LEADERSHIP AND PROJECT MANAGEMENT TIPS FROM AN ISLA® WINNER

InfoSecurity PROFESSIONAL

JANUARY/FEBRUARY 2018

A Publication for the (ISC)²® Membership

Whaling

Targeting Bigger Phish

(ISC)² InfoSecurity PROFESSIONAL 10 YEARS

SOC IT TO 'EM

CPAs inspire an industry-agnostic cybersecurity framework

BLOWN AWAY

Cutting down on the noise in threat intelligence feeds

What's the best kind of code? One that saves you $200 on RSAC 2018.

Each spring, many of infosec's brightest minds jet-set to San Francisco for five days of the industry's best. Best what, you ask? Everything. And as an (ISC)² member, you can get in on all RSA Conference 2018 has to offer… for $200 less.

So from April 16-20, 2018, here's what you can expect:

- Cutting-edge keynotes from cybersecurity experts and compelling speakers, including Brad Smith, President of Microsoft, David Ulevitch, Senior Vice President/General Manager of Cisco, Monica Lewinsky, and more
- (ISC)² CCSP Two-Day Crash Course where we'll cover everything from hacker tools to Cloud application security
- (ISC)² CISSP Two-Day Crash Course focused on the eight domains in the Certified Information Systems Security Professional CBK
- And hundreds of the industry's best exhibitors, spanning two full Expo halls

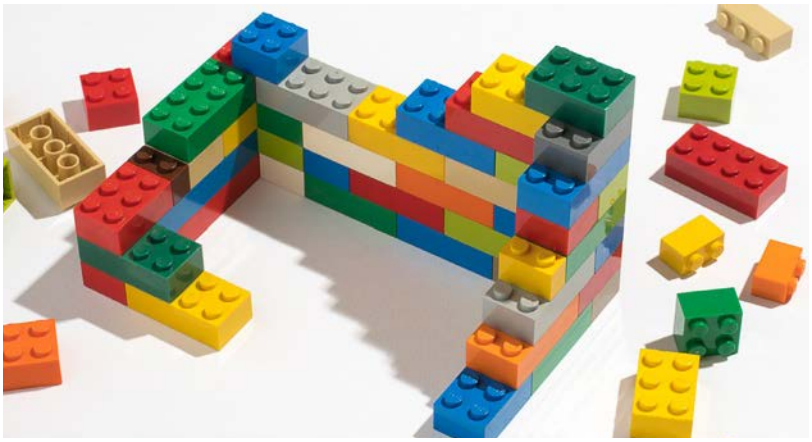
Don't wait for greatness. Register for it. **www.rsaconference.com/isc2**

Use code **18UISC2FD** when you register to save $200 on a Full Conference Pass.

Follow us on: #RSAC

contents

VOLUME 11 • ISSUE 1



You can use guidelines that CPAs follow for cybersecurity examinations and reports to build a stronger security posture. PAGE 22

features

Cover photograph and image above: JOHN KUCZALA

departments

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

editor's note

BY ANNE SAITA

Ten Years Serving the Membership

THIS YEAR MARKS the 10th anniversary of *InfoSecurity Professional*. Technically, it kicks off with one of the spring issues, since the magazine was quarterly until four years ago. That's when a team moved the publication from four to six times a year and added a between-issue e-newsletter, *Insights*. Last year we added a second, bimonthly e-newsletter, *Cloud Security Insights*.

All of these publications not only provide more educational materials to help (ISC)² members in their careers, but also more opportunities for members to contribute their own thought leadership. It is an increasingly complex cybersecurity world out there, not to mention far more is now expected of security professionals, especially those carrying an (ISC)² credential. Hearing from those on the front lines and in boardrooms is important as we work to gain as firm a grasp as we can on the issues of the day.

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

I do hear you. I read every member email asking about disseminating issues to their teams or suggesting future stories. Often, people want to contribute articles themselves, and I encourage it. There is, however, a process we follow—guidelines to make sure magazine and newsletter articles appeal to 125,000 members located all over the world. Are some pieces too simplified? Perhaps. Others too deep? Maybe. But finding that median with such a diverse group is never easy.

Finding innovative ways to continually improve isn't easy either, but we try. That's why I hope to continue hearing from readers on what's working and what needs to improve. Your feedback is always shared with our international editorial advisory board and appreciated by me. Even the critical comments, which fortunately are currently far outweighed by positive ones. I, for one, hope that ratio continues. ■

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

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

TWIRLING TIGER MEDIA EDITORIAL TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

MANAGING EDITOR
Deborah Johnson

EDITOR
Paul South

PROOFREADER
Ken Krause

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

RETURN TO CONTENTS

Join the new (ISC)²® Community!

For cybersecurity and IT professionals

CONNECT.
COLLABORATE.
SHARE.
DEVELOP.

community.isc2.org

THE LATEST FROM (ISC)²'S LEADERSHIP

executive letter

BY DAVID SHEARER, CISSP

Enrich. Enable. Excel. The (ISC)² Guiding Theme for 2018

FOLLOWING THE OUTSTANDING SUCCESS of last year's (ISC)² Security Congress events—which culminated with a record 2,000 attendees at our North America Security Congress in Austin, Texas—I challenged the team at headquarters to ensure 2018 is packed with even greater value for all our members.

What they delivered is Enrich. Enable. Excel., an exciting guiding theme for everything we are doing for members in the coming year. From new CPE opportunities and events to new programs or technology deployments, Enrich. Enable. Excel. is our measuring stick for how we are meeting your needs and delivering the value we owe you.

How does it work?

ENRICH.

Enrich your career and profession by continually sharpening your skills, honing your craft and enhancing your expertise. (ISC)² CPE opportunities enable you to continue enriching your career by educating you on the broad array of concepts you need to build your expertise and help your organization better protect its data.

My challenge to the teams driving any new initiative at (ISC)² is to ensure we are developing enriching content and tools that help you remain a well-rounded, informed cybersecurity professional. In 2018, delivering enriching education through our CPE program, events and anywhere else is a top priority.

David Shearer is CEO of (ISC)². He can be reached at dshearer@isc2.org.

ENABLE.

Enriching CPEs and events will immerse you in relevant domains, timely issues, technical challenges, and soft skills development crucial for your career growth and the health of the profession as a whole. These tactical, focused learning opportunities enable you to become a more well-rounded and effective practitioner.

But just delivering enriching activities alone isn't enough. CPE opportunities must be on point. Education materials and event programs must be easy to access, consume and implement. New online tools in our member portal need to be more efficient and make your life easier. Doing all that is how we will enable members in 2018.

From new CPE opportunities and events to new programs or technology deployments, Enrich. Enable. Excel. is our measuring stick for how we are meeting your needs and delivering the value we owe you.

EXCEL.

This is where you come in.

By taking full advantage of our enriching CPE opportunities, and enabling yourself to focus on what's most important for you and your organization, you will excel. You will achieve your personal and professional goals. And when you excel as an individual, the organization you support becomes better at securing its data, fulfilling its vision and accomplishing its mission.

Everything we do at (ISC)² is focused on helping you strengthen your career. In 2018, it starts with Enrich. Enable. Excel. You may not always see it on a banner or hear it spoken aloud at a conference, but Enrich. Enable. Excel. is guiding all we're doing to help deliver the value we owe you. ■

(ISC)²

SECURE SUMMITS / 2018

#ISC2Summits

Join the Sharpest Minds in Cybersecurity at (ISC)² Secure Summit DC

MGM NATIONAL HARBOR
D.C. METRO AREA

May 7 – 9, 2018

Register Now

(ISC)² Secure Summit DC (formerly CyberSecureGov) unites the sharpest minds in cybersecurity for two days of insightful discussion, workshops and best-practices exchange. Join us and you'll walk away better equipped to tackle today's biggest cyber challenges and advance your career.

WHY ATTEND?

- Secure your place among cybersecurity leaders in government, military, industry and academia
- Gain fresh perspectives from the most experienced minds in our profession
- Earn up to 20 CPEs

Register by March 30 and Save!

Secure your place at (ISC)² Secure Summit DC today.
Early bird registration ends March 30, 2018.

Learn more about **(ISC)² Secure Summit DC** | #ISC2Summits

ENRICH. ENABLE. EXCEL.

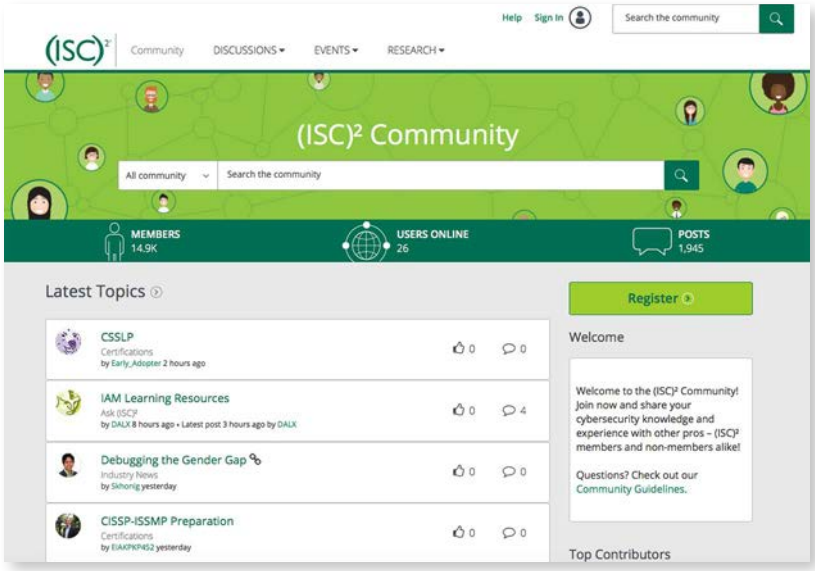
field notes

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

EDITED BY DEBORAH JOHNSON

Attention Pros: There's a New Place to Connect

(ISC)²'s new online community is up and thriving.



GOT A QUESTION about a new potential cyber threat? Or perhaps you have an experience in developing a security platform you want to discuss? The (ISC)² Community website is just the place for you.

You'll be joining more than 15,000 cybersecurity practitioners, both (ISC)² members and nonmembers, who've already signed up to keep up with the latest industry ideas and issues as well as membership and career questions.

The goal of the community is to provide a shared space for all cybersecurity professionals and practitioners to connect, collaborate and develop best practices required to manage the ever-evolving needs and interests of the industry.

To access the new community, please visit https://community.isc2.org. If you already have a login at isc2.org, you'll be able to access the community with your existing credentials. If you do not have an account on the (ISC)² website, you'll need to create one during the login process by clicking "create an account." Once you access the community, you will be able to create your own username, personalize your profile and upload a profile image. Should you encounter any technical issues, contact our Community Management team at community@isc2.org. ■

TOP 10 2017 (ISC)² NORTH AMERICA WEBCASTS

The following were the highest rated webinars as of Nov. 15. Some require registration to view.

Pt. 1: Future of SIEM – Why Static Correlation Fails Insider Threat Detection
https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=257419

Visibility and Security – Two Sides of the Same Coin
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=237215

A NIST Guide on How Identity Management is Reshaping Cybersecurity
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=280685

Scaling Up Network Security: Shifting Control Back to the Defenders
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=270911

GDPR – Now's the Time to Plan for Compliance
https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&PCAT=7540&CAT=10645

Cross Talk: How Network and Security Tools Can Communicate for Better Security
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=237217

Future of SIEM – Remediate Malware and Spear Phishing with Automated Playbooks
https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=257423

CA Briefings Part 5 – Trends and Predictions
https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=225477

Briefing on Demand: Getting it Right – Security and the Internet of Things
https://www.isc2.org/en/News-and-Events/Webinars/Security-Briefing?commid=260785

Building a Blueprint for an Insider Threat Program
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=248443

Reimagine Your Identity Strategy
https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&PCAT=7540&CAT=10580

The Human Target – The Tip of the Spear is Aimed at You
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=256057

Computerized Adaptive Testing Now Available for English CISSP® Exams

AS OF DEC. 18, (ISC)² will provide computerized adaptive testing (CAT) for all English CISSP exams worldwide. Based on the same exam content outline as the linear, fixed-form exam, CISSP CAT is a more precise and efficient evaluation of your competency. CISSP CAT enables members to prove their knowledge by answering fewer items and completing the exam in half the time.

According to the (ISC)² website, "Each candidate taking the CISSP CAT exam will start with an item that is well below the passing standard. Following a candidate's response to an item, the scoring algorithm re-estimates the candidate's ability based on the difficulty of all items presented and answers provided. With each additional item answered, the computer's estimate of the candidate's ability becomes more precise—gathering as much information as possible about a candidate's true ability level more efficiently than traditional, linear exams."

This new format reduces the maximum exam administration time from six to three hours and the items necessary to accurately assess a candidate's ability from 250 to as few as 100 items.

The exam content outline and passing standard for both versions of the examination are exactly the same. Each candidate will be assessed on the same content and must demonstrate the same level of competency regardless of the exam format. CISSP exams in all other languages, as well as all CISSP concentration exams, are delivered as linear, fixed-form exams.

Learn more at https://www.isc2.org/certifications/CISSP/CISSP-CAT. ■

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=10726

TOP 10 2017 (ISC)² APAC WEBCASTS

The following were the highest rated webinars as of Nov. 15. Some require registration to view.

Equifax: Exploring the Root Causes of the Major Data Leak
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=284833

The Nuix Black Report: Find Out What Hackers are Really Thinking
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=242159

Collective Security – Prairie Dogs vs. Humans
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=262777

Recent DDoS and Web Attack Trends
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=259335

DDoS Threats of Past, Present and Future
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=242161

The Evolution of Vulnerability Management – Program Trends and Solutions
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=268223

Improving Credential Abuse Threat Mitigation
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=271153

Research Findings: Quantifying ROI for Application Security
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=263977

Understanding Security Threats and Document Theft (Intrusion) Attacks
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=271451

Internet Security Status Report: An Overview of Web App Attack Trends
https://www.isc2.org/News-and-Events/Webinars/APAC-Webinars?commid=261129

$93,322

Average cost of network intrusion investigation

Source: Baker & Hostetler 2017 Data Security Incident Response Report. Review of 450 incidents.

https://www.databreaches.net/baker-hostetler-2017-data-security-incident-response-report-based-on-450-incidents/

Photograph: iStock/Urupong

(ISC)² Celebrates Outstanding Cybersecurity Professionals in Europe, the Middle East and Africa

THE INAUGURAL (ISC)² EMEA Information Security Leadership Awards (ISLA®) offered the opportunity for the EMEA community to recognize peers going the extra mile to enhance security in the region.

More than 200 nominations in four categories were reviewed by members of the (ISC)² Europe, Middle East and Africa Advisory Council, who scored submissions based on:

- Expertise
- Dedication
- Impact
- Innovation
- Leadership
- Community engagement

And the EMEA ISLA winners are:

Senior Information Security Professional

Patrick Wheeler, Director at CyberWayFinder (Belgium)

A cybersecurity practitioner whose work focuses on securing the global financial sector, Patrick Wheeler works as a consultant and volunteer mentoring women in cybersecurity. His role as director at the nonprofit organization CyberWayFinder led to his selection. CyberWayFinder aims to increase diversity and promote women in cybersecurity through education, training and job opportunities across Europe and Asia and in partnership with the (ISC)² BeLux Chapter. "I had no choice but to pursue this," Wheeler said. "Perhaps this award is the best measure of my work. This is also for all of the supporters, mentors, hiring managers and candidates in the diversity effort."

Up-and-Coming Information Security Professional

Brencil Kaimba, Security Consultant at Serianu Limited (Kenya)

Brencil Kaimba has been mentoring university and high school students through the Cybersecurity Training and Awareness for Young People program in Kenya. She has been praised for playing a key role in facilitating a similar initiative at work, as well as mentoring young girls on issues including cyberbullying and cybersecurity. Kaimba also was lauded for demonstrating expertise in both technical and nontechnical skills in the field. Through her work alone, she has motivated young girls to venture into the profession. "I am thrilled and delighted by this tremendous honor," she said.

Woman Information Security Professional

Denise Murtagh Dunne, Information Security Manager at PwC (Ireland)

Denise Murtagh Dunne was commended for her work as information security manager at PwC as well as her involvement with the company's information security community. She has been hailed for her efforts, through meetings and events in Dublin, in encouraging women to look to the profession as a career prospect. Denise regularly explores creative ways to engage the community and create a real buzz in the sector. Denise stated: "I am delighted to receive this award, as the nomination is made by my peers. It means a lot to me to know that the work I do is so highly regarded."

Information Security Practitioner

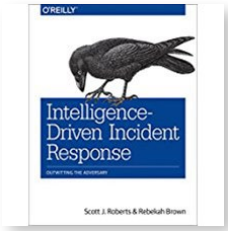
Peter O'Boyle, Information Security Manager at ICON (Ireland)

Peter O'Boyle's award recognizes his implementation of an information security vendor risk program to ensure vendors are risk-assessed before access to data is provided or entrusted to them. His ability to work with business and navigate difficult technical, legal and regulatory obstacles has been regarded as remarkable. O'Boyle also was recognized as a positive influence on others, with colleagues saying he "inspires people to do better and strive for higher standards, as his enthusiasm and energy are infectious." Peter remarked: "I'm delighted and honored to be one of the first recipients of the EMEA Information Security Leadership Awards." ■

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

Intelligence-Driven Incident Response: Outwitting the Adversary

By Scott J. Roberts and Rebekah Brown
(O'Reilly Media, 2017)



WITH THE DAILY INCREASE in successful cyberattacks, organizations are upping their security efforts; as such, business is booming for independent security services. Authors Scott Roberts and Rebekah Brown share their experiences with incident management and threat intelligence in a valuable reference book.

Intelligence-Driven Incident Response focuses on key areas designed to enhance an organization's safety. With a clear, professional approach, the interrelationship between incident management and threat intelligence is outlined along with details on how to build a threat intelligence program.

Understanding the attacks and attackers is key, and the authors offer advice on:

- Mining previous incidents for clues to the intrusions
- Knowing the terrain and understanding the objectives of the attacker
- Knowing where your data is
- Following a "F3EAD" process—find, fix, finish, exploit, analyze and disseminate

Roberts and Brown discuss strategic and operational considerations as well as technology and tools to store threat intelligence and offer tips to enrich this data, such as relying on WHOIS and other DNS information. This book is effective in discussing the use of TAXII/STIX, which is a recent approach in reviewing and analyzing threat intelligence.

Two areas the authors did not address: (a) how best to communicate the threat intelligence to the business user or senior management; and (b) how to prioritize the program of threat intelligence over other security-related priorities.

Overall, *Intelligence-Driven Incident Response* is geared for individuals with exposure to security incidents and threat management and offers valuable insight and suggestions to enhance security professionals' efforts at staving off intrusions. ■

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

TOP 10 2017 (ISC)² EMEA WEBCASTS

The following were the highest rated webinars as of Nov. 15. Some require registration to view.

The Next Generation CISO: How to Find and Train Tomorrow's Security Executives
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=273313

Latest Malware Trends and Attack Vectors
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=262621

A Day in the Life of a GDPR Breach
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=272921

Guarding Against Mobile Malware, How to Avoid the Next Big Threat
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=274717

Reduce Security Vulnerabilities in Enterprise Applications
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=270951

Part 1: 6 Steps to GDPR Compliance
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=270415

Don't Be the Next Victim of a Ransomware Attack
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=259425

Getting started with GDPR, Privacy and Applying Appropriate Security Controls
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=249535

Security in the Age of Open Source
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=240627

Phishing Response: Stop the Chaos
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars/Focused-Webinars?commid=277627

Photograph: iStock/Madrolly

RETURN TO CONTENTS

#nextchapter

EDITED BY DEBORAH JOHNSON

(ISC)² BEIJING CHAPTER

Strong Member Growth for China's Second Official Chapter

Beijing member meeting and security conference.

THE (ISC)² BEIJING CHAPTER provides a strong sense of belonging for the (ISC)² credential-holders in the region. It is China's second chapter; the first is Shanghai, and Guangzhou is progressing through the chartering process. By encouraging individual career development and experience exchanges, as well as information and technical sharing, the chapter has experienced positive growth in a short time, recruiting 110 members in the three years since its formation.

The Beijing Chapter's goal is to establish a network for cybersecurity professionals in the city and surrounding areas. To that end, the chapter has hosted 13 information security salons. With the support of the (ISC)² Beijing Office, these events have enabled members to build up their personal and professional networks. Security salon speakers include both domestic and international cybersecurity experts.

In addition to hosting face-to-face seminars and events, the Beijing Chapter has established its official WeChat page. Member groups and WeChat Moments have been created to facilitate the sharing of knowledge and latest information security updates.

The Beijing Chapter sees a bright future for its members. The chapter welcomes new members and offers speaking opportunities for (ISC)² members who are traveling to the city. ■

(ISC)² BEIJING CHAPTER CONTACT INFORMATION

Chapter Chairman: Zhou Bin

Email: info@isc2chapter-beijing.org

(ISC)² WELCOMES NEW CHAPTERS

Five new (ISC)² chapters were recently added to the North America region.

Central New Mexico Chapter. The Central New Mexico Chapter has more than 49 (ISC)² members and over 42 general members. The chapter hopes to increase community outreach by working with senior citizens and veterans to promote a more safe and secure community.

North Central West Virginia Chapter. The North Central West Virginia Chapter has a prime location in the cybersecurity industry; nearby are the FBI Criminal Justice Information Services Division, NOAA (National Oceanic and Atmospheric Administration) and NASA's Independent Verification and Validation (IV&V) Facility. The chapter's interests are to provide more networking opportunities as well as training and education for its chapter members.

Pennsylvania Highlands Chapter. Located in a remote area in Pennsylvania, the Pennsylvania Highlands Chapter gives information security professionals in the area the opportunity to network, exchange ideas, collaborate, earn CPEs and serve the local community through promoting the awareness of cybersecurity, especially through the local university.

Waterloo Region Chapter. The Waterloo Region Chapter is located in what is considered Canada's Tech Hub. The chapter, with its 18 (ISC)² members, promotes awareness of (ISC)² as well as engages local information security professionals in networking, community service and education.

Wichita Chapter. The Wichita Chapter's interests are to bring cyber academia to local businesses with hands-on learning activities, to help individuals seeking an (ISC)² certification and to promote cybersecurity among local professionals in the community. ■

#nextchapter

Zuohua Lu (L) participates with schoolchildren for a TV program on internet safety.

Q&A ▶ ZHOU BIN, CHAIRMAN, (ISC)² BEIJING

Zhou Bin

What are some of the challenges the chapter faces in growing the membership?

There are two challenges. One is that we are entering a stable growth period, as security professionals are just a small portion of the IT community. We are asking current members to promote our chapter to their co-workers and the community. Hopefully, once more security professionals get to know us, they will join the chapter.

The second challenge is to attract a wider variety of security practitioners. Most of our current members are security managers or directors of information security or risk management. We don't have many members who focus on hacking or vulnerability research. If we can engage those people, the dialogues between defenders and ethical hackers could be very interesting and fruitful.

What are the most requested topics of discussion by members?

Members are eager to follow the latest security trends. Members also request us to invite speakers from big internet companies to understand how they secure the system on a very large scale. Regulation topics like the new China Cyber Security Law are always discussed online in WeChat groups and offline at the members' meeting.

What community outreach does the chapter offer to the public to increase cybersecurity awareness?

The chapter worked with Beijing TV to produce an hour-long program on safe surfing for youths during the summer holiday. Zuohua Lu, the secretary general of the Beijing Chapter, demonstrated ways to protect privacy and identify harmful games. More than 20 youths aged between 8 and 12 participated in the discussion and a quiz. This program was also live on Beijing TV's mobile app and attracted more than 10,000 viewers. ■

MUSINGS ON SECURITY ISSUES THAT IMPACT MEMBERS

advocate's corner

BY JOHN McCUMBER

Answering to Members ... All 125,000 of You

YOU THINK YOU HAVE problems with your boss? I feel you. I recently took a job where I have more than 125,000 bosses, but it's still the best job ever. I am stoked to be the first-ever director of cybersecurity advocacy, North America for (ISC)². In a world of zany titles, what the devil kind of work does this job entail?

Most of this job will require me to ensure I am responsive to you, our members, and reflect your concerns to our federal and state government entities, industry and academia. I am especially honored to be here at this critical time when our profession has leaped into the daily headlines. Large-scale exploits, public data breaches and the daily exposure of security vulnerabilities virtually guarantee most everyone is aware our professionals are on the front lines. It's our time to shine.

Over the last 20 years, we have seen the evolution of computer security management, as it was then known, to the complex technical world where protecting sensitive digital resources and mission-critical applications has become central to our national interests. As director of cybersecurity advocacy, I'm rolling out a strategy to be more responsive to our members by focusing the consortium's outreach on key initiatives, especially as they relate to proposed legislation, personnel issues and workforce development.

One of the first programs I am pursuing involves dramatically expanding outreach programs like Virginia's Veterans Cyber Training. Through this new program, (ISC)² helps our veterans combine their hard-won military experience with education and training to document industry-leading cybersecurity skills that are in great demand across private and public organizations.

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

Other states are now seeing the benefits, and we are at the table to provide both training and a roadmap for rewarding careers. Such programs also serve as a blueprint for state and local governments to provide 21st-century jobs for underserved communities and retrain adult workers. We will continue to help drive this workforce innovation, and help close the skills/employment gap in cybersecurity.

> **Whether you are looking to begin your career journey as one of our associates, or you're a seasoned professional, (ISC)² is committed to being your best resource for career knowledge and advancement.**

This new role also requires me to ensure the consortium pays down the debt we owe to our existing members by providing them with cutting-edge research and analyses they can use to meet the ever-expanding demands of our shared profession. I intend to implement new capabilities to inspire our government and business leaders to engage not only in the business of cybersecurity, but to take an active role in the broader societal changes necessary to make our digital world a safer place for everyone.

Whether you are looking to begin your career journey as one of our associates, or you're a seasoned professional, (ISC)² is committed to being your best resource for career knowledge and advancement. To remain relevant in this fast-paced industry, we aim to be your locus for a lifetime of learning and professional growth.

I will be here to magnify our voices every day, whether it's on Capitol Hill with our legislators, or in the trenches with practitioners and researchers. Please join me in the (ISC)² Community, at one of our many events or as a participant in one of our committees. I look forward to working for you, boss. ■

(ISC)²

SECURITY CONGRESS | APAC 2018

Enrich. Enable. Excel.

SAVE THE DATE

9-10 July 2018 | Hong Kong

50+ Speakers | **2** Days | **6** Tracks | **35+** Sessions

At (ISC)² Security Congress APAC 2018, you'll get to engage with over 350 security-minded individuals, discover solutions to the latest cybersecurity threats, and gain insight from international industry experts. Maximize your learning experience with our multi-subject sessions, panel discussions, and networking opportunities designed to enrich and enable you to excel as a cybersecurity professional.

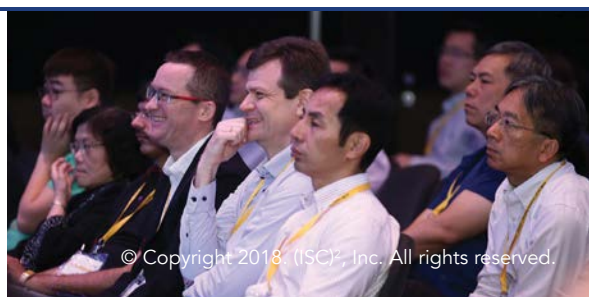
Have questions? Talk to us!

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

In partnership with: image engine

Visit apaccongress.isc2.org

#ISC2congressAPAC



TARGETING THE BIGGEST Phish

TODAY'S 'WHALING' IS BRINGING HUGE PAYOFFS FOR INTRUDERS WHO SUCCESSFULLY IMPERSONATE THOSE TOPPING THE CORPORATE FOOD CHAIN.

BY DEBORAH JOHNSON

THE EMAIL FROM THE CEO of a financial services company asked the client to pay the attached invoices and provided banking information. The company paid. It was a fraud. "They were in the hole for about £200,000."

So relates Carl Chapman, CISSP, the CISO/COO at business consultancy Crescent Bridge, Ltd. based in London, when discussing a successful "whaling" attack on a company with which he was familiar. The attacker "had effectively created a duplicate domain and impersonated the CEO to ask them to pay invoices to a fraudulent bank account."

PHOTOGRAPH BY JOHN KUCZALA

The fraud was eventually discovered "by chance," Chapman says. "Someone spotted it, something just didn't look right. They were able to recover about 75 percent of the amount."

Spear-phishing is not a new threat, but advances in techniques are revealing a more substantial threat for organizations. By more thoroughly researching their targets, these attackers can reel in a considerable payoff—sometimes millions of dollars. Security professionals call it "whaling," because of its success in impersonating much bigger "phish."

According to the U.S. Federal Bureau of Investigation's Internet Crime Complaint Center, between October 2013 and December 2016 there were more than 40,000 domestic and international business email compromises (BEC)—how the FBI designates phishing attacks—adding up to more than US$5 billion in losses.

THE PHISHING EVOLUTION

Phishing has narrowed its focus from the earliest attempts: hackers spreading a wide net to millions of emails loaded with malicious attachments or links, usually from a financial institution, hoping a recipient would fall into the trap. With targeted phishing—spear-phishing—these bogus emails are directed to specific people, seemingly from someone they know—and likely trust.

"It is sent in a way to seem like it is coming from a particular employee," says Kevin Williams, CISO for the City of Austin in Texas. "And based on that person's job function, they craft the message to look like something they would send out. 'Oh, yeah. That's Bob. Bob's a PM. He always sends me something with a link on it.' Then click on it…."

Similarly, Geographic Solutions, a designer of web-based workforce systems based in Palm Harbor, Fla., has received its share of spear-phishing emails, says security and compliance team lead Justin Warniment, CISSP-ISSEP, ISSMP, CCSP, CISM. "We had targeted emails to our financial folks, accounting, also HR. Very targeted at our senior managers, such as directors."

And the emails don't need to be complicated. Nick Johnson, a systems administrator at FNB Bank in Mayfield, Ky., remembers two specific attempts. "They posed as a very high-level bank employee. It was a very simple email that was trying to get us to process a wire. It wasn't like it had a lot of detail to it and that's what made us look at it."

Whaling attacks are "just a continued innovation and evolution of techniques used by hackers," says Matthew Gardiner, senior product marketing manager for Mimecast, an email management and security company based in London. "Instead of pretending to be someone outside the organization, they realized they could be someone with authority inside the organization."

"They posed as a very high-level bank employee. It was a very simple email that was trying to get us to process a wire. It wasn't like it had a lot of detail to it and that's what made us look at it."

—NICK JOHNSON, systems administrator, FNB Bank

Williams adds, "The more sophisticated attacks are usually one link in a very long chain of attacks. In a phishing email posing as a city project manager, when our investigators do forensics on that employee's machine, they will usually find they were the victim of an earlier phishing attack. The earlier attack got the [victim's] name, contact list, message format—all the information that they needed to conduct their next attack. The results of the new attack will become input for the next attack, and so on."

The victims are not only high-profile, news-making organizations. Smaller businesses are impacted just as often, says Erich Kron, CISSP-ISSAP, security advocate for the security awareness training company KnowBe4, based in Clearwater, Fla. "Those companies may lose $20,000 or $30,000"—a smaller sum compared to the losses suffered by larger companies—"but it can be devastating for a company."

KNOW YOUR ENEMY

According to Verizon's 2017 Data Breach Investigations report, which analyzed 42,068 incidents and 1,935 breaches from 65 organizations in 84 countries (http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/), 51 percent of breaches involved organized criminal groups. And these groups are smart, says Kron. "These people are very intelligent—[operating as] businesses more than individuals. We've seen in some of these ransomware strains where they offer tech support. You can chat with them to get them payment."

And just like legitimate organizations, says Mimecast's Gardiner, they find partners. They host "attacks in data centers that will look the other way if you pay them. They split the money the way any company would with those they do business with. 'I'll provide you a ransomware as a service platform if you give me 40 percent of your take.' The key takeaway is: Don't think about it as some random hacker."

Ultimately, says Crescent Bridge's Chapman, "it's actually really simple: It's very cheap to do. Once you undertake that type of attack successfully in one business, then maybe it's an opportunity to do it again and again."

SOME OF THE WHALERS' LURES

The internet and social media have come together as a malicious hacker's dream. The information available online

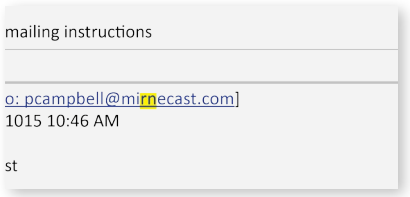
coupled with some knowledge of a specific business can give an attacker all he or she needs, warns Chapman. "A financial services organization that has less than 50 people, it's quite likely they're not going to have all of the services, like payroll and invoicing, they're not going to do those things in-house. They're going to do them externally. If you're able to identify, say—I'll use LinkedIn as an example—C-level individuals at your target business and you can see that they are connected to a managing director of a small payroll business you probably have most of the information you need to perpetrate that crime."

The FBI issued a clear warning in its May 2017 alert: "The subjects monitor and study their selected victims using social engineering techniques prior to initiating the BEC scam. The subjects are able to accurately identify the individuals and protocols necessary to perform wire transfers within a specific business environment."

Social media isn't the only place for data mining. Open-source intelligence provides a raft of valuable information, says KnowBe4's Kron. "You have corporate filings and information like that. Even the company's website has a lot of great information. For example, if an organization is getting ready to do an IPO or a product release, that's great information the bad guys can use to target the executives."

With information from public filings and social media, hackers can create an extremely personal email, says Cory Deeter, director of cybersecurity operations and IT compliance for Finish Line, a retailer of sports shoes and clothing based in Indianapolis. "One example I [saw] was an email sent to a CFO from a supposed close college friend. The email referenced college nicknames for one another and included a malicious attachment."

Domain and email spoofing is another tool in the whaler's tackle box—and even cybersecurity specialists are not immune as Mimecast's Gardiner relates. "We're mimecast—m-i-m-e-c-a-s-t dot com. They sent it from mirnecast.com [m-i-r-n-e-c-a-s-t]; the 'rn' looks like 'm' to the casual viewer *(see image, below)*. They could send email from that domain as if it were our CEO, in fact, trying to get our CFO to send off money."



Mimecast was not alone in this type of whaling attempt. Proofpoint, a security and compliance company based in Sunnyvale, Calif., investigated attempted email intrusions at more than 5,000 large enterprises in Q4 2016. The investigation revealed that two-thirds of those attacks used spoofing.

TALES FROM THE DEEP

SIX WAY TO STOP WHALING ATTACKS

Educate and inform employees.

Use simulations—staged whaling messages—to detect organizational weaknesses.

Make faking messages difficult by using unique identifiers.

Tap technology using gateway protections such as DMARC, DKIM and SPF.

Stay alert through monitoring services.

Rethink procedures for email authentication and financial transfers.

Source: https://www.mimecast.com/resources/infographics/Dates/2016/8/infographic-tales-from-the-deep/

ESCAPING THE WHALER'S HARPOON

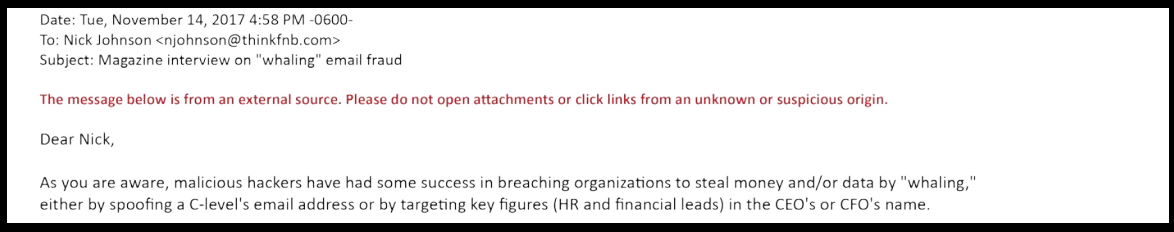
Just as the whalers have the lures and tricks, cybersecurity professionals have their own toolbox.

For Geographic Solutions, Warniment says finding a security awareness training partner, as well as enhancing email security software, has made the company stronger. One key element in training—phishing campaigns. "We target certain users, groups of users or the entire company." Does anyone ever fail? "Oh, yeah. The end user is the weakest link when it comes to IT security and clicking on a malicious link."

EMAIL ALERTS

FNB Bank uses a "transport rule" in its email to alert recipients of potential danger. "A transport rule that we set up for email that comes from outside the bank into the bank, it appends a message at the top of the email that says this is a message from an external source and it has some additional warnings in there about do not open attachments or click links from an unknown or suspicious origin."

—NICK JOHNSON, systems administrator, FNB Bank


Date: Tue, November 14, 2017 4:58 PM -0600-
To: Nick Johnson <njohnson@thinkfnb.com>
Subject: Magazine interview on "whaling" email fraud

The message below is from an external source. Please do not open attachments or click links from an unknown or suspicious origin.

Dear Nick,

As you are aware, malicious hackers have had some success in breaching organizations to steal money and/or data by "whaling," either by spoofing a C-level's email address or by targeting key figures (HR and financial leads) in the CEO's or CFO's name.

Finish Line has also staved off whaling attempts using a combination of approaches, describes Deeter in an email. "We leverage multiple technologies to identify suspicious emails and provide ongoing training for our users. Most importantly, our executives have a keen awareness that they are targets of these types of attacks and they remain vigilant."

Mimecast's Gardiner agrees with the multilayered approach, but sees technology as the strongest component. "It's about having automated controls to try to minimize your dependence on people to always do the right thing, which is hard because people don't always do the right thing. And you have to build up caution in people's minds. You also have to have the process not be dependent on just one email to go wrong. And if you do all these three things really, really well, then you'll be pretty safe from these attacks."

"People are it. They are almost your first and last line of defense," declares FNB's Johnson. The bank has an extensive user awareness program for all employees and focuses on what Johnson calls the "90/10 rule—they're 90 percent of the equation and all of our technology is 10 percent. But," he adds, "if they don't have a buy-in, if you have people actively subverting you from inside and clicking on things they shouldn't click on or going to places they shouldn't go to, then you are not going to get any results."

Williams, in Austin, sees the security challenge through the lens of a public entity. "I think we're better insulated because the CEO just can't come down and tell you 'cut a check. Pay that man right now.' On the other hand, we have a civic obligation to offer things like public Wi-Fi at municipal locations, parks, city hall. We also have to create things

ONE COMPANY'S PROCESS

"We, like many other large companies, utilize a multilayered approach to determining whether an email is safe.

- A typical flow routes emails through a spam detection engine that evaluates a myriad of factors, such as sender reputation, volume of mail coming from that IP address or sender and heuristic indicators of message content. Any attachment to those emails then goes through a virus scanning tool.
- Attachments are then run through another tool that executes the attachment in a sandbox environment to determine if there are behaviors of the file that indicate it could be malicious.
- Assuming it passes those checks, the email then passes to another provider who runs similar tests. If the message and the attachment pass all these checks, then it appears in the user's inbox."

—CORY DEETER, director of cybersecurity operations and IT compliance for specialty retailer Finish Line

to facilitate the public, things like council agendas, websites to take your utility payments or to schedule park space, and things like that. We need to take extra caution, take steps to isolate them from other aspects of the network, and isolate the user interaction where the data may be stored."

NO END GAME

It's widely recognized that perfect security does not exist. There's also agreement that it's going to take enlightened vigilance, ongoing training and the continual improvements in email security software to protect both organizations and individuals.

"The attackers will always shift," warns Matthew Gardiner. "If email gets sufficiently locked down—which is imaginable, it's possible—they'll pivot to something else: IoT compromises or looking for vulnerabilities in web-deployed systems that haven't been patched…."

"The industry is bleeding from a thousand paper cuts," Erich Kron says. "The big ones make the front pages but little ones happen constantly, over and over and over again. They go unreported because there's shame—it could ruin your reputation to say you fell for a phishing attack, that you 'had a breach.' So a lot of companies won't even report that this happened. They'll just eat it and hope for the best." ■

Learn More

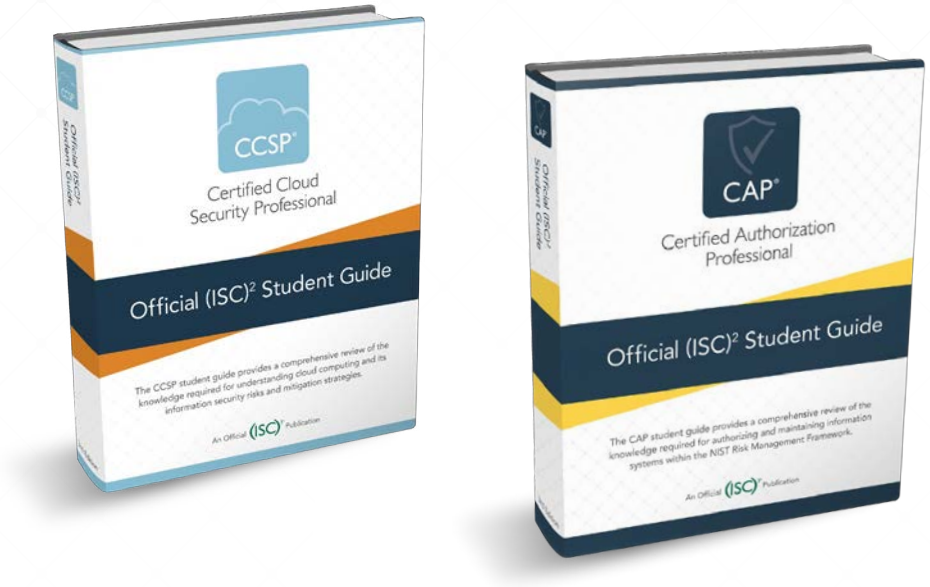
Whaling: Anatomy of An Attack
https://www.mimecast.com/resources/ebooks/dates/2016/5/whaling-anatomy-attack/

U.S. Federal Bureau of Investigation – Internet Crime Complaint Center
https://www.ic3.gov/default.aspx

DEBORAH JOHNSON *is managing editor of* InfoSecurity Professional.

YOUR TRAINERS

OUR OFFICIAL COURSEWARE



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

Don't waste your time and resources developing courseware that already exists. Use ours!

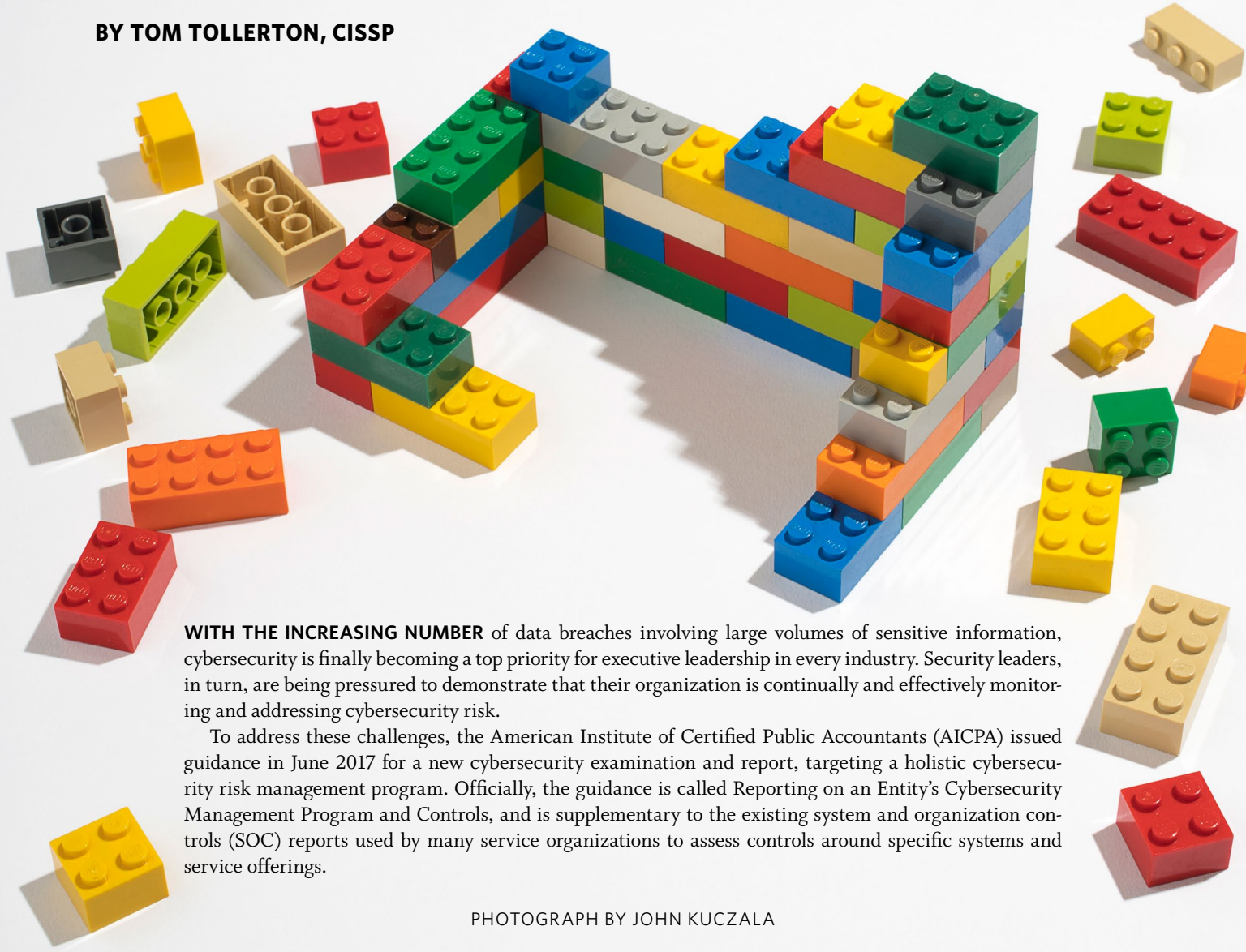
Become an **(ISC)² Official@Work training partner** and gain access to Official (ISC)² Courseware that can be used to teach your employees anytime, anywhere!

LEARN MORE

Reaching 'SOC'-cess

A new industry-agnostic framework can help build better cybersecurity governance at your organization.

BY TOM TOLLERTON, CISSP



WITH THE INCREASING NUMBER of data breaches involving large volumes of sensitive information, cybersecurity is finally becoming a top priority for executive leadership in every industry. Security leaders, in turn, are being pressured to demonstrate that their organization is continually and effectively monitoring and addressing cybersecurity risk.

To address these challenges, the American Institute of Certified Public Accountants (AICPA) issued guidance in June 2017 for a new cybersecurity examination and report, targeting a holistic cybersecurity risk management program. Officially, the guidance is called Reporting on an Entity's Cybersecurity Management Program and Controls, and is supplementary to the existing system and organization controls (SOC) reports used by many service organizations to assess controls around specific systems and service offerings.

PHOTOGRAPH BY JOHN KUCZALA

This new reporting framework allows entities to share information about the effectiveness of their cybersecurity risk management programs to appropriate stakeholders of the organization.

WHAT IS A SOC REPORT?

To better understand the nature of the SOC for cybersecurity, it is helpful to have a basic understanding of a SOC report. The AICPA describes SOC reports as "Internal control reports on the services provided by a service organization providing valuable information that users need to assess and address the risks associated with an outsourced service."

These reports are designed to give clients, partners and other stakeholders assurance around a set of controls (often related to security) applied to a particular system or service offering. Only licensed CPA firms are permitted to perform SOC examinations and issue subsequent reports. SOC 1, SOC 2 and SOC 3 reports all vary in use case and structure. More information about these reporting standards can be found on the AICPA website.

Concurrent with the release of this new guidance, the AICPA refreshed its offerings related to system and organization controls, creating a "SOC Suite of Services" that includes traditional SOC reports for service organizations, as well as the SOC for cybersecurity.

The AICPA also updated its *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy* that are used to define controls for SOC 2 reports. Currently under development is a SOC Report for Vendor Supply Chains that, when released, will focus specifically on internal controls around manufacturing processes.

WHY A NEW FRAMEWORK?

With the SOC Report for Cybersecurity, the AICPA is responding to requests for an industry-agnostic approach to examine and report on the effectiveness of cybersecurity governance within an organization. While many frameworks, standards, certifications and compliance requirements already exist in the marketplace, to date there is no industry-agnostic standard for allowing companies to share thorough, independent reporting on their cybersecurity management program. This new reporting framework allows entities to share information about the effectiveness of their cybersecurity risk management programs to appropriate stakeholders of the organization.

THE NEW SOC REPORT FOR CYBERSECURITY

Unlike previous SOC reports examining the systems and controls associated with a specific service offering, the SOC Report for Cybersecurity is designed to examine key controls across an entire business unit or organization. The existing Trust Services Criteria and Principles within the SOC 2 reporting framework are designed to allow an organization to report on the control environment relative to a particular system or service offering. The new SOC Report for Cybersecurity allows an organization to report on management of cybersecurity risk across an entire organization or business segment.

The SOC Report for Cybersecurity comprises three sets of information. The first is management's "description" of the cybersecurity risk management program. The second is management's "assertion" that the description is accurate and presented as outlined by the description criteria. The third is the "opinion" section, where the examining firm issues an opinion on the description of the design and effectiveness of cybersecurity risk management controls.

The most detailed section of the report typically is management's description. It is a narrative section that thoroughly describes how the organization addresses cybersecurity risk through identifying sensitive information assets, defining policies and processes and implementing various controls to protect data.

Reporting guidance lays out nine key categories called "description criteria" that must be addressed in management's description of the cybersecurity program. These categories are the foundation for outlining the infrastructure and processes in place to support cyber risk management.

1. Nature of the business and operations
2. Nature of information at risk
3. Cybersecurity risk management program objectives
4. Factors that have a significant effect on inherent risks related to the use of technology
5. Cybersecurity risk governance structure
6. Cybersecurity risk assessment process
7. Cybersecurity communications and quality of cybersecurity information
8. Monitoring of the cybersecurity risk management program
9. Cybersecurity control processes

Within these nine categories there are 19 "description criteria," which serve as specific control objectives within a management program.

There are additional details about the structure and

When the organization is prepared for a SOC report, an independent firm performs an examination of these controls and issues an opinion on their implementation.

content of a SOC report, as well as the process for performing a SOC examination that are outside the scope of this article. For security professionals interested in learning more about this exciting new framework, additional reading on the AICPA website is recommended. You can also contact a public accounting firm with cybersecurity professionals experienced in performing SOC reports.

WHAT DOES THIS MEAN FOR INFORMATION SECURITY PROFESSIONALS?

Security professionals are expected to understand their organization's responsibilities for managing cyber risk. As organizations seek better methods of understanding and communicating their efforts to minimize risk of a security incident, boards and senior leadership may look to this new standard as a baseline set of control objectives for evaluating cybersecurity risk management.

Organizations that complete a SOC 1 or 2 examination around a particular service offering may be pressed to demonstrate integration of cybersecurity risk management across the organization or business segment. Obtaining a SOC Report for Cybersecurity Risk Management would provide additional comfort that data security is a top priority for organizational leadership.

HOW DO I GET STARTED?

If an organization has already established a cyber risk management program, or aligned itself with an industry standard framework such as the NIST Cybersecurity Framework or ISO 27001, it likely has a head start in preparing to undergo an examination with this new framework.

Information security professionals should first assess the status of a cybersecurity risk management program within their organization through the performance of a gap assessment. The assessment should start with the nine description criteria categories (listed above) that describe the nature of the business and operation, governance, assessment and monitoring of the cyber risk management program. Consider working with a firm experienced with SOC reporting to help define and examine an appropriate control set that aligns with the description criteria.

If the initial assessment validates the implementation of controls surrounding these criteria, the description of the organization's cybersecurity risk program should be prepared. When the organization is prepared for a SOC report, an independent firm performs an examination of these controls and issues an opinion on their implementation.

If an organization has not established a cybersecurity risk management program, leadership should begin thinking about designing a program to address cyber risk.

Learn More

AICPA SOC Reporting Website
http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx

Cybersecurity Risk Management Reporting Fact Sheet
https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-fact-sheet.pdf

Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program
http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/Cybersecurity/Description-Criteria.pdf

REMEMBER TO GIVE A NEW FRAMEWORK TIME TO WORK

Cybersecurity is top of mind for financial executives and leaders of organizations across all industries. If you are responsible for cyber risk management in your organization and you have requested a SOC report from a vendor, you likely understand the value in independent assessment of internal controls around cybersecurity.

This new report aims to serve as a standard that can bridge the gap of understanding between technical and nontechnical personnel, between executives and operational management, and between cybersecurity professionals and auditors.

It may take some time for this new framework to see significant adoption in the industry. Many organizations are still trying to understand their own industry and regulatory compliance requirements. As the need for a common language that can be understood by nontechnical executives grows, this new framework from the AICPA could become an industry standard, much like existing SOC 1, 2 and 3 reports. ■

TOM TOLLERTON, *CISSP, CISA, QSA, is a senior manager in the Cybersecurity Advisory Practice at Dixon Hughes Goodman. Based in Charlotte, Tom has more than 14 years of experience in the cybersecurity field and helps manage the firm's cybersecurity audit and advisory services. Tom serves as a subject matter leader in cybersecurity risk assessments, payment card industry (PCI) compliance assessments and SOC reporting. He can be reached at tom.tollerton@dhgllp.com.*

(ISC)² Member Perks

SAVE *ON WHAT YOU DO* EVERY DAY

Exclusive to (ISC)² members! Save on over 302,000 different discounts including cybersecurity products and services.

Additional discounts include:

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

JOIN MEMBER PERKS

Include registration code **MBRPKS** when creating an account.

Save anytime, anywhere! Get the members perks app for your iPhone or Android!

Available on the App Store

ANDROID APP ON Google play

blown away by *THE NOISE*

How to manage the growth of threats and the intelligence tools to counter them.

BY VINCENT MUTONGI, CISSP

LAST SEPTEMBER, Atlanta-based consumer credit reporting company Equifax reported a breach resulting in almost half of the U.S. population (143 million Americans) being victims. The company believes the breach resulted from malicious actors exploiting an unpatched flaw in a web application tool Apache Struts being used by the Equifax web portal.

PHOTOGRAPH BY LUCIEN KNUTESON

Appearing before a Congressional panel, former Equifax CEO Richard Smith confirmed that a technician failed to install a critical patch, or perform scans afterward, that could have shown where systems might be vulnerable.

Most likely, threat intelligence tools could have helped to identify such a threat before the company was breached. That is, if someone was paying close attention to threats and alerts.

Despite the promise such intelligence solutions provide, threat intelligence tools remain ignored or underutilized. The reason: noise. When used properly, threat intelligence tools help cut through the proliferation of alerts and rank threat levels to assist with quick decision-making and incident response.

Almost 70 percent of respondents didn't act on proffered threat intelligence because they couldn't keep up with the heavy volume or complexity of alert systems.

TODAY'S CYBER THREAT INTELLIGENCE

In the security realm, cyber threat intelligence is a process that allows enterprises to gather or observe actionable network intelligence, orient themselves, decide and act on it. The process follows the mantra: observe, orient, decide and act. If organizations keep track of actionable intelligence and act on it in a timely manner, they will be in a better position to thwart most cyberattacks.

A 2017 study of more than 1,000 North American and U.K. security practitioners conducted by the Ponemon Institute showed almost 70 percent of respondents didn't act on proffered threat intelligence because they couldn't keep up with the heavy volume or complexity of alert systems.

In the Anomali-sponsored survey report "The Value of Threat Intelligence: A Study of North American and United Kingdom Companies," only 46 percent of security professionals said they used threat data to respond to suspected malicious activity, and three out of four admitted they weren't leveraging threat data as well as they could.

These results underscore something those on the front lines already know: Too often enterprises are falling victim to zero-day exploits, phishing scams, malware, espionage, insider threats, cyberterrorism, intellectual property theft, etc., because they don't (or can't) analyze actionable intelligence. Or, they spring into action too late in the game after attacks are in process or have already occurred.

A robust cyber threat intelligence strategy should identify attacks and allow security pros to block them before they happen. If well designed, cyber threat intelligence feeds and tools can give enterprises a good view into their environment and identify flaws that can be used to compromise the enterprise. This will not only provide a quick response from management, it will also provide an organized response and better allocation of security resources.

For example, if a security team is aware that their Windows servers and workstations have been missing a critical Microsoft patch for the last six months and are not testing and applying this patch, then they are playing Russian roulette. With the emergence of mobile technologies and Internet of Things (IoT) devices, criminal cartels have upped their game and will stop at nothing to get what they want—mostly stealing critical data. A recent SANS Institute study found that 93 percent of respondents are at least partially aware of the benefits of cyber threat intelligence.

BENEFITS OF CYBER THREAT INTELLIGENCE

Visibility across the network and devices

A well-designed cyber threat intelligence strategy gives enterprises clear visibility into networks and devices. This enables security pros to identify and mitigate threats in a timely fashion.

Another benefit: Insight into the capability, intent and opportunity of possible attackers.

Cyber threat intelligence helps enterprises analyze attackers' capabilities, intentions and opportunities. Knowing ahead of time the complexity of attacks and how they can be carried out gives a security team time to react and stop them. This mitigates attacks such as advanced persistent threat (APT) attacks that use spear-phishing or social engineering tricks to access the network, hide in it undetected and create a backdoor that is used to siphon critical and sensitive data out of the enterprise.

Continuous monitoring

Cyber threat intelligence allows for continuous monitoring of feeds that provide information on logs, assets, IPs and URLs that are suspicious. However, having security tools in the environment that are collecting logs is not in itself a panacea.

Enterprises should have knowledgeable and experienced in-house teams that can gather and analyze data, eliminate false positives and make sense of the threats. Integrating cyber threat intelligence into security information and event management (SIEM) provides better access to logs and data. In 2016, SANS reported that 43 percent of organizations were using SIEM systems in an integrated GUI, and another 26 percent used SIEM disparately with other tools and components.

Cyber threat intelligence reports

Most cyber threat intelligence solutions or tools have an option to generate and review reports. The tools can be configured to generate reports on daily, weekly or monthly frequencies. These reports cover emerging threats and

recommend ways organizations can stop these threats. These reports can be analyzed, summarized and shared with decision-making C-level executives.

CHALLENGES FACING THREAT INTELLIGENCE TOOLS (AND SUGGESTED SOLUTIONS)

As much as threat intelligence tools provide enormous benefits, most of them come with headaches.

White noise or false positives

Background chatter or false positives is one of the biggest challenges facing cyber threat intelligence. By nature, threat intelligence tools capture and feed logs from a myriad of appliances and SIEM solutions.

False positives are a product of misconfigured appliances, SIEMs or endpoints. Manually aggregating and analyzing these logs only to realize that a majority of them are false positives can be demoralizing to analysts. It becomes the proverbial "looking for a needle in the haystack" and leads to alert fatigue. That compels analysts to chase shadows and not pay attention to legitimate attack traffic, which could potentially lead to compromise.

Remediating false positives

First, vendors have been working to make sure that their threat intelligence tools can integrate with companies' security logs or incidents reports. These new solutions will identify attack vectors that have similarity with what is being exploited by malicious hackers. This will give analysts a clear picture of what to focus on when analyzing these particularly dangerous feeds.

Second, enterprises should provide better training to analysts so that they can understand what they are seeing and analyzing from cyber threat intelligence tools. Currently there is no clear-cut solution to the problem of false positives. This issue can only be controlled or minimized, but not eliminated.

Excessive amounts of data

Excessive amounts of data can have a negative impact on security analysts (sometimes referred to as drowning in data). When analysts are required to filter and analyze huge amounts of data, they get overwhelmed and tend to ignore serious feeds that require attention. This opens up enterprises to compromise.

Remediating excessive data logs

Fine-tuning SIEMs and network devices by installing the latest signatures will help agencies receive current and better actionable intelligence. This cuts down on data volumes and reduces unnecessary data logs, giving analysts time to analyze critical data streams.

Lack of trained analysts and inadequate user awareness training

Agencies need to employ cybersecurity professionals who can develop and integrate cyber threat intelligence tools into their environments and make sense of various cyber threat intelligence data feeds. Unfortunately, getting such skill sets has been an uphill task and agencies are struggling to get enough experts on their teams. Additionally, retaining these analysts has proved to be a herculean task. In addition, most organizations are failing to provide adequate security awareness training to their end user community. This has led to users falling victims to phishing and social engineering scams.

Remediating lack of trained analysts and inadequate end user awareness training

Providing in-house training to current security analysts and SOC teams will help improve skill sets and retain the workforce. To remediate inadequate end user awareness training, enterprises need to provide mandatory awareness training once a year. These annual training sessions should include emerging cyber threats, how to triage these threats and incident response procedures.

FUTURE OF CYBER THREAT INTELLIGENCE

While enterprises continue to adapt cyber threat intelligence, a number of cutting-edge organizations are starting to shift into a new approach called strategic threat intelligence. Results from a survey conducted by MacAfee Labs in 2015 show that despite a relatively low level of adoption, 91 percent of the 500 cybersecurity professionals—polled from a wide variety of industries across North America, Asia-Pacific and Europe—said they were interested in industry-specific cyber threat intelligence; some 54 percent said they were "very interested."

Unless, or until, more organizations embrace cyber threat intelligence, information security professionals will continue to lose whack-a-mole fights with adversaries. All told, enterprises with sustainable budgets seem to be reaping the benefits of cyber threat intelligence in detecting, preventing and mitigating today's attacks. As cyber threat intelligence matures, we expect organizations to jump onto this bandwagon, reap benefits of securing their networks, and improve their overall security posture while tackling challenges. ■

VINCENT MUTONGI, *CISSP, AWS Solutions Architect – Associate, is a Cloud Security Architect working for Business Integra Inc., a Bethesda, Md.-based information technology services company. He has more than 18 years of cybersecurity experience supporting federal government agencies in the Washington, D.C., area. He is currently providing AWS and Azure Cloud Security support to the Federal Aviation Administration, a U.S. government agency.*

FOCUSING ON EDUCATION AND RESEARCH INITIATIVES

center points

BY PAT CRAVEN

Yes, You Can Make a Difference

I DON'T HAVE TO TELL YOU that working in the cybersecurity world can often be overwhelming. You may ask yourself, "Am I really making a difference?" Or, you may think, "I'm always playing defense. For once, I would like to be on offense."

Well, I have a positive and uplifting way for you to make a difference, and it's fairly simple. Follow the lead of fellow (ISC)² members, who in their own small way are making a big difference. Let me share with you how a few super-busy members like you are making a safer cyber world—and how you can make an impact, too.

Satish Jayaprakash, CISSP, is the vice president of cybersecurity at financial giant JPMorgan Chase. Jayaprakash recognized that the Center for Cyber Safety and Education's Safe and Secure Online program was a natural extension of his company's existing Technology for Social Good program, which provides opportunities for JPMorgan Chase employees to use their technology expertise to give back to their communities.

He recognized the company's global cybersecurity staff as an untapped resource to teach online safety awareness. In less than a year, he mobilized the cybersecurity team to deliver Safe and Secure Online to students and parents in their communities. To date, JPMorgan Chase staff have taught 7,000 parents and children in the United States, EMEA and APAC how to protect themselves online. Jayaprakash has set a goal of sending 10,000 children through the popular Garfield program in 2018. That's the result of one member who took the time to find a way to do what the company was already doing, and make it even better.

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

As you know, building relationships with schools to share the program is key to helping children learn how to be safe and secure online. How about contacting your children's, grandchildren's or local school and sharing the robust Garfield program? You don't even have to give a presentation or do any public speaking. The new Educators' Kit can do that for you.

Photograph: iStock

Bryan Harte, CISSP, is the chief operating officer for RBR Technologies in Pasadena, Md. He pitched his company on the idea of "adopting" local schools and providing them all the materials to conduct—at no cost to schools—Garfield's Cyber Safety Adventures. It didn't take executives long to see the value of being a good corporate citizen. Thanks to a member thinking outside the box, 330 students at Lake Shore Elementary are now learning how to be safe and secure online.

Member outreach to schools in their communities is one of the most common ways members are making a difference. But Harte didn't stop there. His employer is also providing the new digital Garfield cartoon lessons to all its employees so they can watch at home and teach their children.

This is just a sample of how members are doing their part to build a safer cyber world for everyone. What are you going to do? There are so many ways to help that don't require a lot of time or money—just your imagination and your connections. Reach out to me or Christina Johnson at cjohnson@isc2.org for more information. ■

lead in

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

JORGE MARIO OCHOA

Jorge Mario Ochoa is an information security officer at Millicom International Cellular (Tigo). He is from Guatemala City, Guatemala. Of his 18 years in IT, the past eight have focused on information security. Among his credentials and accomplishments: CISSP; C|SISO; CISA; CISM; C)PTE; C)SWAE; Cobit v4.1 & 5; ISO 9001:2008; ITIL v3.1 & v2011; Lead Auditor ISO 27001:2013; Lead Auditor, ISO 22301:2012; Six Sigma White Belt Business Intelligence, Design Thinking.

Congratulations on winning an Americas ISLA® at Security Congress. What did it feel like the moment your name was called?

I already felt very honored to be sharing the finalist's list with outstanding professionals. When I heard my name as one of the winners, I felt very grateful to God for blessing me with a wonderful family that has supported me unconditionally, especially Karina (my wife), great friends, colleagues and co-workers who have had the good disposition to share their knowledge and experience and, of course, (ISC)² for contributing to my professional development through its certifications, conferences and publications.

You won in the project/initiative category. In what ways did you help improve the information security culture at your organization?

As part of the continuous improvement that we promote within my team, we found that most of the employees in our organization are millennials. Knowing that, we designed a program that promotes an information security culture based on gamification. We formed a multidisciplinary team with partners in talent management, internal communication and marketing. In this way, we turned a good idea into a great idea. We understood how to communicate with our people, who were engaged and enjoyed the learning journey.

Additionally, we also designed training for technical teams, to make information security a lifestyle, an automatic thought. From their conception, our projects have integrated security components. As a result, we can spend more time in the second quadrant of time, according to Stephen Covey, which is the "important but not urgent" quadrant. Therefore, we engage in more strategic thinking and spend less time putting out fires.

As an (ISC)² instructor, what do you teach and what skills did you need to develop in order to excel in that role?

In classes, I promote an atmosphere of trust, in which everyone can contribute expertise and knowledge to make a much more enriching course. It also motivates me to constantly evolve, learning new ways to connect with the audience; identifying how the class progresses by analyzing questions and answers; noting body language and even silence. Sometimes the right question provides more answers than a mere explanation. I teach that knowledge is useful only when we share it and identify how to apply it.

Communication is vital in the learning process. What's said is important, but how it is said is even more important. Tone of voice, posture, pauses, expression, energy, confidence, examples, experiences and dynamics used—these allow the student to be connected and interested in participating throughout the course.

How many hours weekly do you work?

Normally I work 40 hours, thanks to our excellent team. We spend less time communicating via email and more time in conversation in person or by phone with colleagues in different areas of our firm. By adopting this philosophy, we better understand their needs and can work as multidisciplinary teams to find the most efficient solutions.

Any advice for (ISC)² members who want to become better cybersecurity leaders in 2018?

Work even more closely with different business units to understand their needs. Communicate with them in their languages by changing bits and bytes into understandable terms specific to each business unit (return on investment, turnover rate, customer satisfaction, leads, net promoter score, etc.). It will also allow you to have a holistic vision, generate synergies. As a result, all areas will see us as a strategic partner and as an enabler. ■

@jmochoagt @jmochoagt

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

CALL FOR VOLUNTEERS

Help develop (ISC)² Exams while earning CPEs!

Throughout the year in a variety of locations, (ISC)² holds several examination development workshops, most lasting about 2.5 days.

As a volunteer, you will help create new exams or update existing exams. It's an excellent way to meet peers while also helping to prepare the next generation of information security professionals.

We are in need of the following members: CISSP, SSCP, CCSP, HCISPP, CAP, CSSLP, ISSAP.

21 CPEs

Earn up to 21 CPEs & travel expenses paid!

Volunteer Today

(ISC)²

(ISC)² SECURITY CONGRESS NORTH AMERICA 2018

CALL FOR SPEAKERS

October 8-10

New Orleans, LA • Marriott

Congress.isc2.org • #ISC2Congress

ENRICH
ENABLE
EXCEL

Benefits of speaking:

- Free All Access Pass
- Access to all Educational and Birds of a Feather Sessions
- Attendee Party Invite
- Town Hall Invite
- Exclusive Speaker Ready Room
- Access to all Keynotes
- Expo Floor
- Members earn up to 28 CPEs

Submit Now

Deadline: February 23