THE FALLACY OF FULL EMPLOYMENT

InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

SEPTEMBER/OCTOBER 2019

HOW TO NAVIGATE AN UNCERTAIN JOB HORIZON

ISSO EXCELLENCE

A lot more than being tech savvy

SUPPLY CHAIN

Demanding vendors be more secure

2019

CLOUD SECURITY REPORT

Cybersecurity INSIDERS

UNCOVER

the Latest CLOUD SECURITY Trends

Organizations are continuing to adopt cloud computing at a rapid pace to increase efficiency, scalability and agility. 93% of them reported that they are moderately to extremely concerned about security in the cloud. Find out how organizations are planning to address their concerns in the **2019 Cloud Security Report**.

Download your copy of the (ISC)² sponsored report and learn:

- The latest cloud security trends and challenges
- How organizations are responding to security threats in the cloud
- What tools and best practices cybersecurity leaders are considering in their move to the cloud

Get the Report

contents

VOLUME 12 • ISSUE 5

features

departments

Cover image: JOHN KUCZALA Illustration above: ANNA GODEASSI

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

Certification is just the Beginning

The Professional Development Institute (PDI) takes you beyond your certification with a portfolio of professional development courses and you earn valuable CPE credits.

Course Types Include:

- Immersive – In-depth training on a variety of relevant and timely cybersecurity topics delivered in an online, self-paced format.
- Lab – Hands-on courses that enable learners to practice specific technical skills.
- Express Learning – Self-paced, short-format courses with on-the-go professionals in mind.

To learn more about PDI and the growing number of courses offered, please visit: https://www.isc2.org/Development

You can enroll and take the courses for FREE by logging in to enroll.isc2.org using your member credentials and selecting "My Courses." Courses also available for purchase by non-members.

Access Free Courses

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

The Fallacy of Full Employment

A RUN OF GLOBAL ECONOMIC PROSPERITY, combined with a worldwide shortage of highly qualified cybersecurity professionals, has led many of you to think it's easy to find and keep a good-paying job.

Don't believe it.

You can be the best at what you do, only to walk out one day shell-shocked from a sudden sack. You can spend months submitting resumes and attending interviews, only to continually come up short. You can eventually give up and go into business for yourself, only to find clients hard to come by.

It may be you, or it may be forces outside of your control. A company may dissolve due to mismanagement or market shifts. A cooling in consumer or B2B spending could lead to layoffs. A government agency facing budget shortfalls may contract.

During an economic recession, all of these things happen. There is more competition for fewer jobs—jobs perhaps located in other, less desirable regions or industries. There also is a growing influx of new cybersecurity professionals entering the workforce through higher education or nontraditional career paths. They are eager, energetic and less expensive to hire.

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

That's why I urge everyone to absorb the advice in this issue's cover story by Deborah Johnson. (The other features by (ISC)² members on ISSOs and supply chain security also are well worth a read.)

You need to pay attention to what is happening around you, from leading economic indicators to internal sales updates. You need to network, both online and in person, so people are familiar with you and your work. You need to continually boost your skills and readily quantify your value to an organization. And, you need to stop thinking you can't ever end up unemployed.

Do all of these things as if your livelihood depends on them. Because, one day, it probably will. ■

ADVERTISER INDEX

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

InfoSecurity PROFESSIONAL

(ISC)² MANAGEMENT TEAM

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

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

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

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

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

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

EDITORIAL ADVISORY BOARD

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

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

RETURN TO CONTENTS

(ISC)²

2019 SECURITY CONGRESS

OCT. 28-30 | Orlando, Florida

CATCH OUR WORLD-RENOWNED KEYNOTE SPEAKER LINEUP

Captain "Sully" Sullenberger

William H. McRaven

Catherine Price

Erik Wahl

From pre-conference trainings to deep-dive workshops and networking with cybersecurity professionals from around the world, this year's Security Congress is taking learning to the next level.

And Don't Miss Out on:

- 200+ Speakers, 175+ Educational Sessions, 18 Tracks and 5 Keynotes
- 16th Annual Information Security Leadership Awards (ISLA) - Americas
- Geeks vs. Nerds Comedy Throwdown *(separate ticket required)*
- (ISC)² Networking Night at House of Blues
- Discount Disney Tickets
  Visit Hotel & Travel on congress.isc2.org to learn more.

$50 OFF

Your All Access Pass with code:
SECPROF19

REGISTER NOW

EARN UP TO **46 CPEs!**

congress.isc2.org #ISC2Congress

How Culture Makes Us Safer

by Wesley Simpson, COO

THERE'S AN UNTAPPED RESOURCE hiding in security departments that many of us may consider an intangible or even undefinable asset. When strengthened, it can have a drastic effect on an organization's security and contribute to its overall value stream. I'm talking about building a strong culture within your cybersecurity team.

There are some very tangible practices you can deploy within your team that can have a huge impact on engagement and satisfaction and make your business more secure at the same time.

One way to do this might be to create a monthly newsletter with some key stats about the number of vulnerabilities discovered, phishing attacks blocked, systems installed or whatever your key metrics are. How many of us actually catalog these achievements throughout the year? Would your teams' confidence and pride grow at all if they saw the cumulative results of their efforts showcased across the company?

And what about extending this to the rest of your organization? Create a leaderboard for all of those correctly-identified phishing emails that your users send you. A competition with monthly or even quarterly winners and associated prizes can help increase user engagement and underscore the importance of everyone within your organization being responsible for cybersecurity—not just your security team.

Wesley Simpson is COO of (ISC)². He can be reached at wsimpson@isc2.org.

Get involved in the cybersecurity community outside of your organization. Our Center for Cyber Safety and Education, for example, is always looking for professionals with your experience to help them deliver lessons to students. Mentorships and internships are also great ways to get involved and shape the next generation of cybersecurity professionals.

Of course, assembling the right team is the No. 1 way to ensure a stable and positive work environment, and that comes down to creating an understanding between IT hiring managers and the human resources team about what they're actually looking for. Many organizations may struggle to find qualified candidates based on narrow definitions or job descriptions that only apply to "unicorns."

Look for the right mix of qualifications, core values and soft skills that blend with your existing team.

That's why it's important to understand your needs and search for the right talent, even if they are nontraditional hires. Look for the right mix of qualifications, core values and soft skills that blend with your existing team.

Does the candidate have values that align with the team's? Are they able to communicate effectively in all directions? Have they demonstrated they can work well within a group dynamic? Can they lead projects if needed? There may even be influential employees who are already within the organization and looking for a change or a new challenge. Would a person on the IT, legal or customer services teams be a good addition to the security team? Clear communication between hiring managers and HR is essential to uncovering the true needs of the team and making sure that the right hires are made.

With the rabid competition for qualified candidates, culture may be a differentiator that helps an organization avoid breaking the bank for talent. By making cybersecurity fun through initiatives like gamification, tabletop or war games, and guest speakers during staff meetings, your organization may be able to attract, retain and even grow your own security team and make your organization more secure in the process. ■

CSA Summit

at (ISC)² Security Congress 2019

Future-Proofing Tomorrow's Cloud

The cloud landscape has become more complex causing organizations to address the security needs for tomorrow's environments. As technologies rapidly evolve for cloud, we must learn to securely manage the data sprawl that ranges across these emerging technologies and multi- cloud usage. Learn about the technology trends that are impacting how we connect to new resources and better understand how to adapt new methodologies for secure agile development and processing of data. Get ahead of standards development by implementing tomorrow's best practices and best known methods for security.

The year 2019 marks the ten-year anniversary of Cloud Security Alliance. From inception, the CSA has been dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment throughout the world.

In its third year at the (ISC)² Security Congress, the CSA Summit will reflect on the lessons learned by enterprises and providers as cloud has become the dominant IT system in the market. We will also explore new frontiers that are accelerating change in information security, such as artificial intelligence, blockchain and IoT.

SUNDAY, OCTOBER 27TH
ORLANDO, FLORIDA

VISIT US AT
BOOTH #110

2019 (ISC)² Security Congress

October 28-30 – Orlando, Florida

Here's a preview of what's happening at this year's conference.

THE KEYNOTES

This year's keynote speakers are sure to engage attendees with their insights, creativity and, in one unique example, a moment of courage.

Monday, Oct. 28, 8:30 a.m.-9:30 a.m.

Captain "Sully" Sullenberger III

It was the "Miracle on the Hudson," when in 2009, Capt. "Sully" Sullenberger safely landed his distressed jetliner in the middle of New York's Hudson River, saving all 155 passengers. Capt. Sullenberger, a passionate advocate for airline safety, will share not only the heroic story, but how his training and leadership led him to that moment.

Tuesday, Oct. 29, 9 a.m.-10 a.m.

Catherine Price – Author, *How to Break Up with Your Phone*

An award-winning science journalist, Catherine Price advocates what she calls a "screen/life" balance. Her work has appeared in newspapers and magazines including *The Washington Post, Men's Journal, Popular Science* and *O: The Oprah Magazine*. Price's latest book, *How to Break Up with Your Phone,* is being published in 26 countries and translated into 18 languages.

Tuesday, Oct. 29, Noon-1 p.m.

Erik Wahl – Author, *The Spark and the Grind*

Erik Wahl's artistry, combined with his ideas about creativity, have excited audiences around the country. His latest book, *The Spark and the Grind,* reveals what it takes to get from an idea to the action of creating. Wahl consults as a business strategist for many major corporations, including Disney, Microsoft and FedEx. He also is a philanthropist, raising millions of dollars for charity through the sale of his unique artwork.

Wednesday, Oct. 30, 5:30 p.m.-6:30 p.m.

Admiral William H. McRaven, USN (Ret.)

William H. McRaven, a retired U.S. Navy four-star admiral, is also a former SEAL and was the commander of the operation that killed Osama bin Laden. He brings insight into today's geopolitical environment, as well as the personal determination to succeed through his experiences. Adm. McRaven is a former chancellor of the University of Texas system and a best-selling author whose latest book is *Sea Stories: My Life in Special Operations.*

NETWORKING OPPORTUNITIES ABOUND

The (ISC)² Security Congress presents a unique opportunity to meet your cybersecurity peers, exchange ideas and see what is happening from colleagues all over the world.

Here's a sampling of the networking events throughout the week. Note: Be sure to sign up for these events when you register here.

Sunday, Oct. 27, 5:30 p.m.-6:30 p.m.

New Member and First-Time Attendee Reception

Location: Southern II-III

This wine and cheese reception will give you a preconference opportunity to meet other attendees. Be sure to bring extra business cards for a special networking activity.

Monday, Oct. 28, 1:30 p.m.-3 p.m.

Town Hall

Location: Pacific Hall/Atlantic C

Members of (ISC)² management and the Board of Directors will be on hand to answer any questions that you may have regarding membership, certifications, the cybersecurity industry and more. The meeting is open to both members and nonmembers.

Submit a question for the panel at the (ISC)² Town Hall at congress@isc2.org.

It's Not Too Late to Register

You've seen some of the great events, and there's even more going on in the presentations and panels. To see what else is on tap, click here to check out the schedule.

Click here to sign up now.

View the details on travel and the hotel here.

Monday, Oct. 28, 9:30 a.m.-5 p.m., and Tuesday, Oct. 29, 10 a.m.-5 p.m.

Career Center

Location: Americas Seminar

Evaluate your career path and bring your resume for expert advice. Schedule a free career coaching and resume review session.

Tuesday, Oct. 29, 8 a.m.-8:50 a.m.

Making Cybersecurity Personal (formerly "Safe and Secure Online Program Orientation")

Session by the Center for Cyber Safety and Education

Location: Pacific Hall/Atlantic C

The place to learn all about the new Safe and Secure Online program, including how to bring Garfield to your local school and how to volunteer to educate members of your community. You'll earn 1 CPE for attending.

Tuesday, Oct. 29, 6:30 p.m.-9:30 p.m.

Geeks vs. Nerds Comedy Throwdown

Location: Northern Hemisphere D-DE Corridor

Engineer-turned-professional-comedian Don McMillan will leave you on the floor laughing as he explores the difference between a geek and a nerd and other real-life workplace situations. Guests are encouraged to dress in their favorite geek chic or nerd attire. Munch on classic comedy club fare. Geeks vs. Nerds Comedy Throwdown proceeds help fund cyber safety programs for children, parents and seniors around the world.

General Admission Ticket: $125

Includes classic comedy club food fare and two beer/wine tickets. General seating, with doors opening at 6:30 p.m. VIP tickets also available for $200. Space is limited.

GET YOUR WALKING/RUNNING SHOES ON!

Tuesday, Oct. 29, 6 a.m.-7:15 a.m.

(ISC)² Congress 5K Fun Run/Walk

Starting line location: Boardwalk, Clamshell Fountain

Get a jump-start on the day with the first-ever (ISC)² 5K Fun Run/Walk. Enjoy the great scenery and work out with colleagues. There will be water stations along the route and participants will get a goodie bag with some great swag, including a race T-shirt.

Sign up during registration. Entrance fee is $35 and event is limited to 300 participants.

Cybersecurity Awareness Takes Center Stage

October focus on security education

October provides a golden opportunity to spread the word about cybersecurity. It's National Cybersecurity Awareness month.

Beatriz Parres, community engagement coordinator for the Center for Cyber Safety and Education, offers some suggestions, particularly for those attending Security Congress during October.

Congress participants have some unique opportunities to get involved:

- Attend the Geeks vs. Nerds Comedy Throwdown on October 29 for a night of fun and laughter to raise awareness and funds for cyber safety education. Just add it to your registration ticket.
- Show your love for Garfield by sponsoring a class for Cyber Safety Day Orlando on October 30 and changing the lives of 30 children. For details, click here.

At home, and year-round, there are many other ways to promote online safety:

- Support cyber safety education without moving from your couch. Visit iamcybersafe.org/giving to change the life of one child for as little as $2.17.
- Feed your social media addiction by liking the Center for Cyber Safety and Education on Facebook, Twitter, Instagram, YouTube and LinkedIn and posting a comment about how awesome we are!
- Take the message to your community by offering free Safe and Secure Online presentations in multiple languages (resources at iamcybersafe.org/volunteers).

(ISC)² 2019 ISLA Government Winners

USPS, Carnegie Mellon University and U.S. DHHS among the lauded

The Information Security Leadership Awards in Government recognize the ongoing commitment of individuals whose initiatives, processes and projects have led to significant improvements in the security posture of a United States government department or agency.

"Innovating in the government space can be a challenge for even the most skilled professional, with policies, regulations and budget constraints playing a role in day-to-day operations," said Wes Simpson, chief operating officer, (ISC)². "We look forward to celebrating these leaders and their teams, as we honor their achievements over the past year."

The 2019 winners were selected by a panel of judges based on nominations by their peers.

The 2019 ISLA Government judges:

- Benjamin Bergersen, CISSP-ISSAP, ISSMP
- David Branscome, CISSP, CCSP
- Dr. Michaela Iorga
- Derek Smith
- Michael Stoner, CISSP

Winners will be honored at the ISLA Americas ceremony during the 2019 (ISC)² Security Congress on Wednesday, October 30 at the Walt Disney Swan and Dolphin Resort in Orlando. This year's awards ceremony will also include the presentation of the first-ever (ISC)² Diversity Award. This award will be presented to a professional who has significantly impacted the advancement of diversity in the field of cybersecurity through activities such as scholarships, advocacy, nonprofit work or other means to create a level playing field for the inclusion of all individuals in the world of cybersecurity.

For more information about (ISC)² awards, please visit http://www.isc2.org/About/Award-Programs.

This year's winners are:

WORKFORCE IMPROVEMENT

Lisa Carol Holman
Deputy Chief Information Security Officer, Corporate Information Security Office, United States Postal Service

UP-AND-COMING INFORMATION SECURITY PROFESSIONAL

Stephen Czerwinski
IT Security and Server Specialist, Public Service Commission of Wisconsin

TECHNOLOGY IMPROVEMENT

William Birchett, CISSP
Owner/vCISO, Logo Systems

MOST VALUABLE INDUSTRY PARTNER (MVIP)—TEAM

Dr. Thomas P. Scanlon, CISSP
Senior Cybersecurity Engineer & Researcher, Software Engineering Institute, Carnegie Mellon University

Additional team members include: Dr. William Nichols, Dr. Carol Woody, Dr. Kenneth Nidiffer and Timothy Chick, CSSLP

COMMUNITY AWARENESS—TEAM

Julie Chua, CISSP, CAP
Risk Management Branch Chief, Office of Information Security, U.S. Department of Health and Human Services

Additional team members include: Erik Decker, Christopher Bollerer, Steve Curren, Nickol Todd, Laura Wolf, Emery Csulak, Nick Heesters, Suzanne Schwartz, Aftin Ross, Seth Carmody, Rose-Marie Nsahlai, Matt Quinn, Matthew Barrett, Nick Rodriguez, Justin Smith, Konrad Miles, Paige Burke, Elizabeth Voeller and Brian Lebeck

> "Innovating in the government space can be a challenge for even the most skilled professional, with policies, regulations and budget constraints playing a role in day-to-day operations."
>
> —Wesley Simpson, chief operating officer, (ISC)²

RECOMMENDED READING

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

Listening In: Cybersecurity in an Insecure Age

By Susan Landau
(Yale University Press, 2017)

A **BATTLE IS UNDERWAY** pitting an individual's desire for online privacy and a government's need to maintain national security. In *Listening In: Cybersecurity in an Insecure Age*, author Susan Landau dives into the fray. Landau is an encryption and surveillance expert, a former analyst for Google and Sun Microsystems and now teaches cybersecurity at Tufts University.

One of the significant issues Landau tackles is government access to an individual's mobile phone. Landau cites the case of the FBI vs Apple following the 2015 deadly terrorist attack in San Bernardino, Calif., with the FBI arguing on behalf of national security and Apple on the right of privacy. Apple refused to provide a backdoor into the phone. The case was dropped after FBI technicians were able to open the phone.

> The bottom line is that the government's role is to ensure security and privacy for its citizens. And what role do we as security professionals play?

Other issues Landau probes include the often-lengthy response time on the part of governments to cybersecurity incidents, and why state-sponsored forays into our networks continue seemingly unabated. Landau advocates increased awareness on the public's part of security and privacy risks. She also endorses the latest efforts in government security and surveillance efforts to protect the public and understand the challenge of both coexisting.

The bottom line is that the government's role is to ensure security and privacy for its citizens. And what role do we as security professionals play? Some specific answers to these to understand the trade-offs between security and privacy questions are included in this thought-provoking book. ■

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

BLIND CONSENT

71%

Percentage of internet users who never or rarely read Terms of Service

Source: Brookings Institution
(2,000 respondents)

GOING UNREPORTED

15%

U.S. cybercrime victims who report crimes to law enforcement

28%

U.K. cybercrime victims who report crimes to law enforcement

Source: CSO Online

READ. QUIZ. EARN.

Earn Two CPEs for Reading This Issue

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

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

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&ACTION=SI&-CatRedirect=10825%7C10825

(ISC)² NEW JERSEY CHAPTER

(ISC)² New Jersey Chapter Conference Takes Aim at Online Scamming

A RANSOMWARE ATTACK against a member of the (ISC)² New Jersey Chapter stoked Chapter President Niloufer Tamboly's interest in taking on the issue of social engineering.

"Our member was on a business trip when his wife told him that their home computer had a message asking for Bitcoins. All his kids' pictures were on the computer and he told me that he had never thought that he would ever consider paying to recover his files. But as he was away for the week, he felt he had no option but to pay. His wife was tricked via email into infecting her computer.

"He asked me what we were doing as a community to ensure that our friends and neighbors knew how to protect themselves. I told him that we had our quarterly chapter meeting in October 2016 focused on social engineering. But I knew that we needed to do more."

That, and the rising concerns about phishing, malware, ransomware and other social engineering scams, led to the Social Engineering Awareness Conference, or SECON 2019, a daylong event planned in conjunction with several other cybersecurity professional groups in New Jersey and with support and involvement from high-level sponsors.

Speakers from across the cybersecurity spectrum shared their expertise to a sold-out audience of 250, including representatives of local companies, technical officers from area schools and colleges, and members of the New Jersey prosecutor's and auditor's offices.

Conference highlights were frontline experiences, Tamboly reports. Daniel Maloney, Verizon's deputy CFO, spoke about the evolution of security functions over the years and the fine balance required to manage insider threats. Edward Amoroso, founder and CEO of TAG Cyber, used humor to convey the need for formal cybersecurity training for compliance with security policy and avoiding phishing risks.

(ISC)² NEW JERSEY CHAPTER

Contact: Niloufer Tamboly

Email: president@isc2chapternj.org

Website: https://isc2chapternj.org/

Above: CISO panel, from left to right, Michael Chirico, ISO, New Bridge Medical Center; Steven Santamorena, CISO, Metropolitan Museum of Art; Tony Chang, senior manager, ITOCHU International; Ken Fishkin, director, CohnReznick LLP.

Left: Keynoter Daniel Maloney, deputy CSO, Verizon.

Jayson E. Street, Phil Caturegli and Adriel T. Desautels, authorities on social engineering, enthralled the audience with their presentation. And hands-on presentations throughout the day included a demonstration by the Netragard team showing ways to hack RFID readers, route WiFi traffic and deploy hidden recording devices used by social engineers.

The chapter received positive feedback from attendees, including:

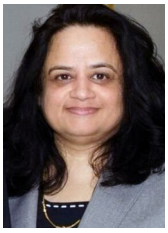
- "The knowledge that I gained from this event was applicable and will immediately help me improve the security program in my company."
- "Thank you for organizing this conference! I really enjoyed it and got a chance to listen to industry experts on how to manage social engineering."
- "Great training!!!"

Overall, Tamboly says, SECON was a success for sponsors and attendees. "They liked the 30 minutes allocated to speakers, which meant we could accommodate more speakers. Something we need improvement on is 'ran out of roast beef sandwiches.'" ■

Q&A

Niloufer Tamboly, CISSP

President, (ISC)² New Jersey Chapter



Tell us about your professional background and your experience with the (ISC)² New Jersey Chapter.

As a risk management professional, I work with companies helping them launch profitable products and services by managing technology and business risks. I hold multiple certifications in IT security (CISSP), audit (CISA, CIA) and fraud (CFE) and am a certified public accountant licensed to practice in the state of New Jersey.

I hold two patents from the U.S. Patent Office for a system for and method of generating visual passwords (US 9,171,143 B2) and for establishing an alternate call path using short-range wireless technology (US 9,392,523).

My friend Gurdeep Kaur, CISO, PSEG, and I cofounded one of the first (ISC)² chapters in the world! I could not attend infosec meetings held in New York City because I had young children at the time. Searching for a local meetup of cybersecurity professionals, Gurdeep and I found out that (ISC)² was accepting applications for local chapters. We reached out to Jayda Shriver, who was in charge of chapter formation. We started the process in 2011 and were granted the official charter in May 2012.

How did you structure the planning for the SECON 2019 with the chapter members?

I partnered with leaders from ISSA and ISACA New Jersey chapters to create an agile core team consisting of two members from each chapter. I had to take nine vacation days to coordinate with our volunteers, speakers and supporters. Volunteers from all three chapters contributed their time generously. Jose Lagdameo, a director of the (ISC)² New Jersey Chapter, ensured that everything went smoothly on the day of SECON 2019.

You were able to recruit many high-level security professionals to speak and gain great sponsors. What were the challenges and what advice would you offer to other chapters planning such a conference?

A few members of our core team like Vimalanathan Subramanian, Ken Fishkin, Mizba Tawa and I used our connections to recruit speakers for SECON 2019. Many of our speakers flew in at their own expense to speak and interact with our attendees throughout the day. It is a humbling experience, and I can't thank all our speakers enough.

For SECON 2019 we had to turn down a lot of vendors who wanted to work with us because, at the outset, our team had decided that we would only accept support from vendors that met our criteria. Our supporters made it possible for us to educate, connect and inspire cybersecurity professionals, academics and students who attended SECON 2019.

My advice to chapter leaders planning conferences is to ensure your members support your efforts. Our members, without whom SECON 2019 would not be a success, are passionate and joined our movement to spread social engineering awareness. Be very selective with vendors who want to sponsor or support your cause.

What was your lesson learned from this conference?

SECON 2019 made me appreciate the importance of marketing in the success of an event. We sold out tickets and could choose sponsors we wanted to work with, without spending any money on paid advertisements because of a thorough and detailed marketing plan. ■

> **"Hackers look for organizations and businesses that seem more vulnerable than others. The ones that have neglected to set basic security standards are more likely to be targeted for ransomware attacks. The process is very similar to burglaries in which the criminals do not target a specific home, but rather cruise neighborhoods to find houses that do not seem to have security systems."**
>
> *—Niam Yaraghi, Brookings Institution, Nonresident Fellow – Governance Studies, Center for Technology Innovation*

(ISC)² MEMBER PERKS

NOW IN LATIN AMERICA!

SAVE *ON WHAT YOU DO* EVERY DAY

Exclusive to (ISC)² members in Latin America! Save on thousands of discounts in products and services all over the region.

Additional discounts include:

- Hotels
- Movie tickets
- Concerts and events
- Pharmacies
- Restaurants
- Spa and massage venues
- Car rentals
- Education
- Local florists
- Technology
- Gym and fitness studios

NOW IN LATIN AMERICA!

JOIN MEMBER PERKS

Create your account using the unique code you received by e-mail.
Contact membersupportlatam@isc2.org for additional support.

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

Available on the App Store

ANDROID APP ON Google play

Are You That Voice?

by John McCumber

JUST ABOUT A DECADE AGO, the U.S. Congress enacted legislation that likely had the biggest positive impact on my life. Tax relief? No. Free snacks in every federal building? Not that, either. They passed the Do Not Call list with associated fines for violators. Almost immediately, the robocalls and offers of credit card relief stopped. It worked—for several years—until it didn't. Of course, now we are all forced to only answer our mobile phones when we see a known caller, and trust other legitimate callers know to leave a voicemail. Many of us now rely heavily on texting.

I was pondering this as I returned from another series of meetings on Capitol Hill, speaking with legislators and staffers. It is always eye-opening to learn what our representatives and their support teams think of cybersecurity issues impacting Americans. This time around, "Congresscritters" are looking to revive the Advanced Cyber Defense Certainty Act, also known as the "hack back" legislation. I am dumbfounded why you would want to enact legislation that would encourage private companies to perform the tricky technological gymnastics required for cyber attribution, then retaliate against perceived culprits—especially if it were a suspected nation-state actor. Yet here we are.

But what are the real national problems in cybersecurity? As I write this, several U.S. cities and towns have been faced with ransomware attacks. The malfeasant attackers will often work with an insurer to extort a large payment in Bitcoin. Ultimately, the taxpayers are going to be stuck with the bill, and this new type of successful extortion will only encourage similar attacks.

We have also entered a completely new era where global technology companies are toying with different forms of censorship, and nations are using technology to spy on their citizens. Technology is being used by miscreants to stalk and harass others.

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

Image: iStock

Social platforms are being leveraged to dox and expose users who wish to remain anonymous. Mob tactics are employed to railroad and attack people for their opinions, some losing their employment in the process. This is just a glimpse at some of the new and emerging threats our profession has an obligation to help fight.

The time to speak up is now. Cybersecurity professionals need to lend their voices to the public debate on the critical issues of our time. In addition, we all need to recognize cybersecurity is no longer the sole purview of those who have "security" in their job title. Anyone who recommends, acquires, deploys, manages or even simply uses these technologies has a cybersecurity role to play. Whether it's just your own personal data, or terabytes of sensitive information on citizens, we all have to apply sound security practices to ensure the confidentiality, integrity and availability of these critical assets.

Please take a moment to look around and see where you can help. These are not technical problems. These are social, moral and ethical dilemmas that must be confronted by this generation. One more voice of reason may be what is needed. Are you that voice? ■

HOW TO NAVIGATE AN UNCERTAIN JOB HORIZON

Advice on how to mitigate a sudden job loss due to redundancy, recession or 'rightsizing'

BY DEBORAH JOHNSON

DIANA CONTESTI WAS A BUSINESS CONTINUITY PLANNER at a major steel manufacturer in Hamilton, Ontario, when a recession hit the Canadian steel industry in the early 1990s. The economic contraction forced companies to cut jobs.

Her employer called it "rightsizing" when leadership announced it would cut approximately 3,000 positions. The layoffs were based on seniority by department, and based on that criterion, Contesti knew she was out.

"I was extremely worried. I'm a single mother and all those fears, 'Oh, my God! How am I going to feed my kid?' kicked in."

For years now, a growing global cybersecurity workforce shortage and robust economies have left information security professionals with a strong sense of job security. Still, companies merge, an industry contracts, an organization realigns its focus. That's when your job may be in jeopardy and, depending on where you live or work, a comparable position elsewhere may be difficult to come by.

If you were to find yourself "downsized," "rightsized," "redundant" or any other euphemism for being forced out, would you be prepared?

IMAGE BY JOHN KUCZALA

In Contesti's case, after her initial panic, the CISSP says she "took a step back and said, 'I have two degrees. I have skills.'" Those skills came into play. An opportunity arose when the same company decided to create a centralized information security system. "I understood risk and risk management. I was fortunate that I had some skills that led me into the position," she says.

'I FIGURED SOMETHING WAS UP'

Another (ISC)^2 member with experience surviving a downsize is Glenn Leifheit, CISSP.

Leifheit was a member of the internet architecture team at his company when he began observing layoffs throughout the organization. Despite three years in his role, the job cuts left him unsettled. "There's kind of that pit in your stomach as to what the hell's going on," he recalls.

It quickly became clear that his team was being disbanded. "I was nervous. I was frustrated."

Throughout his tenure, Leifheit had developed additional skills, as well as strong relationships. "I had a little birdie chirp in my ear" that there were opportunities ahead. After a very short interview with the CISO, Leifheit got the new job before he officially lost the one he had.

"Yes, my technical skills played a big part in it, but it was the fact that I had the people skills to work through a seven-minute interview [and] was able to adjust to the adversity that was going on behind the scenes."

Based in the Seattle area, Leifheit is now a senior security program manager for Microsoft's Customer Security and Trust team.

ADVICE FROM THOSE WHO'VE BEEN THERE

"Take on the additional challenges you may have. Work on something new. Add value to the group, to the company."

—Glenn Leifheit

"Always look at what your next career is going to be. Just because you're doing something well, and doing it well for many years, it doesn't mean that's where you're going to wind up. Keep your options open!"

—Diana Contesti

"We used to say, 'I don't play politics, I just do my job.' Fine. But the other person has the savvy and is going to get the next job, and you just may be out of a job."

—Joan Tabb

'I THOUGHT GREAT WORK WOULD BE REWARDED'

"It was like I was stabbed," recalls executive and career coach Joan Tabb when she lost her job as a marketing executive for a major Silicon Valley computer networking corporation in the early 1990s. By then, she had many successes that she believed would inoculate her from a layoff.

"I was ranked No. 1 in marketing in this huge corporation I was in, so I thought I was sitting pretty." Little did she realize that when her company merged with another computer networking organization, her job was at risk. "So when I was taken into that little room and told my job was eliminated, I was shocked."

Political savvy "to see how the winds are blowing" is crucial, Tabb says. "I have to say, as smart as I was, I did not have political savvy."

Now an author, blogger and career coach in the San Francisco Bay Area, Tabb helps others advance or change their careers.

THE 'R' WORD

Since the global economic downturn in 2008, the tech sector has grown steadily as innovations in data storage, security and applications have flourished. "The companies that … came out of it relatively unscathed were a lot of the software companies that were offering cloud and software as a service (SaaS) subscriptions," says John Freeman, vice president of Equity Research at the Center for Financial Research & Analysis (CFRA), a global investment research company.

The U.S. Bureau of Labor Statistics estimates that employment of computer and information technology occupations will grow 13% from 2016 to 2026, faster than the

SO YOU WANT TO BE A CONSULTANT?

5 MUST-HAVES BEFORE YOU STRIKE OUT ON YOUR OWN

You've been downsized, "rightsized," squeezed out. Okay, you say. I'll just be a consultant. Not so fast, warns consultant Ted Demopoulos *(left)*, an author, speaker and SANS instructor who's been an independent consultant for 25 of his 30 years in information security.

"A consultant is not an unemployed person looking for any kind of work," he says. "It takes somebody that's motivated and a self-starter."

Demopoulos says there are some key items to understand, and prepare for, before you hang out your shingle.

1. You need clients.

"Often, the easiest client to get is one that you've worked with before." But, admonishes Demopoulos, you need to reach out. "Are you in touch with them? Are you connected with LinkedIn?" Use your past relationship, he advises. "Maybe you worked together well. Just send them a message, say, 'Hey, remember when we did this? It was great working with you.'"

2. You need more clients.

"A lot of consultants work relatively well based on existing contacts. But very often, after three or five years, the consultant is out of contacts as clients." People move on to other work or they retire. "What a consultant has to do is, even when they're really busy, work on getting new clients." And the best way to do that? "Regularly do something to raise your visibility in a positive way … ideally by giving back to the community … speaking at conferences or just reaching out and helping people."

3. You're running a business.

Things like invoicing clients, understanding your cash flow, setting up a bank account, filing the appropriate government forms: "These are 'little' things about running a business that none of us typically think about."

4. Recovering from a failure.

"It's going to happen whether it's your fault or not," warns Demopoulos. "You simply accept responsibility. To avoid it, he recommends spelling out the details in writing. "What I always like to do in any consulting engagement is have a definition of what success looks like with the client … here's what we're trying to achieve." Whether it's a formal statement of work or an email, have clear communications and document it. "This is both for the client and for you."

5. Be prepared.

There's a lot of prep work required before you go out on your own. And, have contingencies for times when business slows and to handle increased workloads when times are great.

—Ted Demopoulos

average for all occupations, adding about 557,100 new jobs. The sectors hiring the most: cloud computing, the collection and storage of big data, and information security.

Several nations, including the United States and Australia, have experienced long stretches of economic growth in recent years (almost three decades for Australia). This has many wondering when the next recession will come, and how severe it may be. The National Association for Business Economics released a survey earlier this year in which 77% of the 281 respondents "expect an economic recession by the end of 2021."

But an economic downturn can happen quickly, and sooner, based on geopolitical events or market jolts, such as the collapse of the U.S. housing market that set off a global

GAP IN CYBERSECURITY PROFESSIONALS BY REGION

According to the (ISC)² 2018 Cybersecurity Workforce Study, these areas have the largest talent shortages:

Global	2,930,000
Asia-Pacific	2,140,000
North America	498,000
Europe, The Middle East, Africa	142,000
Latin America	136,000

financial meltdown in the previous decade.

The technology sector can weather a potential economic storm, according to a published report by economists at the BCG Henderson Institute in the April 2019 *Harvard Business Review*. "Technological progress will not stop during a downturn; neither, therefore, can companies afford to put their digital change agendas on hold."

But as we've seen, businesses can refocus priorities, companies can be bought or sold. Any of these changes can eliminate jobs. Here is some expert advice on how to hold on to employment during economic upheaval.

1. Be Prepared and Don't Panic

"You should always be ready for something to happen," warns consultant Ted Demopoulos. "Often, we're blindsided by downturns, whether it's in the economy or our employer."

Demopoulos is an information security veteran with 30 years of experience and says every professional should maintain an updated resume and/or CV and LinkedIn profile.

The way to stay at the top of your game is to be both technical and strategic, advises Deidre Diamond, founder and CEO of CyberSN, the cybersecurity job network. "People who are both technically hands-on and also possess leadership qualities and problem-solving skills are the 'purple unicorns.'"

And start planning now how you'll earn those skills, she adds. "Don't just wait for something to happen."

Despite her initial shock and fear, Diana Contesti says she didn't freeze. "Was I angry? Yes, I was angry for a day or two. But you have to shake it off and move on."

Even though her company was downsizing, she had the skills to fill the newly created security position. "I was in the right place at the right time."

2. Network (Yes, It's Who You Know...)

Don't expect your skills and technical prowess to speak for themselves. You need to get in front of people to be noticed now. "The majority of people find jobs by networking," Diamond says.

"Most [jobs] come from personal contacts or contacts of contacts," Demopoulos concurs.

Staying connected takes constant effort, admits Tabb. "You've got to keep your network working by attending professional associations, keeping up with colleagues, people you used to work with, managers you used to have, people who know you do good work."

"But I'm not a people person," is a common refrain. "Reach out and engage with people," Demopoulos says. "They may love you, but if they haven't heard from you in a year … you're not top of mind."

Glenn Leifheit's "little birdie" was a former manager from a previous company, someone he said he'd "be happy to work with again." In addition, Leifheit took steps to ensure he was comfortable talking to anyone at any level. He joined Toastmasters, the international organization that promotes "effective communication."

"The decision was life-changing," he says. "I feel that the trajectory of my career drastically changed."

3. Know Which Way the Wind Is Blowing

Political savvy is absolutely crucial, according to Tabb. Yes, you need to be excellent in your position, but there's more.

HIGHEST PAYING CYBERSECURITY POSITIONS

Position	*Salary Range, USD*
Manager, Information Security	$120,000 - $185,500
Application Security Engineer	$120,000 - $182,500
Network Security Engineer	$115,000 - $172,500
Cybersecurity Engineer	$110,000 - $140,000
Cybersecurity Analyst	$100,000 - $140,000

Source: The staffing company Mondo

"You need to look beyond the scope of your job. You need to see the winds of change as they're coming in your industry and your company."

And ask questions, she adds—lots of questions. "What are the priorities coming up and how can my skill set match those? And to whom are these priorities going to be given? The big budgets? Who should I talk to?"

Diamond sees the importance in knowing how the actual job may be changing.

"People need to stay in tune," she says. "Pay attention to the marketplace in general, of what's happening to the function of the roles that we do. It's not the job that gets eliminated. It's certain tasks and projects based on technology … or outsourcing. Part of this is knowing how the economy works."

CFRA's John Freeman advises looking ahead to the latest applications in security, with an eye to leverage the skills you have. Like automation: "Get yourself up to speed on any of the automation tools. It's what you want to get control of because it allows you to secure your job."

Artificial intelligence (AI) and machine learning are also on his list. "Figure out what subset of AI, what specific techniques are being applied on the cutting edge in the specific area you are in."

There are nearly 3 million information security jobs going unfilled, particularly in the Asia-Pacific region, according to the (ISC)² 2018 Cybersecurity Workforce Study. The study also reports that there will be an increase in corporate spending for security in the years ahead. That's good news, especially if you work for an organization that has prepared ahead of time for slower economic growth, or even a recession.

If you are feeling the winds of change blowing your way, know that there are opportunities as long as you know how to recognize them—and act on them. ■

DEBORAH JOHNSON *is the managing editor of* InfoSecurity Professional *magazine.*

THE 'SWISS ARMY KNIFE' OF CYBERSECURITY PROFESSIONALS

With governments needing to invest more resources to protect systems, ISSOs and their equivalent outside the U.S. are needed more than ever. **Do you have what it takes to excel at this level?**

BY BARBARA FINK-OSTER, CISSP

MORE THAN A YEAR AGO, while I was assisting several of my fellow federal information system security officers with various security documentation needs, we began to informally discuss what it takes to be an ISSO.

In that and subsequent discussions, we came to realize what was obvious from the start: Being an ISSO is not easy. And, finding an out-of-the-box-thinking, skills-proficient ISSO is a challenge.

Let's explore why that is.

ILLUSTRATION BY ANDREA COBB

WHAT IS AN ISSO?

Although ISO/IEC 27001 requirements do not identify specific security roles to manage information systems, there is the experiential definition of an ISSO, and then there is the formal definition. The latter can be found using well-documented sources, such as Director of Central Intelligence Directives (DCID), FedRAMP and the NIST Risk Management Framework (RMF).

Embedded in these cybersecurity, risk-management paradigms, various roles are identified and defined. They include: chief security officers, security managers and senior security officers. All the roles in these guidelines were created to:

- Develop and manage all organizational technical and nontechnical cybersecurity policies and requirements.
- Maintain visibility and manage cybersecurity risks.
- Keep the non-cyber-trained system owners, operational users, managers and technical staff on the narrow "cyber brick road" throughout the lifecycle of the system.

The following is the definition of an ISSO or SSO based upon the previously stated security paradigms.

- DCID: The person responsible to the ISSM [manager] for ensuring that operational security is maintained for a specific IS [information system], sometimes referred to as a network security officer.
- FedRAMP: The person who reviews security packages.
- NIST RMF: The individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
- CNSSI-4009: The individual assigned responsibility by the senior agency information security officer, authorizing official, management official or information system owner for maintaining the appropriate operational security posture for an information system or program.

WHAT IT TAKES TO BE AN ISSO

After more than 20 years working various DoD and federal cybersecurity jobs, I have seen my role as an ISSO change over time. Early on, I never observed any role-specific, formal training programs for how to do the job. That may be because the role of the ISSO changed with each organization where I worked.

Based on how others see a fully functional ISSO (see "ISSO Roles and Responsibilities," p. 24), I created two broad categories that describe the skills and talents required for an ISSO.

Category 1: Required Cybersecurity Skills

These refer to skills directly related to cybersecurity and can include:

- Formal training and certifications directly related to cybersecurity.
- Training and/or experience with cybersecurity tools.
- Direct cybersecurity experience, both technical and nontechnical.

Unfortunately, I am not aware of any formal ISSO-specific certifications. An organization's ISSO needs will drive the skills and certifications needed to do the job. Typically, the most popular cybersecurity certifications will suffice. Some organizations also require computing environment or software platform certs, as detailed in DoDD 8140.01 and DoD 8570.01-m.

If the ISSO is short on experience, I recommend the ISSO become familiar with:

- Department of Education's Cybersecurity Core Competency Training Requirements.
- Department of Homeland Security's ISSO Guide.

Category 2: Non-Cybersecurity Skills

These skills directly relate to technical, documentation, people and task management, and compliance audit or assessment skills. They can include:

- Organizational and project management (resources, scheduling, writing, tracking, plan of action and milestones, etc.).
- Auditing.
- Technical abilities (system, application or networking admin experience).
- Technical writing to assist with drafting policies and procedures.

BURNOUT AND OTHER CHALLENGES

For those in ISSO roles, burnout is a problem. In some organizations, there are serious ISSO shortages in which there is one ISSO supporting many systems. However, even if there are no shortages, other sources of burnout can include:

- The ISSO having to assist with fixing operational, software patching or other system maintenance issues even before the cybersecurity requirement can be declared compliant.
- Tedium due to the ISSO having to manually perform tasks when automated tools are not available (i.e., audit log reviews, reconciling asset and software inventories, port and protocol and firewall change reviews, etc.).
- The ISSO inheriting problems from a previous ISSO.

- When security assessments are being performed, finding and getting the required artifacts to support security requirements; this can be a full-time job for several weeks to months.
- Attempting to meet unrealistic expectations from customers, managers or the ISSO herself.

In order to combat ISSO burnout, my advice is this:

- Know your environment (people, mission and technology).
- Know organizational policies.
- Engage with the users, management and technical staff; solutions frequently require team input.
- Get the training you need to do your job (informal, organizational and cyber-recognized certifications).
- Communicate issues to the right people.
- Use Mental Ninja tactics.
- Find a mentor.
- Take care of your physical needs (rest and relaxation, exercise and diet).
- Set realistic goals and expectations.

CHALLENGES FOR MANAGERS

When I became a manager of ISSOs and had to hire individuals for an ISSO position, I noted that finding an individual who knew all the tasks of an ISSO is rare. Also, the ISSO candidate talent pool appears to be inconsistent.

If finding qualified ISSOs is not hard enough, just finding an ISSO seems to be almost as difficult. I have personally experienced and observed in my current job that managers have reviewed anywhere between 30 to 50 resumes of ISSO applicants and only one or two come close to meeting the prerequisites of the job.

To compound the problem, I am noting that non-cybersecurity managers of ISSOs and ISSOs themselves are not totally clear on what an ISSO truly is or what an ISSO does.

The 2018 (ISC)^2 Cybersecurity Workforce Study assessed cybersecurity workforce shortages. Of the shortage of approximately 496,000 cybersecurity professionals in North America, the report also identifies that 37% of the current staff lack skills and experience to do their jobs. It is unclear to me how many of these cybersecurity professionals are ISSOs.

On May 11, 2017, U.S. President Donald Trump issued Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

EO 13800 directs U.S. departments and agencies to address four core areas: securing and modernizing federal networks, protecting the critical infrastructure that

ISSO ROLES AND RESPONSIBILITIES

THE ROLES AND RESPONSIBILITIES of an ISSO are broad and vary by agency, but there are three documents that I believe adequately define an ISSO and the associated roles and responsibilities. These are NCSC-TG-027, NIST Special Publication 800-37, and NIST Special Publication 800-53 Revision 4.

The first source, NCSC-TG-027, defines "Information System Security Officer Responsibilities for Automated Information Systems" as:

> *"Within an organization, the ISSO may be one or more individuals who have the responsibility to ensure the security of an AIS. 'ISSO' does not necessarily refer to the specific functions of a single individual. Also, additional responsibilities may be defined by the ISSO's specific organization."*

Further along in the document, in the section called "ISSO Areas of Responsibility," the list of responsibilities is a bit daunting. It includes physical security requirements (contingency plans, declassification and downgrading of data and equipment), administrative security procedures (personnel security, security incidents reporting, termination procedures), security training, security configuration management, access control (facility access, identification and authentication), data access and risk management, audits (audit trails and auditing responsibilities) and certification and accreditation.

Although NCSC-TG-027 and the other documents in the Rainbow Series have been superseded by other guides and instructions, it still is accurate, based on my own experience as an ISSO.

NIST SP 800-37's daily duties of an ISSO are detailed. With the evolution of privacy concerns, NIST has combined the ISSO and privacy officer duties in the same section.

The ISSO must be qualified in the job and manage the security aspects of an organization (i.e., physical and environmental protection, document and manage various security plans, perform incident handling, support and manage changes, and provide personnel security and awareness training). That person also must interface with the privacy officer and, in some instances, perform the duties of a privacy officer, to "ensure compliance with privacy requirements and manage the privacy risks to individuals associated with the processing of PII."

Lastly, in NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, the ISSO is called upon to perform risk assessments, support incident response and audit log reviews, assist with identification of common controls and support or be a voting member of configuration management control boards.

—B. Fink-Oster

maintains the American way of life, deterring America's adversaries in cyberspace, and building a stronger cybersecurity workforce. This EO provides requirements for both private and public sectors.

This, along with a DoD Cyber Workforce Improvement Initiative, has spawned various government-level cybersecurity workforce programs such as: Cyber Workforce Management Program (DoDD 8140.01 and DoD 8570.01-m), DoD 8570 baseline certification requirements and NIST National Initiative for Cybersecurity Education (NICE).

Although government and other organizations have mandated cybersecurity requirements for the workforce, it will take some time for the effects to be felt in both public and private sectors.

PARTING ADVICE FROM AN EXPERIENCED ISSO

From the many years I have worked either as an ISSO or in some capacity supporting or managing ISSOs, and from the formal definitions of an ISSO, I would personally change Information System Security Officer to Information System Security "Offiziersmesser" (the German word for Swiss Army knife) as it provides a better image of what is required of an ISSO.

Until such time that government workforce programs are fully and broadly implemented and resources (funding, skilled talent, etc.) are available, organizational managers will have to develop tailored and deployable strategies to bridge the gap.

As for the organizational-level solutions, I recommend that managers:

- Create specific ISSO charters to keep the ISSO role focused.
- Use other organizations' existing ISSO core competency requirements to create internal ISSO hiring and training and internal certification needs.
- Hire a core set of senior ISSOs to train and mentor

a team of junior ISSOs.
- If required, modify the ISSO role to an office function rather than an individual.

And managers: Don't forget those automated security tools.

Finally, I recommend that a security consortium create, deploy and assess a survey to determine targeted ISSO issues and possibly create ISSO certifications classes or groups. For example, there may be certifications based upon specific roles and functions, such as:

- C&A ISSO (supporting the CAP certification and focus on RMF Steps 1-3).
- Vulnerability Management and Assessment ISSO (by vendor-specific certifications more focused on security features and not so much on CE configuration and administration of the software).
- Auditing and Incident Response ISSO.
- Software Development/Approved Product ISSO.
- Privacy/PII (based upon NIST SP 800-122) ISSO.

The ISSO shortage challenge is real and the need is great … and *growing*. Though we've focused on the situation from a U.S. perspective, it is likely the same issues face ISSO equivalents elsewhere in the world. It will take a large collective of resources and talented professionals to determine a standard path forward, yet allow for job-specific flexibility. I do believe, though, with time and enough attention, that will indeed happen. ■

BARBARA FINK-OSTER, *CISSP, MSA, is a current information systems security officer and retired Major in the U.S. Air Force.*

SUPPLY & DEMAND

Outsourcing can come at a much higher cost after you sign that vendor contract. BY RAJENDER SINGH, CISSP

PRIOR TO 2013, it was unlikely that a significant data breach could happen due to an exploited third-party HVAC system. But retail giant Target found out it could. Who thought that an online chat service provider could be an exploitable vector targeting the payment information of multiple giant retailers until it happened to Delta, Sears, Kmart and Best Buy? Others, like CSC, suffered a customer data breach when a third party gained unauthorized access, while Ticketmaster's breach originated from a malware-infested third-party customer support system.

ILLUSTRATION BY ANNA GODEASSI

What do they all have in common? The breach that impacted the customer data of every one of those companies originated with a third-party vendor. You can outsource operations, but not your risks when sensitive information flows and resides in third-party networks and physical boundaries outside your offices.

Risk management involves identifying, assessing and remediating risk to an acceptable level. Understanding the overall lifecycle and interactions between the business and a third party, you will find that sometimes security controls are well-designed but poorly managed; and sometimes they are nonexistent.

... sometimes security controls are well-designed but poorly managed; and sometimes they are nonexistent.

A secure supply chain is an ecosystem that can be trusted by the ultimate consumer or customer without worry of any breach or exposure. This is a huge effort for businesses, but by carefully placing the key building blocks, it will eventually give the desired result. A secure supply chain also adds to the overall trust and assurance of a brand name.

Here are some key practices that can make outsourcing more secure.

Call for security from the start

Information security needs be part of the outsourcing model right from the start. Call for security at the earliest stage of outsourcing—even prior to the bidding phase. Security can't be an afterthought; the vendor's security posture and maturity should be evaluated as part of the Request for Proposal and be part of the selection criteria. Security requirements need to be part of contractual documentation, such as the Master Services Agreement and the Statement of Work. Once the supplier is onboarded and connected to the business, these security requirements should be monitored on a regular basis, and results should be used to build criterion to rate suppliers or partners on their security performance and maturity.

Communicate policies or standards

Writing the policies or standards, but not communicating them, can be a fatal error. Though we expect everyone in the outsourcing business to be aware of security policies and requirements, they may not be. All security requirements, such as security policies, data protection guidelines, baseline security requirements and awareness material for the relevant audience should be drafted and communicated in the right format, and kept up to date.

Create a vendor security awareness program

Organizations create awareness programs for their employees but not often for their third-party vendors. The key to developing awareness is a good understanding of the nature of work, profile of employees and threats at each third-party remote site. Overloading employees with too many training videos only adds to confusion, so an effective program will be up to date, accessible when required, interactive and have the right content. For example, tag access provisioning activity with policy awareness training. Good practices also build a positive, security-aware culture in an organization where users understand policies related to account security.

Extend compliance beyond physical boundaries

Companies try to limit the scope of their compliance program to save time, effort and money. But the objective of compliance is to demonstrate confidence in security controls and data safeguards to stakeholders, businesses and the partner ecosystem. Perform supplier site assessments to address all security gaps or issues before launch and on an ongoing basis. As suppliers have access to sensitive customer information and mission-critical processes, compliance programs must be extended to cover the supplier ecosystem as well.

Have a solid risk management program in place

In order to build a secure supply chain, a robust and comprehensive risk management program needs to be in place. The organization should profile the suppliers and perform a comprehensive risk assessment. Understand that every supplier is different; differences in the geographic location, maturity of processes, culture of the organization and other factors play a vital role in risk remediation. All security personnel, such as architects, operations, incident handlers and other relevant teams, should contribute to the risk management framework so that all the risks are captured and addressed.

Ensure visibility into infrastructure architecture and vulnerabilities

Attackers are constantly looking for potential vulnerabilities, and infrastructure is one such entry point for a large number of attacks. The attack methods are so sophisticated that the attack remains covert and very hard to detect. Visibility into infrastructure means logging all the required events at the right layer and nodes to establish traceability and see vulnerabilities at the infrastructure layer. For example, at the network layer, you should be able to generate connectivity and traffic flow (protocols, source/

destination and ports) between the organization and its suppliers. Network modeling and visualization tools give us the ability to see how network devices are configured and generate a network security posture of the entire network or a particular network segment.

Better identity and access control

Each supplier maintains its own independent employee hiring and exit processes, including the onboarding and departure of supplier employees. The business is dependent on the supplier organization to notify it of changes in employee status; delays in communication will result in risk of information exposure and unauthorized access. As supplier employees do not belong to your organization, it becomes an architectural challenge to bridge these two entities in such a way that there are no risks to business operations and supplier employees are enrolled and managed as well. Such challenges should be addressed by process and technology.

Organizations should not overlook threats from their third-party ecosystem, but rather should do the groundwork of developing the right processes and framework for capturing risks and addressing them. Vendor risk management is now a known factor within information security governance that is keeping businesses safe from disruption or losses. Automation and a tool-assisted approach play an important role when managing a large vendor base on an ongoing basis. Businesses need to have a continuous monitoring and assessment program for their third-party suppliers. ■

RAJENDER SINGH, *CISSP, is a Bangalore-based cybersecurity consultant with experience in third-party vendor security assessments, ISO 27001-based ISMS, PCI DSS consulting and penetration testing. He contributes to the information security community through his articles and public speaking.*

Children Increasingly Living Online

by Pat Craven

IN 2016, the Center for Cyber Safety and Education (then called the (ISC)² Foundation) released a research study investigating how younger children (ages 8-14) use the internet. At the time, most existing research focused on teenagers' and adults' behaviors. No one dug deeper into what children, especially younger children, were doing online. That Children's Internet Usage Study found that 40% of the younger children we interviewed had already communicated with a stranger online! They had given out their phone numbers and addresses, and in some cases, even met them in person. It was this information that led the Center to redesign its family outreach efforts and create the award-winning Garfield's Cyber Safety Adventures program as a way to reach, engage and educate younger children.

Today, there is a lot more research on how younger children around the world are using the internet. Not that the message is getting any better, but the findings are opening the eyes of parents, educators and companies to the need to teach children solid basic cyber safety practices from the first moment they connect online. You will find this hard to believe, but our efforts to educate younger children were initially met with resistance from educators because they didn't see the need for it. That is finally starting to change.

In its new study, the Family Online Safety Institute found that 43% of parents have looked to schools or other parents for how to manage their child's technology use. Parents are concerned about keeping their connected children safe online, noting they find it challenging to monitor their child's use of technology, access to inappropriate content, who their child is engaging with and total screen time.

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

A 2018 report by the U.K.-based Ofcom found that 35% of children ages 8 to 11 already have their own smartphone, and 47% own a tablet. Ninety-three percent are online more than 13 hours a week. Similar to our own report, researchers found that 18% of these children have a social media account (despite the fact that most platforms require you to be a minimum of 13 years old to join). The same report showed that children ages 12 to 15 spend more than 20 hours a week online, and 69% have a social media profile.

We are so encouraged that our efforts to start cyber safety training at a younger age is catching on around the world; however, don't think we are ignoring older children. We already have available for your use a free downloadable presentation for kids ages 11-14. And thanks to the committed members of (ISC)², we are in the process of translating the presentation into multiple languages to help us reach as many children as possible.

In addition, over the next few months (with a big launch at Security Congress in October), you will begin to hear about an exciting new program that will help us reach high school-aged students. This new effort will not be a simple 45-minute PowerPoint but rather a four- to six-week, curriculum-based program focused on a better screen/life balance for teenagers. The renowned Pew Research Center found that 95% of teens have access to a smartphone, and 45% say they are online "almost constantly." Helping teenagers (and adults) reduce their screen time will make them safer *and* more productive. ■

Photograph: Fstop123/iStock

Advice on Upgrading Firmware and Anti-Malware for Linux Machines

The (ISC)² Community has more than 20,000 cybersecurity professionals connecting, sharing knowledge and offering solutions in the online forum. Note that the questions and responses may have been edited for clarity and brevity.

QUESTION:

What's your professional guidance on upgrading firmware?

In the contemporary mode at mysonicwall.com, a TZ300 will say the latest firmware is a 6.5.4.3. But if I look in classic mode, all versions are available for download. Classic also reveals that the general release is 6.5.1.3, and that 6.5.4.3 is a recent feature release.

Phone support always pushes for the latest release, but my practice is to stick with the most stable release, and not to upgrade at every turn. So, are there any early adopters? All 14 of you SonicWall users should respond! Thanks!

—Submitted by ericgeater

SELECTED REPLIES:

Sticking to a stable version of a software might sound like an attractive idea, particularly if you don't want to risk some undocumented bug causing havoc in your organization. Then there's the other side of the coin: If a vendor-supported solution isn't up to date, they aren't likely to accept responsibility for anything that goes wrong with it and may not provide assistance to resolve issues.

I'll give you an example involving Juniper firewalls. After observing something unusual during manual config backups, we contacted support. They gathered information and did some troubleshooting, but made no progress, and finally told us this: "This behavior may be attributable to an undocumented bug in the older firmware that the customer is using. The customer is advised to upgrade to version <> to rule this out—after which we can provide further assistance."

(In other words, they couldn't explain it either—but if we wanted to avail of their support, we had to upgrade to the latest stable version.)

After this, things went fine until we tried out an application control feature. It didn't work perfectly; when we contacted support, they asked us to upgrade to the latest firmware version again. Seeing a pattern?

—Submitted by Shannon

You should generally be OK on N-1 of releases until the new release "stabilizes." If the release overwrites firmware and you have no means to back it out, I'd stay as is unless you need the feature you mentioned.

I've used the NSA series, and they were OK as midrange, single-box UTMs internally within the network, but [they] didn't have the bells and whistles you'd expect with other vendors, such as Palo Alto or FortiGate.

—Submitted by Steve-Wilme

So, from my experience, regardless of the technology being used, the first answer from phone support is "push the latest release and that will fix the issue."

Unfortunately, that does not always work, but it is their "stock and standard" answer. So, you go away, upgrade to a potentially flaky version of the software/firmware and still have the issue.

We went through this many times when things stopped working, or began working differently, and we had to spend hours on the phone trying to convince first-level support that, yes, we were at the most recent version, before they would escalate internally.

So no jokes about SonicWall; it seems to be a trait of the industry.

—Submitted by dcontesti

Find this complete thread here.

QUESTION:

This is a longstanding debate in the security world about whether a Linux device needs antivirus. Is it worth it? And what are the risks for public-facing and internal Linux systems? All opinions appreciated.

—Submitted by Deyan

SELECTED REPLY:

Linux may be more inherently secure and less impacted by malware than Windows, but that doesn't make it invulnerable. Based on how critical a system is for business operations and its exposure, you may have to provide extra protection.

Our organization employs an application running on Linux; when I asked the vendor administrator to gauge the impact of running an anti-malware solution on it, he flatly stated that "Linux didn't need anything like that."

Shortly after, the system began generating a lot of unexpected traffic, and a worm was discovered in it. Now, all our Linux servers are running anti-malware. And this happened to be an internal server...

—Submitted by Shannon

Find this complete thread here.