, then who?"

What is the top issue facing the information security community in your chapter?

During our last meeting, we had a long discussion on GDPR [the EU General Data Protection Regulation, which takes effect May 25, 2018] and the related legislation process in Poland. I expect there is more to come on this topic.

What keeps your members motivated, both in being part of (ISC)² and in the information security industry?

Thanks to a wide variety of topics presented during the chapter meetings, there is the chance for our members to enhance their knowledge and go behind the areas their jobs are related to. As I've mentioned above, dynamic growth of the economy brings challenges in several fields, including security. Moving to e-commerce and digitalization requires constant effort in the information security area, and our members are part of this process.

What do you see for the future of the chapter in terms of leadership in the information security industry in your region?

Our aim is to keep a high quality and good variety of presentations at chapter meetings. Additionally, we hope to improve our presence at security conferences in the region. The chapter itself provides good opportunities for networking and keeps the community updated on the latest industry issues. ■

A SOUNDING BOARD FOR THOSE WITH SOMETHING TO SAY

members' corner

BY DR. RICHARD N. KNEPP, CISSP

It's Always Wise to Plan Ahead, Especially in Your Career

CONGRATULATIONS! You have the experience, certifications, knowledge, skills, abilities and education to land a great job in cybersecurity. However, rather than focusing on the job at hand, it's important to always be looking forward. When asked where do you see yourself in the next five to 10 years, few say, "Same place as now."

Therefore, getting to that future state requires a lot more than daydreaming; it demands a solid, active five-year career plan that includes lifelong learning with a purpose and periodic review.

To help you to get to what's next, I have developed a simple career plan to get you started. The first bit of advice is to think of yourself as your own "company" (because, who knows, you may become an entrepreneur someday soon). Ask yourself these questions:

- How do you make yourself more marketable?
- Do you stand out, or are you just another IT clone?
- Do you want to learn something new, or more of the same?
- What is your objective?
- What are your goals?
- Where are you now?
- Where do you want to go?
- How will you get there?
- Do you have a career plan?
- Do you have an action plan or a contingency plan?

GOAL-SETTING AND A GAP ANALYSIS

The ultimate outcome of a long-term career plan is to have a goal or set of goals to achieve within a prescribed period. Then take in where you are now vs. where you want to be and what it will take to get there. That's what is referred to as a "gap analysis."

Additionally, an "environmental scan" is important. These are sometimes called SWOT analyses because they are honest appraisals of your strengths, weaknesses (development needs), opportunities and threats. You may benefit from outside perspectives in conducting your SWOT analysis, just in case there are blind spots you are too close to see.

Once these foundational steps are done, it's time to get started on that five-year career plan.

LONG-TERM PLAN CONSIDERATIONS

Every company has a corporate mission. So should every individual with a career plan. To help determine your professional (perhaps even personal) mission, ask yourself:

- What are the things you want to accomplish?
- Why do you want these things?
- How do you plan to make this happen?
- Who is going to help you accomplish your mission?

You also need to know what "success" will look like by creating "success indicators" that describe the milestones toward a full goal achieved. These measurable milestones help you know if you are still on the right track or have veered off course.

A plan can initially seem overwhelming. That's why it's a good idea to break it down with trigger points. As you achieve one goal, you move on to the next. If they do not or cannot occur, what is your contingency plan?

BRIEF AND DETAILED ACTION PLANS

Five years can seem far off, but short- and long-range action plans can come more quickly than you think. As you build out your action plans, consider the time, resources and support it will take to bring such a plan to fruition.

Then build a detailed action plan with a timeline.

Keep in mind these goals relate to your career but may widely vary, from earning a degree and/or certifications to spending more time with family. It's all how you envision yourself living and working within the next decade or less. And have a contingency plan in case things don't go as planned.

Once you have achieved your goals, start anew. Always ask yourself: What's next? ■

Dr. Richard N. Knepp, CISSP, is a senior enterprise architect at the Marine Corps Logistics Command.

ISHPI

advanced technology • native know-how

(ISC)² OFFICIAL TRAINING PROVIDER

ISHPI works in concert with other defenders of the Homeland to fortify national preparedness, agility, strength and advantage in the cyber domain. Our business units work in unison to provide experienced people, proven processes, technology, advice, and leadership to enable full spectrum cyber capability.

- Training and Consulting
- Information Operations
- Advanced Information Services
- C5ISR Engineering and Technical Services
- Health Care IT Services

CMMIDEV / 5 SM
Exp. 2020-02-09/Appraisal #28477

Inc. 5000 HONOR ROLL
SEVEN-TIME HONOREE

WASHINGTON TECHNOLOGY FAST 50

WWW.ISHPI.NET

MAN VS. MACHINE

BY JAMES HAYES

Let's take a step back and determine if we're really ready to breathe new life into artificial intelligence tools.

MENTION OF ARTIFICIAL INTELLIGENCE (AI) can bring out strong reactions with some folks. Über thought leader Elon Musk, for instance, warned that in creating intelligent systems, humans were "summoning the demon." Efforts to apply AI techniques to cybersecurity have evoked some equally strident views, although no one (as of yet) has warned about the summoning of demons; anyone employed in cybersecurity knows that the demons are already here.

ILLUSTRATION BY TAYLOR CALLERY

THE BATTLE OVER AI—IS IT REAL OR SCIENCE FICTION?

The potential for AI in some form to be used to counter threats has long been debated by industry researchers and academic theorists, and some commentators nominate AI as a key component in next-generation cybersecurity strategies, along with threat-intelligence-led penetration tests, encryption-as-a-service and retaliatory defensive action ("hacking back").

More recently, products said by their makers to variously use AI in some form have entered the market. It's hard for outsiders to tell how good they are, but industry insiders evidently were impressed.

Startups like Harvest.ai, Invincea and Niara were swiftly acquired by big names (Amazon, Sophos and HP Enterprise) before they had much chance to pit their intelligence against either competitors or threats.

Other players like Dark Trace, Cyberlytic, Cybereason, Cylance, Instart Logic, PatternEx, Webroot and ZoneFox, for example, continue to champion AI as the latest caliber of silver bullets in the armory of cyber safeguards. This has brought forth some contentious debate, with AI skeptics suggesting that, at best, the technology is immature to the point of impracticality and, at worst, that some AI-hyped solutions are more artificial than intelligent. AI advocates argue that even rudimentary forms of the technology serve as tangible aids in the fight against online adversaries. Potential users of such solutions must sort out constructive critique from rival-knocking.

Kaspersky Lab CEO Eugene Kaspersky, for one, is firmly with the myth busters. He reckons that AI in cybersecurity is an unready technological concept that, as it stands, has not much to bring to the fray. More than that, he is scornful of vendors who bandy around the term in order to whip up market interest and bamboozle customers.

"AI still doesn't exist," Kaspersky declared in a June 2016 blog posting, and in September 2016, with a further denunciation. "What's going on now in the field of 'AI' resembles a soap bubble…. And sadly, the cybersecurity field has not escaped this new AI bubble…. This 'new' technology…adopts an aura of cutting-edge science; it gets to have the most glamorously [sic] sophisticated marketing campaigns. And all of that is aimed at the ever-present human weakness for belief in miracles." Another danger in the rush to coronate AI, Kaspersky warns, is the threat to the possibilities of machine learning. "[The] AI bubble discredits machine learning (ML)—one of the most promising sub-fields in cybersecurity [and also] the reason why humanity hasn't drowned in a gigantic mass of data." That AI/ML security systems can deliver more than greater operational effectiveness is something that vendors are just starting to evangelize about.

ARTIFICIAL VS. MACHINE LEARNING: YES, THERE IS A DIFFERENCE

Some cybersecurity specialists have been known to say AI when they mean ML, and vice versa. And some marketers may be inclined to talk up ML in AI terms if they think it will help win business. Add in any cybersecurity vendor predilection to speak of having "AI-like capabilities" or "elements of AI" in their products, and it's little wonder there's confusion.

For Ilia Kolochenko, CEO and founder of High-Tech Bridge, a mobile and web security provider headquartered in Geneva, the confusion is dangerous. "Many cybersecurity companies misuse the acronym 'AI' for advertising and marketing. The biggest problem, however, is vendors who claim to use AI, but cannot even explain *why* and *how* AI implementation in their product can help their customers achieve [security] efficiency. While ML is just a specific technology and group of algorithms which can leverage big data to take decisions and solve tasks which are not hard-coded into their logic," ML is "an embryo that may, potentially, become an AI in the future."

Gabriel Coelho-Kostolny, director of product management at Palo Alto's Instart Logic, agrees that there is confusion. "On the vendor side, 'AI' is widely understood as the blanket term for a broad collection of techniques used to help computers make sense of information. Whereas, 'ML' is a term for specific classes of algorithms that are used to solve a subset of problems to which AI, in general, can be applied."

AI and ML are "closely related, but they are not the same thing," emphasizes Carl Herberger, VP of security solutions at cybersecurity provider Radware. "In many ways, ML is an enabler for AI. While AI is how we hope to make machines 'intelligent,' ML is the behind-the-scenes computation that makes AI possible. [In the cybersecurity market now] ML is the fastest-growing area [related to] AI, which is why there is such buzz around it—and also why there is confusion about what ML can do [in comparison with] 'true' AI."

Cybersecurity solutions are already taking advantage of ML, Herberger reports, by using behavioral analysis to enhance attack mitigation systems. As a result, mitigation systems can perform more advanced threat analytics on a much larger scale.

MOVING CLOSER TO MERGING MACHINES AND MANPOWER

For some industry experts, the future lies in coupling AI and ML. Working in concert, says Hal Lonas, CTO at Colorado-based Webroot, there is no doubt that AI "can provide new tools for threat hunters, helping them protect

new devices and networks even before a threat is classified by a human researcher. Machine learning techniques, such as unsupervised learning and continuous retraining, can keep us ahead of the cybercriminals."

Sam Curry, chief privacy officer at Cybereason, agrees that ML could be defined as a preliminary step on the way to truly defined AI, as it revolves around teaching a system to learn on its own without further human input and make decisions based on its findings. "The concepts of ML and AI are very similar, so it is unsurprising they have become somewhat interchangeable," Curry says. "The term 'AI' generally applies to more far-reaching and complicated uses that could potentially mimic human thought processes. For the most part, cyber practitioners with firsthand experience will know the difference—but confusion will certainly mount at the board level if hype increases."

Information security leaders tasked with seeking funds for AI/ML solutions this budget season might face less of a comprehension deficit than they used to. Radware's 2017 *Executive Application & Network Security Survey* claims to indicate a "perceptional shift" among C-suite executives, some of whom seem amenable to the idea of security supported by AI, ML and other automation. Of the executives polled:

- 33 percent reported "trusting automated systems more than humans"
- 24 percent said they trust humans over machines
- 24 percent said they trust people and machines equally.

The remainder reported that as both have vulnerabilities, they trust neither.

This case is further helped by two additional aspects of the AI/ML combination: its ability to free up information security professionals from relentless data analysis workloads and refocus their expertise on predictive threat analysis strategies (such as those informing threat intelligence-led penetration tests); and its promise of more insightful analysis of threat data that can enable a targeted organization to better understand its adversaries, especially as larger enterprises move closer to retaliatory engagements with cyber foes (maybe with their own offensive AI/ML tools).

Information security professionals will need to plan for and adjust to new working methods that AI/ML systems entail. According to vendors, such solutions bring new disciplines to cybersecurity practices and these new approaches should be formulated and proceduralized as fundamental new work regimes. "[With AI/ML,] IT security teams have to figure out what [they] do best and what machines do best," says Webroot's Lonas.

"Machines are great at repetitive tasks where a high degree of reliability and uniformity are desirable," he says. "Humans are best at tasks that require some creativity and insights that only humans can provide. IT security teams need to recognize this and allow machines and AI to do the majority of high-volume [data crunch] tasks—tasks which bore, overwhelm, frustrate most people—and then refocus human assets on learning how to leverage the machines to best advantage."

Lonus suggests that AI/ML classifiers will be able to identify slight variations in malware and phishing sites, enabling their human colleagues to more quickly identify even newly devised threats.

AI- and ML-based tools will require organizations to focus on what data is collected for analysis, explains Coelho-Kostolny of Instart Logic. "With human-based analysis, organizations have typically focused on reducing the amount of data that must be collected and analyzed because humans are very inefficient and error-prone when dealing with large volumes of data. AI-based tools flip this equation: they function best when supplied with as much data as possible." When companies do this, Coelho-Kostolny suggests, they can also realize gains in the efficiency of their human operators, "because despite the higher data volumes, the intelligent systems are able to surface only the most relevant data, reducing the human workload."

Kevin Bailey, vice president of Applied Intelligence GTM (Go-To-Market) Strategy at BAE Systems, based in the United Kingdom, agrees that the introduction of AI/ML cybersecurity means the relationship between technologist and technology will alter. "A greater trust in the automation of manual tasks and also the alerts of possible cyber incidents needs to be embraced," he believes. "AI is the combination of many components that will increase

the efficiency of back-office activity, but will also use ML to increase its effectiveness. This means that data centers and cybersecurity personnel need to change the appreciation of AI when a system reacts differently based on 'learnt' knowledge, rather than applying the humanistic policy of what [their] experience has taught them."

It is crucial that before implementing any AI/ML systems, an organization needs to evaluate risk. Ian Trump, head of security at ZoneFox, an Edinburgh, Scotland provider of behavior and data analytics, advises that, as with any incoming technology, risk assessment should form part of due process.

"There are two types of risk at opposite ends of the spectrum. An organization could place too much trust in an AI, which results in bad judgment calls; or it could ignore its insights, so the AI learns that prolific 'bad' behavior is actually normal. Using a fully autonomous AI solution without proper tuning can enable it to make decisions which negatively impact business productivity, which is why we haven't seen products like this take hold yet—the technology simply has not matured enough to allow a fully 'hands-off' approach. The second type of risk can be mitigated by appropriate tuning and setup and, at least, semi-frequent use of a system; so again, organizations will get out of [AI-based cybersecurity] what they put in."

At the other end of the deployment, information security technologists should not overlook the possible effects that newly introduced AI/ML solutions might have on end users. Cybersecurity analysts and user experience experts point out that end-user behaviors have a quantifiable impact on the effectiveness of cybersecurity systems.

"All intelligence systems go through a period of trialling," says BAE Systems' Kevin Bailey. "High rates of false positives are due to an overactive system that has been too granular in its operation, hence trapping innocence. A good AI system will not only [try] to act efficiently, but also alert to inefficient procedures, policies and rules."

For Instart Logic's Coelho-Kostolny, "the fundamental reason for using these AI-based approaches is because they are more capable and flexible than the more simplistic rule- or heuristic-based mechanisms deployed to date. By analyzing much larger volumes of data and then being

trained with human feedback as they surface possibly 'questionable' behavior, over time these systems become smarter, and can account for a broader range of allowable behaviors."

If the desire is to enforce secure IT usage policies on a stricter and more granular basis, however, Coelho-Kostolny says that AI-based systems can be useful. "By combing through potentially every bit of user behavior, policy violations can be easily flagged and then addressed, rather than just picking up a small sampling of behaviors. This approach may be appropriate for more strictly managed organizations such as banks, while being less appropriate for some more flexible BYOD-amenable environments."

USING AI TO BRIDGE THE GAP BETWEEN IT AND EVERYONE ELSE

ZoneFox's Trump sees AI as having potential to provide stark insight into end users' bad practices. "AI-based products can uncover the harsh reality of what is actually going on within an organization. These products excel in providing such visibility, and it is up to the organization to use this information to ensure that employees are sufficiently trained on what is—and is not—acceptable.

"CSOs are stuck in an impossible place, as they control only one-third of the cybersecurity business problem. Typically, HR or business units are responsible for onboarding employees, which may or may not include some basic security awareness training," he continues. "This means that CSOs and IT leaders are not usually engaged in the process the business uses to drive revenue. So, for the most part, the only thing they actually control is the IT budget.

"This stacks the deck against CSOs, as they are only in control of 33 percent of the organizational information security problem. The question here is: Can AI help them narrow that gap? The answer: Potentially, yes." ■

JAMES HAYES *is a U.K.-based freelance writer and past contributor to* InfoSecurity Professional.

Creating Security Awareness Requires SYNERGY

BY STEFAN BEISSEL, CISSP

Raise your company's security consciousness through more collaboration and interaction.

IN ORDER TO ENSURE employees are complying with a company's IT security measures, it is essential to create an environment of security awareness. For most companies, it is obvious that awareness measures are important safeguards that must not be overlooked when establishing an appropriate protection level. Since awareness measures lead to certain costs, professionals might be restricted in implementing the desired measures. A trade-off between benefits and costs is usually the prerequisite for getting the needed approval from senior management.

By creating synergies within the organization, the relative costs of the awareness measures can be reduced so that they are more cost effective. With synergies, the measures look more beneficial when performing trade-offs and will, therefore, be more likely approved by senior management.

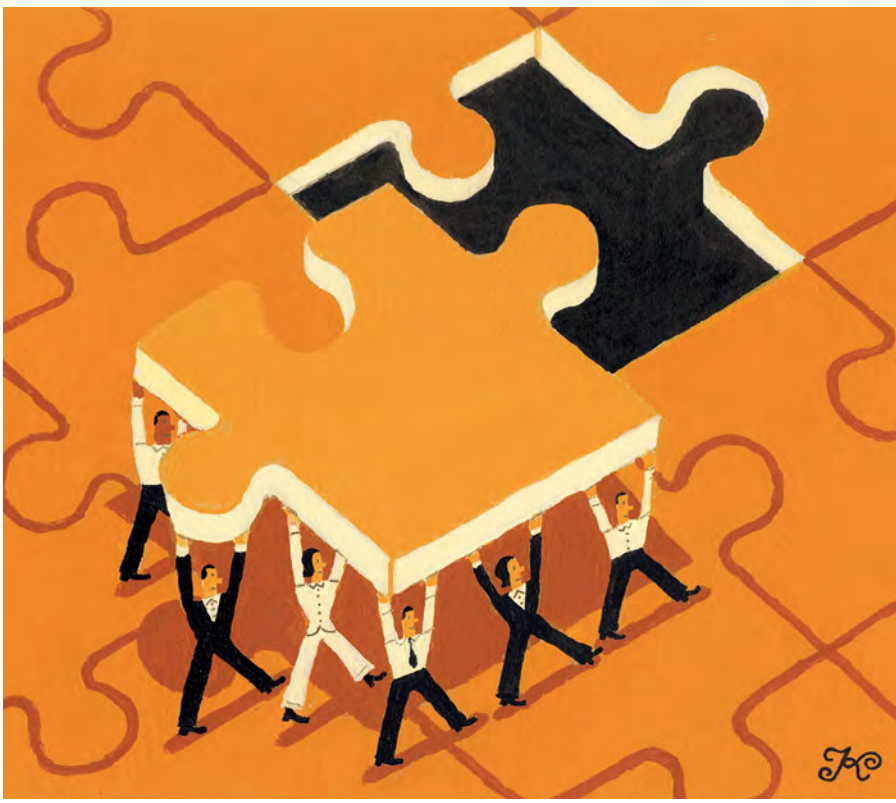


ILLUSTRATION BY JAMES KACZMAN

Positive synergy effects can lead to decreased resource needs in the production of goods or services and the improvement in quality due to more extensive know-how.

COLLABORATION + INTERACTION = POSITIVE SYNERGY

In general, synergies are facilitated by an interaction between separate units. These units can be entire companies, departments, functions, processes or projects. The effects of these interactions, also called *synergy effects*, can be positive or negative. Positive synergy effects can lead to decreased resource needs in the production of goods or services and the improvement in quality due to more extensive know-how. Negative synergy effects can occur when existing resources are overloaded or the combined units become too complex.

When companies endeavor to create synergy effects, they are usually focusing on positive synergy effects. Whether these effects can really be achieved cannot always be predicted with certainty. In order to reduce the uncertainty as much as possible, the planned synergy approaches should be well conceived and include as much information on the probable impact as possible. An important source of information is the experience gained within the company or similar well-known entities. If the company itself cannot build up a sufficient information base to be able to make a well-founded synergy decision, it may be necessary to appoint external consultants that can provide the appropriate information.

POSITIVE SYNERGY LEADS TO SUCCESS

There are different synergetic approaches to IT security awareness.

Cost-reduction synergies usually revolve around the preparation or implementation of awareness measures, such as decision-making, planning, acquisition, implementation, operation and maintenance. These expenses can be reduced through the cooperation of different employees, departments or even whole companies.

Scale effects can be generated by increasing the number of services provided. For instance, when producing a larger number of security awareness handouts or brochures, the variable costs, such as paper, are increased, but the fixed costs, such as design, remain the same or increase modestly. The total costs per service are reduced because of the relative reduction of the fixed costs per service. This is called "fixed cost digression."

Compound effects occur when additional services are provided to the initial planned services. The new services must be linked to the existing ones to ensure synergies. Processes can be standardized and automated, reducing the cost per service. For example, the same graphic designer could be entrusted with the design of all print products around awareness. This would make certain work steps, such as the integration of the corporate design, are more efficient or partially automated.

Density effects can be achieved if the supply path is important for performing the service. If many receivers of the service can be concentrated in an area, the aggregated supply paths are shorter than those for widely distributed receivers. For example, geographically distributed employees might need to be trained in several events. In this case, density effects can then be created by grouping the employees by their geographic position rather than using other criteria, such as the hierarchy level.

Time-reduction synergies can be achieved by accelerating, parallelizing, reducing or summarizing activities.

Acceleration shortens the duration of time required to perform an activity. This can be achieved, among other things, by providing additional or better tools and more staff. For example, when printing security awareness posters, the company can purchase high-quality printers with faster printing processes or additional printers so that the work can be accelerated. Avoiding waiting times can also lead to acceleration, e.g., a faster network connection enables faster transfers of image files to a printer.

Parallelization allows the execution of different activities at the same time. Sequentially arranged activities can be carried out in parallel. Single activities can also be divided into several sub-activities that can be performed in parallel. As a result, the overall duration of the activities is reduced. For example, activities for creating an awareness brochure can be performed in parallel if one employee designs the cover while two other employees create one chapter each.

The *reduction* of partial or complete activities is advantageous if the removed activities have prospectively no additional value for the result. Mostly, the value can only be assessed after the activities have been completed. However, if similar activities are repeated regularly, the value may be estimated by analyzing the outcomes of the previous activities. For example, if awareness documents are regularly checked for spelling and grammar, but almost no corrections were needed in the past, this activity might be removed in the future. Besides, the reduction of less valuable activities might lead to a more effective usage of work capacity because it can be focused on more valuable activities.

Summarizing groups two or more activities that are

performed by different people into a single activity that is performed by one person. Above all, this avoids interface problems. If consecutive activities are performed by the same person, nothing needs to be handed over, and there will be no waiting times or bottlenecks between these activities resulting from scheduling problems of the second person. Therefore, a different or separate handling of sub-activities by different persons can be avoided. For example, all activities related to designing, creating and sending a newsletter can be combined, so that problems or delays are prevented when handing the newsletter draft from one person to another.

WAYS TO IMPROVE QUALITY OVERALL

Quality improvements can result when employees with different skills, knowledge or experience interact. Different resources can also lead to higher quality. If project requirements are fulfilled more exactly, the quality can be increased. In principle, quality can be increased by preventing or detecting defects in a better way.

Taking measures to prevent defects before project completion increases the quality level. At that stage, the organization can be adapted or processes can be reorganized. The creation of training content may, for example, be reserved for the employees who have experience in IT security. A synergetic cooperation of several employees would increase the likelihood that suitable employees are available.

Early defect detection can also be accomplished by quality audits that are integrated with the help of other employees or resources. For example, quality audits for advertising texts may also be applied to awareness texts.

STEPS TO CREATING SYNERGIES

When selecting specific synergies, the focus should be not only on the results, i.e., cost and time reductions, or the quality increase, but also on the additional cost and time required to establish the synergy. Among other things, processes or structures often must be adapted to create synergies. Some specific examples of synergies in IT security awareness are:

- In *co-working*, employees with different tasks and positions work together in an open space. Even if they are not involved in the same project or work in the same department, they can benefit from proximity. The increased exchange of knowledge can lead to quality increases. Besides, the shared use of office space might lead to lower costs.
- The *common purchase* of goods and services is advantageous because the negotiating position of the buyers will be strengthened. Companies can aggregate their need for awareness products or services to reduce costs through scale effects.
- The *joint use of the infrastructure* can also reduce the overhead costs through scale effects. For example, instead of a new web server for online trainings, an existing web server that still has capacity could be used.
- The *cooperation of workforce* members can lead to more flexibly (e.g., between awareness officers and the marketing department). If a larger group of employees can perform the same tasks, time can be reduced by accelerating or parallelizing activities.
- An *increase in know-how* can be achieved, among other things, by mergers, outsourcing or networking. With more know-how, security awareness activities without a value can be identified and eliminated. Thereby, time reduction and quality increases may be achieved.
- *Sharing supply routes and facilities* is also a way to save costs. By bundling routes, cost reduction can be achieved through density effects. Participants of awareness events can travel together or event locations can be shared with other companies.
- *Combining compliance activities* for various regulations can lead to a time reduction in selecting and implementing awareness measures that will be achieved. Different requirements can be covered by appropriate measures without creating redundancy.

SUMMARY

Improving a company's security consciousness can be a delicate issue because of the accompanied costs. By creating synergies, the trade-off between costs and benefits can be adjusted so that senior management's approval is more likely.

As described above, multiple synergies can be considered to reduce costs and time, and improve quality. Realizing just a few appropriate synergies, like scale effects when producing handouts, or parallelization of security activities, can strongly improve the overall trade-off.

Besides, general measures for improving processes or structures, i.e., co-working and joint use of the infrastructure, should always be considered to facilitate synergies around security awareness activities. ■

STEFAN BEISSEL, *PhD, MBA, CISSP, CISA, PMP, is the information security officer at Blue Cross of Idaho.*

(ISC)² EMEA Secure Webinars

Explore the Series. Earn CPEs. Get Involved.

The (ISC)² EMEA Secure Webinar Channel features live and on-demand online events where regional industry experts, (ISC)² members and solution providers offer their thought leadership on a variety of topics to help today's cybersecurity professionals tackle current threats and challenges.

- 150 + hours of on-demand, educational and CPE worthy content
- Lunch & Learn Live: convenient timings for those based in Europe, Middle East and Africa
- Moderated by (ISC)² members
- One CPE per hour for live or archived webinars, automatically added to (ISC)² members' profiles
- Free of charge to members and non-members

(ISC)² CPE Opportunities

VISIT THE CHANNEL

Become a Presenter or Moderator

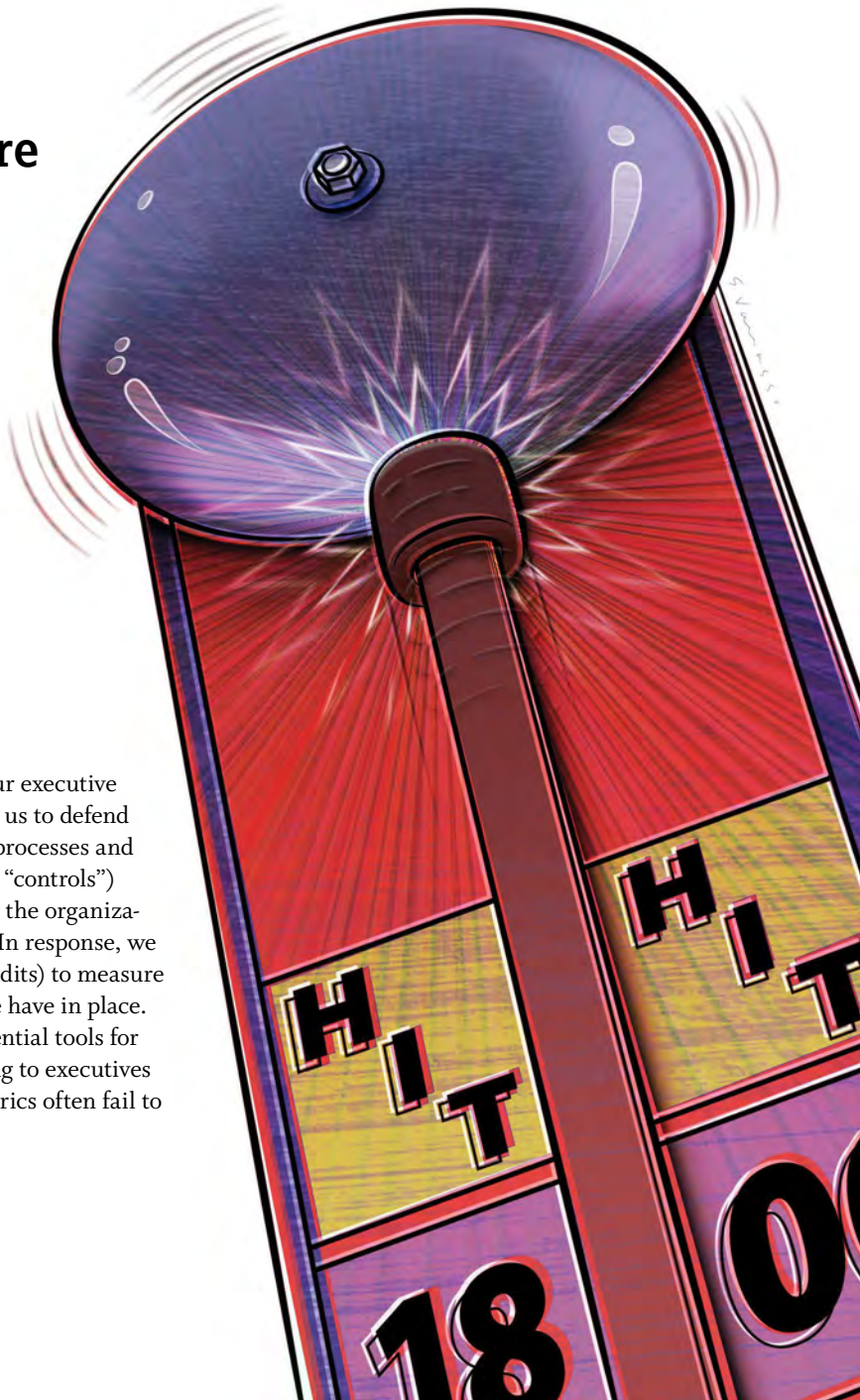
(ISC)² EMEA is dedicated to delivering educational content of the highest quality through our Secure Webinars series. We are seeking sessions that will be relevant to an audience of experienced information security professionals from a variety of industries. We like to see anything that squarely fits into the spectrum of: Cybercrime, Cloud Security, Supply Chain, Application Security, Forensics, Human Factor.

Learn more about presenting and moderating by contacting Patricia Reiner van Heerden at preiner@isc2.org

Achieving Performance EXCELLENCE in Cybersecurity Management

A new tool helps measure and communicate the business value of information security to business and government leaders.

BY ADAM STONE, CISSP-ISSMP, HCISPP

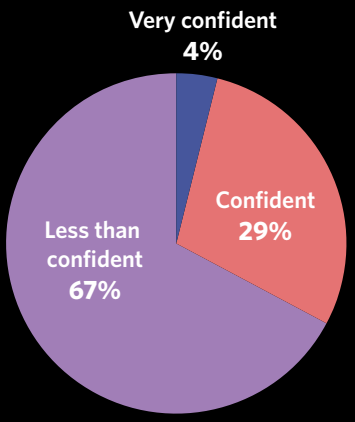


AS SECURITY LEADERS, our executive teams regularly challenge us to defend investments in the tools, processes and people (collectively called "controls") dedicated to safeguarding the organization's information assets. In response, we may use common methods (such as assessments or audits) to measure and communicate the effectiveness of the controls we have in place.

No doubt, controls assessments and audits are essential tools for the information security leader. When communicating to executives and board members, however, the controls-based metrics often fail to translate into the language of *business value*.

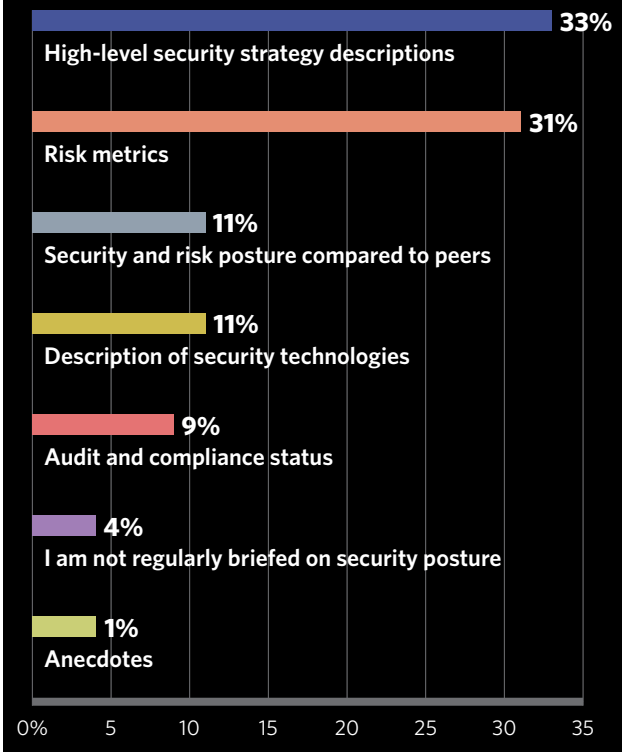
ILLUSTRATION BY ENRICO VARRASSO

Figure 1: **How confident are you that your companies are properly secured against cyberattacks?**



Source: *Cybersecurity in the Boardroom.* 2015 Report by NYSE Governance Services/Veracode

Figure 2: **How do you prefer information regarding cybersecurity be presented?**



Source: *Cybersecurity in the Boardroom.* 2015 Report by NYSE Governance Services/Veracode

In today's digital economy, our executives and board members want clarity when it comes to cybersecurity. As security leaders, we need to communicate in a manner that improves, not muddles, decision-making at the executive level. To do so, we must adopt new strategies for demonstrating that the security function and its corresponding controls add value by offering meaningful metrics squarely focused on organizational goals and objectives. Though information security leaders may manage cybersecurity with controls, we must take conscious steps not to use controls as our metric for communicating program effectiveness.

To take this leap, security leaders must first acknowledge the shortcomings of the controls-based methods used to measure, prioritize and communicate program effectiveness. This bottom-up approach to denote security effectiveness may be contributing to the problem.

As security leaders communicate progress toward goals using data from the bottom up, we are often inclined to report on the trees, when the executives want to know about the forest. The C-suite asks: "In what way does a given control contribute to corporate earnings and sustainable growth?" We often get the answer wrong, because we tend to focus on the controls themselves and not the business objectives driving the need for controls.

Our executive leaders need business-focused data to help ensure that investments in security will produce the sorts of returns they expect. But it is *mismatched expectations* that can get the security leader in trouble.

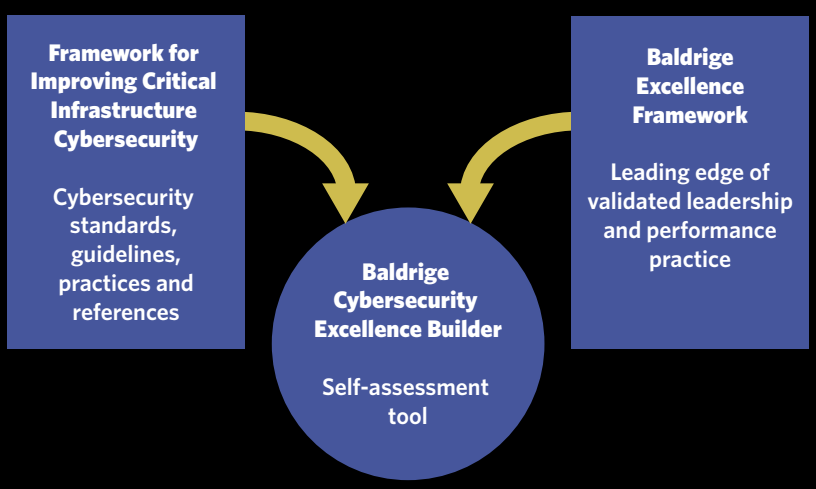
Due to our historical emphasis on controls-based security messaging, executive decision-makers may continue to view cybersecurity as a moat that protects the castle. When the moat is crossed and the enemy has launched a sneak attack from within, exasperated senior leaders shake their heads and wonder where their investment went. This has a direct impact on the credibility of the security leader, and it can quickly erode the trust and confidence we seek.

SHIFTING HOW WE MEASURE CYBERSECURITY

To build our standing among the executives, security leaders must shift focus to *organizational performance* and *process maturity* as the foundational metrics used to communicate how well—or not well—the information security function is helping to enable sustainable business growth.

Those unmoved by the last assertion should ask their executive stakeholders for feedback on what cybersecurity metrics they need and want in the current business environment. Decision-making at this level requires an understanding of cybersecurity's impact on corporate reputation, resilience, operational efficiencies, innovation and speed-to-market.

Figure 3: **BCEB framework**

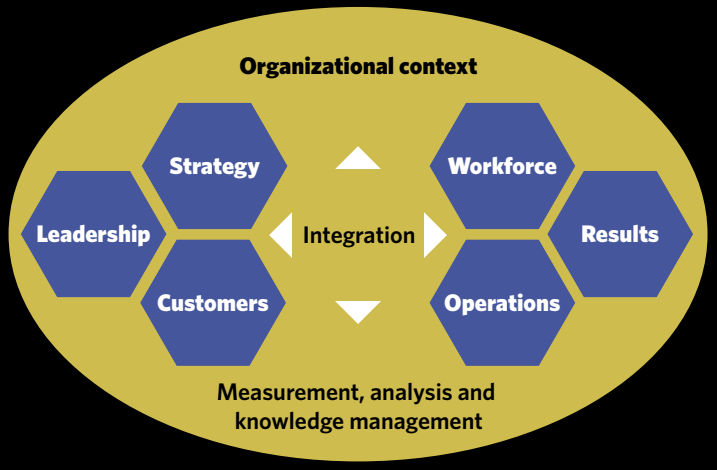


Source: Baldrige Performance Excellence Program. "Baldrige Cybersecurity Excellence Builder." 2017. National Institute of Standards and Technology.

The reality today is that only a small number of security leaders define and track metrics that align to these business factors, and even fewer take advantage of opportunities to communicate this sort of data to stakeholders. The result: Executives make economic decisions based on a flawed model that regards cybersecurity as a finite problem rather than an ongoing process of incremental improvement (https://hbr.org/2017/06/the-behavioral-economics-of-why-executives-underinvest-in-cybersecurity).

For some time, executives and board members have voiced frustration with their security leaders' controls-based messaging. Overall, two-thirds of executives have little

Figure 4: **Core values and concepts**



Source: Baldrige Performance Excellence Program. "Baldrige Cybersecurity Excellence Builder." 2017. National Institute of Standards and Technology.

Organizational context
Understand the business factors and organizational priorities underlying your cybersecurity risk management.

Workforce
Engage and empower your entire workforce to achieve your cybersecurity-related objectives.

Results
Use data and information to evaluate and improve cybersecurity-related policies and operations in alignment with your strategy.

Operations
Design, manage and improve your cybersecurity operations for effectiveness and efficiency.

Measurement, analysis and knowledge management
Through measurement and analysis, align cybersecurity policies and operations with your objectives. Manage your organization's cybersecurity-related knowledge.

Customers
Understand and exceed the cybersecurity-related requirements and expectations of your customers.

Leadership
Understand how your leaders' actions guide and sustain your cybersecurity risk management.

Strategy
Create clear strategic priorities for your cybersecurity program.

or no confidence in their organizations' ability to prevent cybersecurity breaches, according to an NYSE Governance Services/Veracode report entitled "Cybersecurity in the Boardroom" (https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf) *(see Figure 1, p. 29)*. This same report also finds that 64 percent of executive-level respondents want today's security leader to focus on strategy and the role of risk when communicating *(see Figure 2, p. 29)*.

Security leaders should take note of these striking figures, as they appear to correlate with the level of trust and confidence executives have in our ability to manage an effective cybersecurity program.

Enter the Baldrige Cybersecurity Initiative (https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative) and a powerful new tool to address the dual challenge of identifying and measuring cybersecurity performance excellence (https://www.nist.gov/baldrige/self-assessing/baldrige-key-terms#P) and improving communications with executives and board members.

Baldrige's self-assessment tool, the Cybersecurity Excellence Builder, Version 1.0 (BCEB) (https://www.nist.gov/sites/default/files/documents/2017/04/03/baldrige-cybersecurity-excellence-builder-v1.0.pdf), is the only freely available assessment methodology connected to Baldrige's internationally-recognized framework (https://www.nist.gov/baldrige/publications/baldrige-excellence-framework) for evaluating the quality and maturity of key business processes and their impact on *results*.

SEEKING EFFICIENCY, TEAMWORK AND EFFECTIVENESS

Greg Witte, a senior security officer for Maryland-based G2, Inc., and key

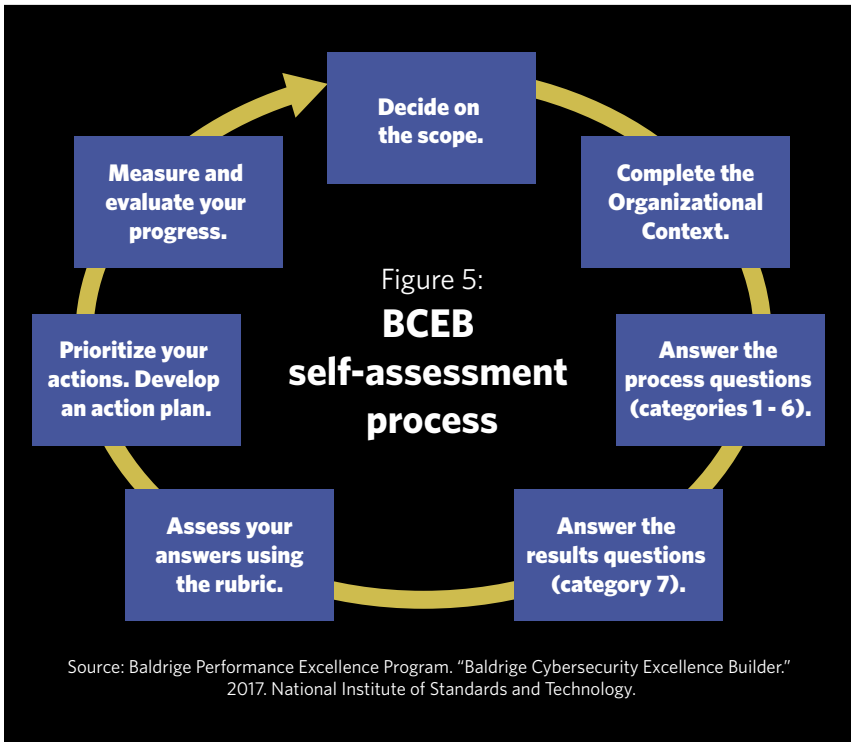


Figure 5:
BCEB self-assessment process

Source: Baldrige Performance Excellence Program. "Baldrige Cybersecurity Excellence Builder." 2017. National Institute of Standards and Technology.

contributor to the BCEB, describes the tool as where "maturity and operational excellence go hand in hand."

"An operationally excellent organization understands how to achieve its mission with efficiency, teamwork and effectiveness—and then achieves that goal," Witte says. "Maturity, in turn, is the application of processes that help to achieve performance excellence, progressing from a random, ad hoc approach to one that is optimized."

The Baldrige Performance Excellence Program (https://www.nist.gov/baldrige), administered by the National Institute of Standards and Technology (NIST), emerged from legislation passed in the mid-1980s, prompted by an urgent national need to improve the quality of U.S. products and services in response to global competition. The program, named posthumously for former quality advocate and Secretary of Commerce Malcolm Baldrige, oversees the presidential award (https://www.nist.gov/baldrige/baldrige-award) for performance excellence. The Baldrige Excellence Framework (https://www.nist.gov/baldrige/publications/baldrige-excellence-framework) is the embodiment of the program's mission and purpose. It helps organizations of all sizes answer three questions essential to achieving goals, improving results and becoming more competitive: "Is your organization doing as well as it could? How do you know? What and how should your organization improve or change?"

The BCEB presents a deviation from the usually function-neutral Baldrige approach, as it singles out information security as a critical resource for organizations. The Cybersecurity Initiative followed NIST's publication of the Cybersecurity Framework (NIST CSF) (https://www.nist.gov/cyberframework), which was itself set in motion by an Obama-era executive order that called for cybersecurity improvements for the nation's critical infrastructure. The NIST CSF received a presidential boost in May when the Trump administration issued an executive order that explicitly directs most federal agencies to use this document as the basis for their cybersecurity management programs. Together, the Baldrige Framework and CSF define the key principles, objectives and metrics of the BCEB *(see Figure 3, p. 30)*.

The BCEB is organized according to seven categories representing critical aspects of managing and performing as an organization. The background for these is the Organizational Context, which outlines key business factors that relate to and impact cybersecurity *(see Figure 4, p. 31)*.

Once the assessor determines scope, the BCEB self-assessment process begins with consideration of *organizational context*, followed by an assessment of process management factors. The next section (*measurement, analysis* and *knowledge management*) helps identify key decision points aligned to organizational performance objectives and recommendations for improvement. The last section addresses the measurement of performance with *results*. Once completed, a BCEB self-assessment yields two distinct assessment dimensions (*process* and *results*) across four *process* factors and four *results* factors to arrive at a final assessment *(see Figure 5, above)*.

The BCEB's assessment rubric provides clear, business-focused and actionable information about an organization's cybersecurity program. The assessments provide both qualitative and quantitative evaluation data that can easily scale with the size and complexity of the organization using the self-assessment tool *(see Figures 6 and 7, p. 33)*.

Ultimately, the BCEB assessment system provides leaders with an understanding of how well the organization is performing against those processes that work effectively for firms that excel at product and service quality. By completing the BCEB and identifying the organization's cybersecurity performance excellence maturity level, security leaders benefit by understanding, prioritizing and improving those processes that are critical to achieving sustainable results. Executives and board members benefit from the BCEB's business-focused language and clear alignment to organizational mission and objectives.

EARLY CHALLENGES

The BCEB does appear to have some early challenges. Baldrige released the first draft of the BCEB with modest fanfare in September 2016. During the period from draft to version 1.0, the document did not receive wide attention from security professionals. At its formal unveiling in April at Baldrige's Quest for Excellence® Conference, the first published version of the BCEB was greeted by a relatively small audience of Baldrige fans and supporters.

Evidence suggests that, to date, few organizations have conducted a BCEB self-assessment, though the actual figures are difficult to verify. Nevertheless, this author strongly believes that the Cybersecurity Initiative and the BCEB will take some time to establish their place as indispensable resources for business leaders.

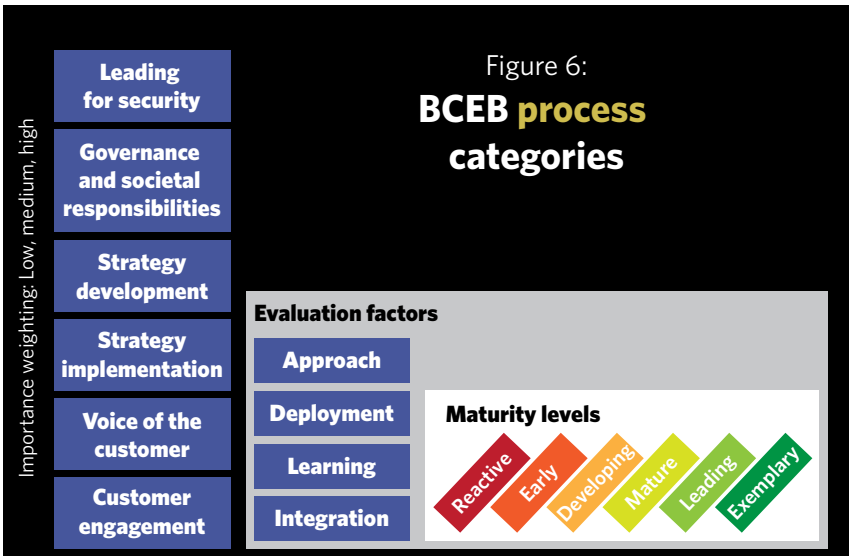
At this point, the fate of the BCEB rests in the hands of security professionals. "Expansion of the BCEB," says Witte, "will be based on future funding and community feedback."

Security leaders may also discover some road bumps while introducing the concepts of BCEB to stakeholders and peers. First, some practitioners may find that quality is too foreign a concept to serve as a cybersecurity-focused metric, fearing that this idea is too closely connected to global industrialists. It shouldn't be. Security leaders who aspire to some degree of conformance with ISO standards—namely, ISO/IEC 27001—already have some fluency in the international language of quality.

There are also those who may doubt that they can free their superiors from engrained perceptions about information security as an IT issue needing exclusively IT-focused solutions. Those who have experienced such pushback in the face of change understand that they are in the vanguard of a new movement, which is seldom a comfortable place to be.

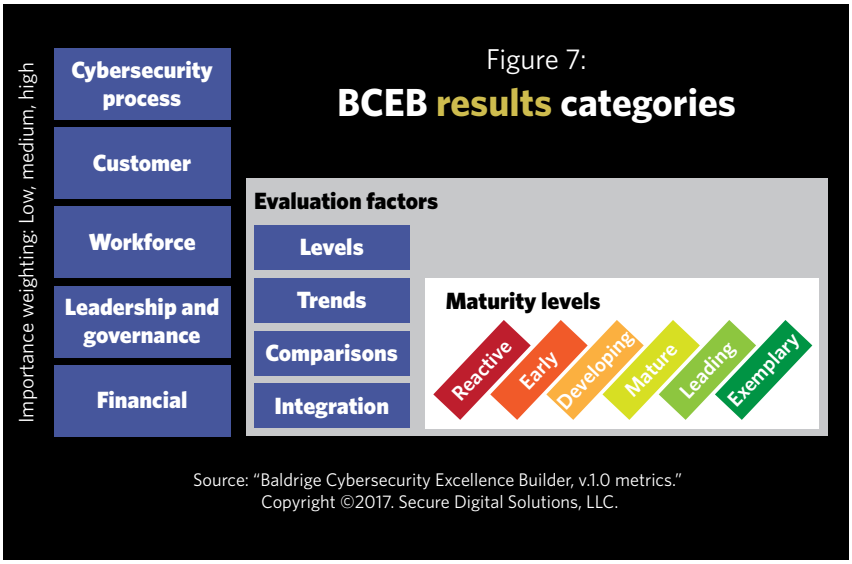
Nonetheless, for those brave security leaders who desire that coveted "seat at the table" with key stakeholders, the BCEB provides a fresh starting point to be heard. ■

Figure 6:
BCEB process categories



Source: "Baldrige Cybersecurity Excellence Builder, v.1.0 metrics." Copyright ©2017. Secure Digital Solutions, LLC.

Figure 7:
BCEB results categories



Source: "Baldrige Cybersecurity Excellence Builder, v.1.0 metrics." Copyright ©2017. Secure Digital Solutions, LLC.

ADAM STONE, *principal consultant and chief privacy officer for Minneapolis-based Secure Digital Solutions, has more than 27 years' business leadership experience with 17-plus years overseeing data privacy and security functions for healthcare, insurance, financial services and marketing organizations. He can be reached at astone@trustsds.com.*

For more information about the Baldrige Cybersecurity Initiative, visit www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative.

ARE YOU REINVENTING THE WHEEL?

BY DANIELA COOPER, CISSP

Making the most of free cybersecurity resources can save time, not just money.

ILLUSTRATION BY ENRICO VARRASSO

WITH INFORMATION SECURITY, it's always tempting to forge ahead with your own ideas to make your organization more secure. While you shouldn't forget or abandon your own ideas (you truly may have thought of something original), before leaving the planning stage, you should check certain resources to make sure something hasn't already been done—and done better.

The following resources are both comprehensive and free (at the time of writing).

NIST—National Institute of Standards and Technology (U.S. Department of Commerce)

www.nist.gov
http://csrc.nist.gov/publications/PubsSPs.html

NIST was founded in 1901 and its mission is to advance measurement in science, standards and technology. The particular group of standards that are worth mentioning:

- SP 800—Computer Security
- SP 1800—NIST Cybersecurity Practice Guides
- SP 500—Computer Systems Technology

I used the NIST Special Publication 800-30 to create information risk assessment forms. They have evolved quite a bit since then, but this publication gave me a really good starting point. When you are staring at a blank white page, it's hard to get started. Standards like these give you a good starting point; from there, you can refine it and make it relevant to your organization.

ENISA—European Union Agency for Network and Information Security

www.enisa.europa.eu
https://www.enisa.europa.eu/publications

ENISA, founded in 2004, is a center for cybersecurity excellence in Europe. ENISA's activities include recommendations, policymaking and implementation, and collaboration with operational teams throughout the EU.

ENISA regularly provides threat landscape reports as well threat landscapes for specific technologies. In addition, ENISA offers publications on risk management (including cloud risk assessment) and business continuity and provides example templates. ENISA is a treasure trove of information and one definitely worth investigating.

UCISA—Universities and Colleges Information Systems Association

www.ucisa.ac.uk
https://www.ucisa.ac.uk/publications

UCISA is a nonpartisan association that represents most of the United Kingdom's universities and higher education colleges with an interest in information systems and technology.

UCISA publishes best-practice toolkit guides and case studies. One such toolkit guide is the UCISA Information Security Management Toolkit (2015) that was created by a collaboration of several U.K. universities. In the pipeline, there is ongoing development work to create an ISMS (Information Security Management System) compliance tool that will look at consolidating an organization's information and allow the organization to link relevant information on different levels.

There are other information security publications worth looking at, including *Secure Network Management* and *Effective Risk Management for IT and Business Change Projects*.

CIS Benchmarks and Controls—Center for Internet Security

https://www.cisecurity.org/
https://learn.cisecurity.org/benchmarks
https://learn.cisecurity.org/20-controls-download
https://www.cisecurity.org/cybersecurity-tools/

The Center for Internet Security is a nonprofit entity that helps private and public organizations defend themselves through the use of the benchmarks and controls that CIS has developed. These benchmarks and controls are the international standards and recognized as best practice for securing IT systems and data. The CIS also provides tools, services and memberships. Some of these are provided for free; all are worth checking out.

The CIS benchmarks are configuration guidelines that will help you secure your operating systems, software and network. They have benchmarks for more than 100 platforms and technologies.

The CIS controls are a list of controls in order of priority that will help you protect your organization from attack. The first five controls are listed as the most important and those that will help you eliminate the majority of vulnerabilities from your organization. All of the 20 controls in their entirety will help to protect your organization as a whole.

ISO—International Organization for Standardization ISO/IEC 27000 Series

https://www.iso.org/
http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

The International Organization for Standardization (ISO) is an independent international organization founded in 1947. ISO now has 163 members from national standards bodies and 779 technical bodies that work on standards development.

Though there are many ISO/IEC series, the ISO/IEC 27000 Series is a strong starting point. This series consists of 20 ISMS-related standards. They cover controls, measurement, risk management, auditing requirements, governance, guidelines for telecommunications organizations, guidelines for financial services, cloud services, guidelines

for the energy utility industry and information security management in healthcare.

A lot of organizations now ask for ISO 27001 certification as a prerequisite for buying or using a service. It has become a benchmark that organizations look for when buying a new service.

The ISO/IEC 27000 Series alone will keep you very busy, but there are other standards worth looking into.

- ISO/TR 17944—Framework for security in financial systems
- ISO/IEC 21827—Systems security engineering
- ISO/IEC 27036—Information security for supplier relationships
- ISO/IEC 29100—Privacy framework

There are many more but these are a good set to get started.

While there are many other useful resources out there, I have tried to focus on the freely available options with an emphasis on information security. It's worth bearing in mind that no standard or policy is likely to be a perfect fit for your organization without doing some editing to make it appropriate for your needs. However, checking out these resources may help you discover something that you hadn't even thought of, and it's those little gems that are worth looking for.

So, before you commit yourself to creating a new framework or guideline from scratch, I encourage you to check the numerous free resources available and see if you could save yourself some time and effort. ■

DANIELA COOPER, *CISSP, lives in the United Kingdom. She has worked in information security for 13 years and is currently focused on building security awareness within organizations.*

FOCUSING ON EDUCATION AND RESEARCH INITIATIVES

center points

BY PAT CRAVEN

Hugely Successful Garfield Cyber Safety Adventures Continue

IN OCTOBER 2016, your Center for Cyber Safety and Education launched one of its biggest initiatives to date: teach children how to be safe online through an exclusive partnership with Jim Davis, the creator of everyone's favorite cartoon cat, Garfield, and Dr. Cybrina, CISSP.

Garfield's Cyber Safety Adventures is the series of cartoons and comic book safety trainings that has helped some 10,000 children worldwide learn different ways to remain safe while online. The first official lesson, released last October, focused on basic safety and privacy. Lesson two, released in March, looked at the dangers of posting too much on social media. The third lesson, to be released in October, takes on the hot topic of cyberbullying.

More Garfield Adventures are already in production, tackling tough topics like illegal downloading, sexting and malware.

The Garfield program is being well received worldwide. Educators' kits have been shipped to a dozen countries. In addition to schools and libraries adopting the program, there are discussions with several countries about making the Garfield program and Safe and Secure Online their official curriculum on cyber safety.

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

There are other great educational programs available. But we believe the Garfield one is the best. Here's why:

1) The content is developed by the best cybersecurity professionals in the world…the members of (ISC)². No other organization can offer that kind of quality.

2) Every part of the Safe and Secure Online program is fresh and new. Some of the other programs you see out there haven't been updated in years.

3) Garfield. No one else has the rights to use Garfield to teach young children how to be safe online. Other organizations have developed their own cartoon characters, but they don't have the instant recognition and acceptance of Garfield. Children (and many of us adults) have grown up with Garfield. They love to sit and watch a Garfield cartoon or read a comic book on one of his adventures. The entire lesson only takes about 20 to 30 minutes.

4) It's almost entirely free. Most of the safety programs offered are available for free online at www.SafeAndSecureOnline.org. The educators' kits for the classroom, which include everything needed to teach 30 children, are sold at cost.

The next year promises to be even better as the Center for Cyber Safety and Education continues to develop more Garfield lessons and expand into different languages.

I encourage everyone to review materials available at www.SafeAndSecureOnline.org and find out how you can help get these fun lessons in the hands of children, parents and senior citizens around the world. It will take everyone to make it a safer cyber world. ■

5 minutes with...

JULIETTE KAYYEM

She's a homeland security expert, successful consultant, Harvard scholar, author and cable news contributor. Juliette Kayyem also is a keynote speaker at Security Congress this month in Austin.

Given your accomplishments in security, media and academia, how does a focus on cybersecurity help you with the other facets of your work life?

I think we have a tendency in the security world to think of cybersecurity as different than other vulnerabilities, like natural disasters, and we tend to put it on a pedestal. But for the most part, dealing with and addressing cybersecurity is very consistent with other challenges we face: How do you minimize the risk? How do you maximize the defenses? How do you ensure that after something happens, you limit the consequences? How do you build more resilient systems?

In many ways, cybersecurity, while technologically different, is very similar to other disciplines. Don't isolate cybersecurity so much that you ignore it or don't include it in an overall risk reduction strategy.

Which is scarier: addressing homeland security officials, Harvard students, *Boston Globe* readers or CNN viewers?

Definitely the most demanding would be students. It's not too corny to say people really do try to work together, even in these highly polarized times. When it comes to safety and security, there really is a unity of effort in most instances.

With CNN, most of the time I'm alone in a room with a camera. So that's relatively easy. But with students, just given their expertise and the anxiety that students face about the world they are entering, they need the most tender love and care.

Your most recent book, *Security Mom*, talks about ways for all of us to feel safer in our homes and homelands. What is the biggest takeaway still relevant in today's geopolitical climate?

Each of us has the capacity to own our own safety and security. We should not delegate to the experts like myself. And that begins at home.

My goal is to tell the story of our homeland security that people can relate to because our own sense of preparedness begins at home. The message of that book is you can't ignore it and you can't be paralyzed by it.

What's your view on the value of cybersecurity certifications?

I think it's absolutely essential. In the absence of strong federal oversight, which is highly controversial and not likely to happen, we need best practices, protocols, common baseline compliance measures that establish the expert from the riffraff. Without that, as anyone in the industry knows, there's a lot of crap out there and so it's essential that organizations try to create common floors.

How do you recharge?

I'm a big fitness person. I've got the Peloton bike. I run with my dog. I'm a longtime surfer, so if I can sneak out for a couple of hours to get into the ocean, great. I try to put down my phone because the news can get overwhelming. And I try to figure out where my teenaged kids are at any given moment.

Any recommendations for Security Congress attendees while they are visiting Austin?

I've been all over the country, 46 states and Texas numerous times. For whatever reason, though, I've never made it to Austin. I've been invited twice to speak at South by Southwest, but missed it. So I have no idea what to recommend, but I'm so excited to finally be making it to Austin and to Security Congress. ■

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

Photograph: Douglas M. Wei

TechTarget | SearchSecurity

It takes minutes to compromise a system.

Only seconds to be better prepared.

Free Membership Offer

In 93%* of confirmed data breaches, it takes attackers "minutes or less" to compromise a system. It's critical that you arm yourself with the latest information about the industry.

Take 60 seconds to join SearchSecurity, where professionals turn every day to solve their toughest security challenges. As an (ISC)² member, it's **FREE** to join, and you'll gain access to our monthly online **Information Security** magazine, which covers topics like:

- **Malware analysis** beyond the sandbox
- Defending against the **digital invasion**
- Regaining control of **cloud compliance**
- Emerging **security threats** from every which way
- Strategies for **perimeter network security**

Get your free SearchSecurity membership and online magazine at:
www.SearchSecurity.com/ISC2

* 2016 Verizon Data Breach Investigation Report

JOIN THE **LARGEST** CLOUD SECURITY COMMUNITY **TODAY!**

Cloud is becoming the central IT system by which organizations are transforming themselves; the Cloud Security Alliance (CSA) is dedicated to working across the industry to ensure the secure adoption of cloud and emerging technologies.

As a member of CSA your organization can benefit from training, certification, information sharing and the latest research to aid in achieving a trusted technology ecosystem.

TO LEARN MORE ABOUT THE BENEFITS OF JOINING CSA, VISIT

www.cloudsecurityalliance.org

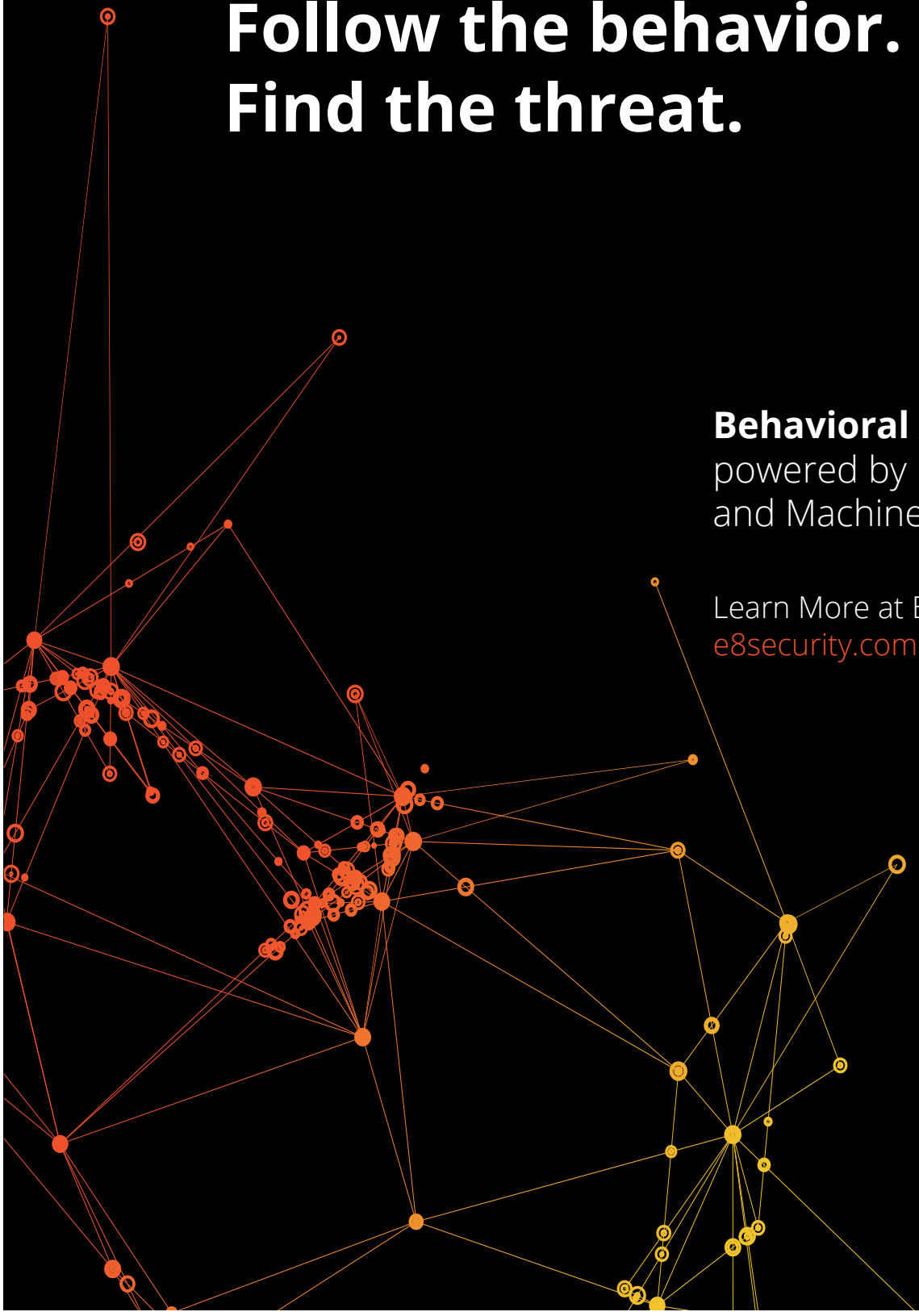
cloud security alliance®


E-BOOKS
ARTICLES
BLOG POSTS
INFOGRAPHICS
CASE STUDIES
NEWSLETTERS
SUCCESS STORIES
A NEW PERSPECTIVE ON YOUR BRAND'S NARRATIVE
Using words and images that are unique to your branding, Twirling Tiger Media can help you tell your company's story cohesively across multiple content marketing solutions.
TWIRLING TIGER media
creators of content you can sink your teeth into
Contact info@twirlingtigermedia.com
Photograph: Aneta Ivanova

E8 SECURITY

DETECT. HUNT. RESPOND.

Follow the behavior. Find the threat.



Behavioral Analytics
powered by Data Science and Machine Learning.

Learn More at Booth #211
e8security.com