CREATING MORE CYBERSECURITY OPPORTUNITIES

InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

JANUARY/FEBRUARY 2019

What's the RUSH?

FIRST RESPONDERS and faulty ICS gateways

PHISHING AND VISHING Latest ways to hook unsuspecting users

isc2.org facebook.com/isc2fb twitter.com/ISC2 linkedin.com/company/isc2 community.isc2.org

(ISC)²®
SECURITY
CONGRESS
2019

CALL FOR SPEAKERS

OCTOBER 28-30

Orlando, FL

Walt Disney World
Swan & Dolphin Resort

Benefits of speaking:

- Free All Access Pass
- Access to all Education Sessions
- Networking Night Invite
- Town Hall Invite
- Exclusive Speaker Ready Room
- Access to all Keynotes
- Expo Floor
- Members earn up to 46 CPEs

Submit Proposal

Deadline: March 11

ENRICH
ENABLE
EXCEL

Congress.isc2.org
#ISC2Congress

contents

VOLUME 12 ▪ ISSUE 1

A default configuration could wreak havoc in a town near you. PAGE 24

features

Cover image: JEFF MANGIAT Illustration above: SAM WARD

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

editor's note ▌▌▌ *by Anne Saita*

Beyond the Blockchain

BLOCKCHAIN RECEIVED a lot of buzz in 2018, and there's no reason to think the hype won't continue as business leaders eye its potential to manage more than cryptocurrency. I've covered the IT space long enough to recognize when a technology is in a marketing bubble, and blockchain appears to be in a big one. For those whose companies are interested in these digital ledgers, we can help you do your due diligence by reading (ISC)² member Tuan Phan's cover story on the technology, including security and privacy implications.

It remains to be seen what becomes the Next Big Thing, but, regardless, you can bet the bad guys will have exploited any inherent vulnerabilities as soon as it hits the market. The 2018 (ISC)² Cybersecurity Workforce Study (formerly known as the Global Information Security Workforce Study) shows cybercriminals still have an advantage among the growing number of organizations that can't hire information security professionals fast enough. The research shows a gap of nearly 3 million cybersecurity professionals worldwide—with a majority of the need in the Asia-Pacific region. More colleges, universities and trade schools are offering cybersecurity programs to fill the pipeline, but, as you dear readers know, you don't just pick up cyber skills, degrees or certifications overnight. It takes a great deal of dedication to become a CISSP, CCSP, HCISPP, etc.

On a much more upbeat note, the survey shows women now account for 24 percent of the broader security and privacy industries—up from 11 percent just two years ago. So, my eyes weren't deceiving me at last fall's Security Congress when I saw more female attendees and even lines to use women's restrooms.

Time may not always be on your side; but the (ISC)² organization is. Its leaders and staff are committed to providing you with the tools you need to meet both today's and tomorrow's workplace demands. That includes everyone who puts together this membership magazine and its sister newsletter, *Insights*. On behalf of our editors, writers, illustrators, photographers, graphic designers, sales team, publisher and editorial advisory board members, thank you for helping to keep us all safer in the coming year. ■

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

©Rob Andrew Photography

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

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

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

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

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

EDITORIAL ADVISORY BOARD

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

TWIRLING TIGER MEDIA EDITORIAL TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

MANAGING EDITOR
Deborah Johnson

EDITOR
Paul South

PROOFREADER
Ken Krause

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

The Business Case for Diversity in Cybersecurity

by Deshini Newman

Illustration by Jing Jing Tsong/theispot.com

JUST A COUPLE OF MONTHS AGO, (ISC)² issued its 2018 Cybersecurity Workforce Study, which revealed a global gap of 2.93 million skilled cybersecurity professionals needed to protect vital infrastructure and our corporate, government and personal digital assets.

It's going to take all of us to close that gap and create the next generation of trained personnel. That includes recruiting under-represented minorities. The study showed that 24 percent of the cybersecurity workforce is female. While this feels like progress, can we honestly say that we're fully harnessing the potential of half the population in the working world? If we could get that number closer to 40 or 50 percent while the industry's headcount continues to grow, might we be able to bridge this gap? This goes for other minorities as well, be they racial, religious or otherwise marginalized populations.

I was raised in apartheid South Africa and saw the negative impact on a country that did not encourage and celebrate diversity. The late Nelson Mandela is my hero. He never gave up the battle to fight for a fair and just society where all people are given opportunities for growth and development. I also experienced the challenges of being black and female throughout my career. However, I have had some amazing role models, chief among them former Pearson CEO Marjorie Scardino, who encouraged me to be confident in my talent.

Now, I try to create opportunities too. I proudly served as the executive sponsor for the Women in Leadership initiative at Cambridge Assessment, where I encouraged and mentored women leaders. I also sat on the U.K. diversity committee at Pearson Learning. Throughout my career I have sought to recruit the best from a diverse group of candidates, which has always resulted in high-performing teams that deliver excellent results.

In my own backyard, the U.K. government has financially supported the Cyber Skills Immediate Impact Fund to increase diversity in the U.K. cybersecurity workforce. Still, we need to give more attention to attracting girls and other minorities to technical careers.

We need to converse in a language that embraces and encourages all people to be part of this industry. In addition to providing more opportunities for minorities as early as possible in their educational and career trajectories, we need to "make cybersecurity cool," a theme highlighted at the 2018 (ISC)² Security Congress in New Orleans. This shouldn't be a tough sell. Our colleagues in this industry are protecting some of the coolest technology on the planet on a daily basis and engineering ways to keep us safe and secure in the cyber world.

To meet the demands of the future workforce we need to ensure that we attract a wider pool of potential. More than just filling seats, a diverse workforce provides a more creative approach to solutions. As the need for cybersecurity increases, we need to ensure that we use the creative intelligence across the population to resolve challenges and find solutions. If it takes a village to raise a child, I think it also takes an entire industry to build a diverse workforce. ■

Deshini Newman is Managing Director, EMEA at (ISC)². She can be reached at dnewman@isc2.org.

RETURN TO CONTENTS

(ISC)²

SECURE SUMMITS / LATAM

#ISC2LatamSummits

ENRICH ENABLE EXCEL

Join us at the (ISC)² Secure Summit LATAM 2019

September 25-26 | Hotel Camino Real Polanco, Mexico City

The event will offer educational sessions presented by thought-leadership experts from all over the region and abroad.

Come share best practices and knowledge and meet your peers in a relaxed learning atmosphere.

(ISC)² members can earn up to 16 CPEs

Call for Speakers is open!

latamsummits.isc2.org

SAVE THE DATE

(ISC)² Secure Summit LATAM | September 25-26, 2019 | Mexico City

field notes EDITED BY DEBORAH JOHNSON

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

2018 Security Congress— A Sold-out Success

(ISC)² CEO David Shearer shares some of his highlights

MORE THAN 2,000 ATTENDEES flocked to the meetings, keynotes, presentations and vendor displays at the New Orleans Marriott for the 2018 Security Congress. In his blog, (ISC)² CEO David Shearer, exulted in the success. "Our attendees were genuinely enthralled with the caliber of speakers and sessions we pulled together and made me as proud as I've ever been to call myself a member of the cybersecurity community."

In his remarks opening the Congress, Shearer made clear the role the (ISC)² members play in our highly dynamic society, from information technology and security to manufacturing, healthcare and public utilities. "At (ISC)², our members don't make many of the products and services you depend on, they make many of the products and services you depend on better."

"At (ISC)², our members don't make many of the products and services you depend on, they make many of the products and services you depend on better."

—David Shearer, CEO, (ISC)²

This was the second year in a row that the North America Security Congress sold out. Previous events had been co-located with ASIS annual conferences. This has set the stage for next year as the (ISC)² Security Congress will be held at the Walt Disney World Swan and Dolphin Resort in Orlando, which, Shearer says, offers great flexibility. "The new venue will provide us with a lot of increased capacity to continue to grow the event and to welcome more of our colleagues from around the globe"

Registration is now open: Congress.isc2.org.

For more of David's comments about 2018 Security Congress, read his blog post at https://blog.isc2.org/isc2_blog/2018/10/congress-highlights-shearer.html. ■

(ISC)² Welcomes Four New Board Members

Congratulations and welcome to the newest members of the (ISC)² Board of Directors. They were selected in September 2018 by the (ISC)² membership.

- **Cindy Cullen**
  CISSP – U.S.

- **Dr. David Mussington**
  CISSP – U.S.

- **Lori Ross O'Neil**
  CISSP – U.S.

- **Gabriel Alexander Bergel**
  CISSP – Chile

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&PCAT=7777&CAT=10798

RETURN TO CONTENTS

The Gap Widens

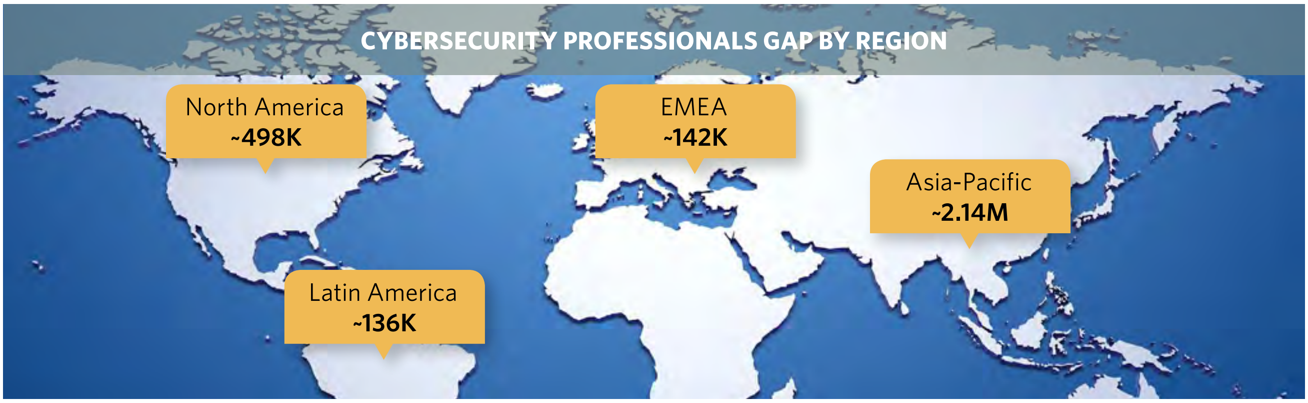
Insights from the (ISC)² Cybersecurity Workforce* Study, 2018

The 2018 (ISC)² Cybersecurity Workforce Study amassed data from nearly 1,500 respondents from North America, Latin America, Asia-Pacific and Europe (EMEA).

How large a workforce gap is there? Close to *3 million* globally, according to (ISC)² research.

**Formerly known as the (ISC)² Global Information Security Workforce Study*

CYBERSECURITY PROFESSIONALS GAP BY REGION



Shortage of Cybersecurity Staffing

63%

of respondents say they have a significant or slight shortage of staff dedicated to cybersecurity

Where Expertise is Needed Most*

Security awareness	58%
Risk assessment, analysis, management	58%
Security administration	53%
Network monitoring	52%
Incident investigation and response	52%
Intrusion detection	51%
Cloud computing security	51%
Security engineering	51%

**% of respondents saying need is "critical"*

Top Job Concerns

Lack of skilled/experienced cybersecurity personnel	37%
Lack of resources to do my job effectively	29%

For the full study: https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study

> **Building tomorrow's security workforce is essential to address this challenge and deliver robust and long-term security for organizations in the digital age. Filling the skill shortage will require organizations to change their attitude and approach to hiring, training and participating in collaborative pipeline development efforts."**

—Steve Durbin, managing director of the Information Security Forum

Source: SC Media, Cybersecurity job gap grows to 3 million, report

> **This research is essential to fostering a clearer understanding of who makes up the larger pool of cybersecurity workers and enables us to better tailor our professional development programs for the men and women securing organizations day in and day out."**

—David Shearer, CEO, (ISC)²

Source: Security Boulevard, Widening Cybersecurity Workforce Gap Nears 3 Million Globally, Says Survey

Cybersecurity Budgets

60%

of respondents say they need larger budgets

Image: Tito Onz/iStock

RETURN TO CONTENTS

A Wake-up Call for Healthcare

ECRI Institute ranks cybersecurity the No. 1 health technology risk

CYBERSECURITY PROFESSIONALS have long sounded the alarm over the dangers hackers pose to networks around the globe, in any field. The healthcare industry continues to be a prime target, given the price for stolen medical records is far higher than credit card numbers.

One international nonprofit research organization, ECRI Institute, in its report, 2019 Top 10 Health Technology Hazards, puts the danger posed by malicious actors at the top of the list: "Hackers can exploit remote access to systems, disrupting healthcare operations."

This isn't news to (ISC)^2 members, of course. But it does show that healthcare organizations are—or at least should be—paying closer attention and should invest enough resources to adequately protect their networks, databases, devices and electronic health and medical records, especially given how heavily regulated the industry now is.

Through incident investigation, device testing and interviews with health practitioners, ECRI analysts developed a call to action for the healthcare industry: "Attacks can render devices or systems inoperative, degrade their performance, or expose or compromise the data they hold, all of which can severely hinder the delivery of patient care and put patients at risk."

Locked out of its records, the hospital paid $55,000 in Bitcoin to get its data back.

An example of what a successful intrusion can do to a medical institution is the January 2018 ransomware attack against Hancock Health in Greenfield, Ind. Locked out of its records, the hospital paid $55,000 in Bitcoin to get its data back. And they were lucky; often victims pay up but are still locked out.

ECRI urges the healthcare industry to institute and adhere to strong cybersecurity practices and to monitor all remote access. If you work in healthcare IT or are interested in specializing in that field, consider the Healthcare Information Security and Privacy Practitioner (HCISPP) certification.

For more information: www.ecri.org/2019hazards. ■

And the Award Goes to ... GARFIELD!

The Center for Cyber Safety and Education series lauded by teachers

TEACHERS' CHOICE AWARD TCA FOR THE CLASSROOM 2019 LEARNING MAGAZINE

(ISC)^2 congratulates the Center for Cyber Safety and Education and the Garfield Cyber Safety Adventures program for winning the national *Learning Magazine* 2019 Teachers' Choice Award. The award, selected by teachers, recognizes the series for its ability to engage elementary school children in core cyber safety lessons.

Patrick Craven, Center director, said, "Teachers are one of our most important audiences for cyber safety education. ...We could not be prouder to know that the entire series of *Garfield's Cyber Safety Adventures* exceeds educators' expectations and meets students' needs in the classroom."

Judges' comments underscored the success of the program:

- "I would and did recommend this product to the principal and purchasing committee for the next year. Bullying and internet safety are two primary focuses for the school, and this product made the lessons engaging and appropriate for the students in our school."
- "I love how it includes not only the comic book booklets for the students but also take-away awards from completion. I believe the take-aways will leave a lasting impression on young students."

The Center for Cyber Safety and Education's *Garfield's Cyber Safety Adventures* was introduced in 2016. "When we first gave Garfield the job of cyber safety champion for kids, we thought we were on to something," said Garfield creator Jim Davis. "This award validates that relatable, engaging characters like Garfield make becoming a good digital citizen not only easy but fun." ■

RETURN TO CONTENTS

RECOMMENDED READING

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

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World

By Bruce Schneier
(W.W. Norton & Company, 2018)

BRUCE SCHNEIER
CLICK HERE TO KILL EVERYBODY
Security and Survival in a Hyper-connected World

AS THE INTERNET OF THINGS has taken hold, author Bruce Schneier peers into the future with a cautionary eye on what our smart devices are not only doing for us but, more chillingly, are potentially able to do to us.

Click Here to Kill Everybody presents the here and now of IoT, then moves to what could happen in a fascinating, thought-provoking book. With the plethora of internet-accessible devices available now (not to mention what's over the horizon), Schneier warns the reader that even though there is more personal convenience, all those devices are listening and recording everything, perhaps risking personal security.

Schneier worries that these products are being released without standards and policies. Users, he says, expect, perhaps naively, that the vendors will patch security holes automatically, thereby protecting them. But he presents frightening scenarios where hackers take control of cars and other IoT devices. While Schneier acknowledges that the benefits to society are enormous, he is a realist and asks that the risks and dangers be considered.

Our laws, rules and norms, Bruce Schneier cautions, are not ready for this new future.

Our laws, rules and norms, Schneier cautions, are not ready for this new future. His pessimism verges on the apocalyptic. While he sees promise in the technologies of artificial intelligence and machine learning, he is concerned that the current level of security is determined by the market even though people will demand controls and process to mitigate the security risks. He hopes that governments will not allow bad internet security policies to flourish, but rather implement needed protections before a catastrophe occurs.

Schneier argues for government assuming its responsibility to help create a future for good. He supports a mesh of technology and public policy as a career path and endeavor. An enjoyable book—the author describes security of the future, the internet of the future and the challenges that must be faced to provide for a safe and knowledgeable citizenry. ■

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.

Threat Hunting Tips—Insight from an (ISC)² Member in a New Book

Blue Team Handbook:
SOC, SIEM, and Threat Hunting Use Cases
Notes from the Field
A condensed field guide for the Security Operations team
Don Murdoch

Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases: A condensed field guide for the Security Operations team (Volume 2)

By Don Murdoch, CISSP-ISSAP, GSE#99

(CreateSpace Independent Publishing Platform; 1.0 edition, 2018)

The second book in the Blue Team Handbook series, *SOC, SIEM, and Threat Hunting Use Cases*, focuses on security operations, SIEM technologies, growing better analysts and making the best use of the numerous data sources that feed a SIEM platform.

This book includes techniques for making a security operations center effective and provides real-world insight on using dozens of data sources for security operations and threat hunting. In addition, there is a specific use case on building a SOC/SIEM with a fully developed example and guidance for the SOC analyst.

Author and (ISC)² member Don Murdoch has deployed numerous SIEM systems for medium-sized to large enterprises across multiple industries, with a primary focus on healthcare. The book encapsulates numerous life lessons learned deploying a wide variety of SOC and SIEM technologies based on a 15-year career, most recently, running an MSSP practice. The Blue Team Handbook motto is "Life Experience, Shared Efficiently."

Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases is available on Amazon. ■

RETURN TO CONTENTS

(ISC)² SWITZERLAND CHAPTER

Sharing Knowledge Builds Membership

RESPONDING TO CONTINUED interest by (ISC)² members for opportunities for shared learning and networking, the (ISC)² Switzerland Chapter recently hosted its first daylong Chapter Security Conference.

Organized by (ISC)² Switzerland Chapter members, including officers led by president John Alexakis, the conference aimed to bring together information security professionals from throughout the region. The conference presented 10 sessions on topics of high interest including the EU GDPR, cloud security, IoT, blockchain and much more. The keynote on cyber risk management was presented by Alain Beuchat, Chief Information Security Officer at UBS.

The conference, which attracted more than 100 cybersecurity professionals, was well-received, says Alexakis. “We did a survey to get feedback and the results were really good, with an average mark of 4.03 out of 5 for the overall conference.”

The interest for the conference sparked a boost in membership. Nearly half of the tickets were purchased by non-members; about 35 of them joined the chapter, increasing membership to 170.

Founded in 2011, the (ISC)² Switzerland Chapter is the oldest chapter in the EMEA region. It promotes the community and specialist networks in information security that are resident or working in Switzerland, or have close ties to Switzerland. Its mission is to advance information security in the local community. ■

(ISC)² SWITZERLAND CHAPTER

Contact: John Alexakis, President, (ISC)² Switzerland Chapter

Email: board@isc2chapter-switzerland.ch

Website: http://www.isc2chapter-switzerland.ch

Q&A

John Alexakis

President, (ISC)² Switzerland Chapter

The (ISC)² Switzerland Chapter enrolled quite a few new members after your Security Conference. Did that meet your expectations?

Yes, certainly. We had some members that left the chapter over the previous years because of relocation or for personal reasons, like a change in professional direction. But with the occasion of the 2018 Chapter Security Conference, we offset the inactive members with new ones. It was the biggest increase in new members during a calendar year, since founding the chapter.

What cybersecurity issues are your members most concerned about?

I dare say that the explosion in the number of IoT devices and the associated security risks are concerns to everybody. However, we also offered a wide selection of topics to focus on areas some members might not be that concerned about yet. For example, many IT professionals have the misconception that blockchain is secure by default, which is not true because, as any other piece of software, it is vulnerable to bugs and security issues. Another not-so-widely-known topic we offered was quantum security. Our goal was that everybody would leave the conference having learned something new and I think we achieved that.

> “...Many IT professionals have the misconception that blockchain is secure by default, which is not true because, as any other piece of software, it is vulnerable to bugs and security issues.”
>
> *—John Alexakis*

What has been the impact from the GDPR in the months since it when into effect? What have you heard from the members?

I think the biggest impact of the GDPR so far is that it

RETURN TO CONTENTS

raised awareness about personal privacy to the general population, as well as forcing companies to think about privacy more seriously. The level of material impact that GDPR will have on preventing data misuse remains to be seen on the long term.

The (ISC)² Switzerland Chapter participates in the Safe & Secure Online program. What are some of the projects you've undertaken and what has been the response?

Every year, in November, there is a special day in Switzerland called “National Future Day.” The goal is to promote open career and life planning for schoolchildren, regardless of gender. On the Future Day, hundreds of businesses and organizations across Switzerland open their doors and organize events for kids that would allow them to get an idea of professional life. We use this day to organize events based on the Safe & Secure Online program, together with our employers, to raise security awareness. Typically, such events are fully booked because every parent is concerned about how children are using the internet. My impression is that kids are always a step ahead—I was surprised to see that in a class of 40 10-year-olds, 90 percent of them already had Instagram and Snapchat. Our goal is to also reach schools; in the future, that will be much easier when the Safe and Secure Online material is available in the local languages. ■

> “Our goal is to also reach schools; in the future, that will be much easier when the Safe and Secure Online material is available in the local languages.”
>
> —*John Alexakis*

A Safe and Secure Cyber World— One Step at a Time

by Tony Vizza

INFORMATION SECURITY PRACTITIONERS have a passion and commitment to their craft that is almost impossible to find elsewhere. Why is this the case? I feel that infosec unleashes the creative "inner child" that helps us figure out how to break controls and bypass security (I got started in cybersecurity as a child by breaking things!). Years of experience, the skills picked up along the way and the maturity that comes with hard lessons learned help us defend against threats, safeguard private information and make us the professionals we are.

This devotion to our field can hinder us, too. Outsiders can feel intimidated by cybersecurity. We often like to smugly remind non-IT professionals when they are doing "silly" things. We use tons of insider buzzwords and jargon. We are known as "no" people by colleagues and coworkers. These (at times) well-founded preconceptions can serve to scare off many bright men and women who could and would consider a career in cybersecurity.

As practitioners, we accept that our choice of profession challenges us to continually learn and manage constant change. As individuals, we aim to protect the public good and seek to ensure a safer and more secure cyber world. At the same time, we see a huge skills shortage in our field, despite the industry offering some of the highest levels of remuneration in the workforce. We continue to see breaches get bigger and more widespread with each passing day. We readily admit that we don't always get it right and face considerable challenges to deliver on our aims. We acknowledge the significant gender and diversity disparity that exists. How can we address these challenges?

Recently, I was in New Orleans for the (ISC)^2 Security Congress. I was walking through the hotel lobby when I overheard a family of four discussing what (ISC)^2 stood for. Using my Australian accent, I was able to get away with stating that I overheard the conversation and described our association and purpose. The son in the family then exclaimed that he was studying information technology at university and had entertained the possibility of considering a career in cybersecurity. Hearing this, I offered to show the family around the Congress exhibition.

Tony Vizza is the Director of Cybersecurity Advocacy for (ISC)^2's Asia-Pacific region and is based in Sydney. He can be reached at tvizza@isc2.org.

As practitioners, we accept that our choice of profession challenges us to continually learn and manage constant change.

We then spent 30 minutes introducing them to my colleagues and discussing the various aspects of cybersecurity and its career prospects. At this juncture, the daughter in the family stated that "I didn't know anything about cybersecurity, but I have learned so much today that I am now considering a career in it!" As I was leaving, the father of the family chased me down to personally thank me for making cybersecurity "relatable and understandable to someone who barely knows how to turn a computer on" and expressed a desire for his children to work in the field purely because of "the passion and enthusiasm" he witnessed.

I'm often asked, "Tony, what do you do at (ISC)^2?" I like to think that I help make cybersecurity relatable, understandable and relevant to all. In advocating for better cybersecurity, my approach is always to consider what we are trying to achieve from the perspective of the people we work to protect. This includes organizational leadership but also includes employees, customers, stakeholders, shareholders as well as members of everyday society.

As certified and proud information security professionals, it is incumbent on us as an association to further the knowledge of cybersecurity not just within our own lives, families and workplaces, but also within our communities, nations and around the world. We can help create a safer and more secure cyber world—only by taking one small step at a time. ■

RETURN TO CONTENTS

THE (ISC)^2 CERTIFICATION PREP KIT

Your Ultimate Guide to Exam Planning

Going for another (ISC)^2 certification? The path to achievement starts with a plan. And confidence comes from knowing you're ready for what's next. Find all the tools you'll need to conquer your exam in (ISC)^2's Certification Prep Kit.

Prep Kit Includes:

- Official training course previews
- Training myths... debunked!
- Fast facts infographic
- Justification letter
- Advice, tips and more!

CISSP ISSAP ISSEP ISSMP SSCP CCSP CAP CSSLP HCISPP

(ISC)^2 Direct: Training from the Creator of the CBK

The (ISC)^2 Direct Advantage

Top-Notch Instructors

Comprehensive Training

Most Up-to-Date Content

Official Study Tools

Knowledge Checks

Choosing the Right Study Tools

Textbooks: Official (ISC)^2 Common Body of Knowledge (CBK)

Insider's tip: The foundation everyone needs.

Set Yourself Up for SUCCESS!

INSIDE...

- Fast Facts About (ISC)^2 Training and Study Tools
- Training Myths... Debunked!
- Official Training from the Creator of the Common Body of Knowledge (CBK)
- Courseware Preview and Justification Letter
- Choosing the Right Study Tools
- 7 Tips for Success

Available for: CISSP, SSCP and CCSP

Get Your FREE KIT

Training Myths.....

Debunked

Myth 1

Pass rates of 90%+ are guaranteed.

Learn why this is a **myth** and check out additional **misconceptions** inside!

EMERGING TECHNOLOGY

What's the RUSH?

Is your company considering adopting the technology this year? Then let's be sure you understand what it is, what it isn't and what it means for security and privacy.

BY TUAN PHAN, CISSP

WHEN BITCOIN topped $19,000 per coin across the various crypto-exchanges around the world in 2017, cryptocurrencies drew worldwide attention beyond that of technology enthusiasts and crypto miners/traders. As a result, blockchain technology, which made Bitcoin possible, also entered the mainstream in a big way. Suddenly, everyone from product marketers to cyber pundits touted blockchain's potential to improve business processes, from recordkeeping and transaction tracking to many other back-office activities like asset management, procurement, inventory, financial reporting and tax preparation.

ILLUSTRATION BY JEFF MANGIAT

While supply chain applications are obvious, security ones are not. That hasn't stopped vendors from claiming the blockchain is the Next Big Thing. Is blockchain technology viable beyond cryptocurrency? What are the possible use cases and their drawbacks? Is blockchain ready for prime time? Can blockchain be the solution to the world's biggest problems? These are the questions that this article seeks to answer in defining and then identifying and assessing opportunities and obstacles for blockchain applications.

WHAT IS BLOCKCHAIN?

In *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business and the World* (Portfolio, 2016), authors Don and Alex Tapscott describe the technology as "an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value." Specifically, in the blockchain technology stack, applications shift from centralized servers to transparent, secure and user-centric decentralized networks.

> **In essence, blockchain technology is a new operations paradigm that shifts trust from central bodies to codes and protocols using a one-stop technology platform.**

In addition, blockchain technology incorporates architecture designs such as peer-to-peer computing (e.g., distributed networking) to provide high availability and resilience to lower the transaction costs for the blockchain network. It also provides cryptographical techniques to provide identification, authentication and authorization of transactions, as well as the immutability of the digital ledger.

To lower transaction costs and eliminate the need for a central authority, blockchain employs smart contracts (e.g., program codes or logic that run on the blockchain platform) and a consensus model that allows the distributed nodes to verify transactions and maintain the valid transactions in an immutable ledger.

In essence, blockchain technology is a new operations paradigm that shifts trust from central bodies to codes and protocols using a one-stop technology platform. This accelerates operational processing; reduces transaction costs; provides automation and standardization; and offers disintermediation or the elimination of the middlemen.

BLOCKCHAIN TECHNOLOGY AT WORK

It is difficult to disagree that blockchain technology is appropriate for managing cryptocurrencies, especially given there were more than 2,000 cryptocurrencies in existence as of September 2018. Cryptocurrencies thrive in untrusted environments like the internet and in the absence of central authorities, such as the country of the fiat currency or network operator.

However, for blockchain technology to become more widely accepted, its uses must extend beyond cryptocurrencies. Accordingly, drawing from the cryptocurrency space, three possible generic use cases for blockchain applications emerge.

Proof of ownership

The broadest use case for blockchain is proof of ownership. This encompasses all transactions that represent the lifecycle from acquisition to transfer of the ownership. Possible applications include real estate properties, financial instruments, loans, patents and trademarks. Proof-of-ownership applications should only be utilized for situations where ownership may be acquired (e.g., purchased), transferred (e.g., sold) and disputed (e.g., liened) and, accordingly, ownership information must exist or be available in a public forum.

Proof of chronology

The second popular use case is proof of chronology, which incorporates time and order with the proof of ownership to track transactions over time. Possible applications include the following:

- Regulatory reporting and compliance
- Accounting and auditing
- Financial management and procurement
- Federal personnel workforce data and appropriated funds
- Federal assistance and foreign aid delivery
- Clearance/background investigations
- Professional certifications
- Marriage certificates
- Auction/bid processes
- Clearing and settlement
- Escrow services
- Tracking of payments and deliveries
- Other goods and services in which time plays a key role in the fulfillment of the transactions (e.g., food spoilage)

Proof of existence (and identity)

The third generic use case is proof of existence, which does not consider the time aspect and simply demonstrates the existence of something, regardless of its lifecycle, to offer integrity and assurance of legitimacy. Proof of existence can apply to internet domains, email addresses and corporation/brand names and, conversely, to records such as criminal convictions, debarments, fines and complaints.

Proof of existence can streamline and reduce the friction between multiple systems (e.g., reduction of paperwork burdens, prevention of data errors, reconciliation of transactions) by acting as a microservice to handle the finality of transactions among those systems.

Proof of identity may also be viewed as a special case of proof of existence as it leverages identification and authentication to prove identities. Practical applications of proof of identity include:

- Single sign-on services to websites
- Digital signatures
- Birth certificates
- Drivers' licenses
- Passports
- Visas
- Health benefit cards
- Other identity-related documentation

IMPACT OF BLOCKCHAIN TECHNOLOGY

One way to measure blockchain's potential impact is to consider the technology's integrity, scalability and, of course, security and privacy implications.

Integrity consideration

Integrity affects public and private blockchain environments differently. The public blockchain network exists in a permissionless environment where anyone can conduct transactions on the network with the appropriate software. Furthermore, the network is not controlled by a central authority, and the participants, both the users conducting the transactions and the nodes that verify the transactions, are not trusted.

Accordingly, user and node identities rely on the user/node public addresses and authentication is accomplished using the corresponding private key. Timestamped transaction data is shared node to node to ensure network concurrency.

To verify the validity of the transactions, each node races to examine its collection of transaction data, craft a new block for the transaction data needing processing and present that block to the peers.

The network selects and rewards the winning node to publish the block (e.g., making those transactions permanent by incorporating the valid block to each node's version of the ledger) from those that provide the fastest response time to the new block with the highest quality meeting a set of predetermined validation rules.

Meeting the fastest response time and the highest quality requirements are collectively known as proof of work (PoW), and this consensus model ensures that the integrity is maintained for the network through the consumption of computational resources (e.g., computer hardware, electricity). PoW provides strong integrity guarantees and tolerates up to a threshold of attacks (i.e., requiring attackers to gain at least 51 percent of the network's total hashrate in order to impact the network—what is called a "51 percent attack"). However, this type of attack actually needs at least 75 percent of the total nodes to work, to be honest.

Other than identification and authentication mechanisms and an immutable ledger, there is little similarity between public and private blockchain environments.

Other than identification and authentication mechanisms and an immutable ledger, there is little similarity between public and private blockchain environments.

A private blockchain network runs in a private, permissioned environment, typically with a designated network operator, where the participants are known to the operator and other participants. A private blockchain is costlier to operate and does not reward nodes (i.e., tokenless) as decisions are made using a voting scheme, typically the Byzantine Fault Tolerance (BFT) consensus model, where a set number of nodes agrees to the validity of a block of transactions.

BFT offers a greater degree of adversarial tolerance of up to 33 percent of the total nodes as malicious vs. 25 percent from PoW. A private blockchain also places stricter controls on privacy and access to the transaction data for the nodes, but it eliminates the computation and environmental impacts associated with PoW. This mechanism is necessary to provide transaction privacy for the participants, such as those in a network of buyers/consumers and suppliers/providers.

For example, a buyer using the same network may source the same product from multiple suppliers using different unit pricing based on the quantity and other intangibles uniquely negotiated between the buyer and the supplier (and, of course, kept private from other suppliers). In addition, instead of producing their own product for the buyer, the suppliers may choose to be the buyer themselves and resell the product using their own set of pricing and other intangibles over the same network.

The integrity of the blockchain equates to the degree of trust. PoW requires transaction data to prove transaction history and binds that degree of trust to expending computing resources. The more resources consumed and transactions examined, the more trustworthy and, accordingly, the higher the integrity given to the blockchain.

By replacing the PoW with BFT, the nodes do not have any real consequence to submitting invalid blocks; therefore, they are more likely to yield inconsistent outcomes at the cost of availability. Accordingly, BFT may be unacceptable in scenarios where integrity in the transactions must be kept high.

The detraction from decentralization also impacts the integrity of a private blockchain. Nodes must still be compensated for providing the infrastructure that processes the transactions and this typically comes in the form of fiat currency provided by the network operator. As the payment does not make use of a utility token of the network, the integrity of the network may suffer since consequences for submitting invalid blocks are not considered. When coupled with the smaller number of nodes available, the network operator may exert more influence on the network than intended, requiring more trust to the network from the participants. This weakens the network's value proposition.

All of these factors may impact the network's availability and generate fraudulent or third-party interference, which may lead to censorship.

The immutability of the ledger can also be influenced by the selected environments.

Verified transactions are aggregated into a block and incorporated into the ledger based on an append-only approach on the time-order basis using the hashes of the transactions and the hash of the block header of the prior block. Accordingly, the chaining of the current block to previous blocks and so forth makes any attempt at altering past transactions extremely difficult and prevents tampering with the transactions after they have been accepted as valid. Any transactions not documented as part of the history are regarded as nonexistent.

However, if transactions were faultily recorded, possibly due to faulty underlying infrastructure design errors or incorrectly programmed smart contracts, how can they be corrected? For public blockchains the short answer is: They can't. Faulty transactions cannot be corrected and are generally accepted as is. For significant issues, major changes are accomplished through a major code update (e.g., a hard fork), which involves a complete ledger revamp across all impacted transactions to address the issue identified. Hard forks contradict the guiding principle of ledger immutability and are often contentious discussions within the blockchain community.

In the world of cryptocurrencies, hard fork debates have led to the creation of competing solutions such as Ethereum from Ethereum Classic and Bitcoin Cash from Bitcoin. By contrast, corrections of faulty transactions in private blockchains are trivial in nature as the design allows for such corrections to be facilitated by the network operator, an implied trusted central authority.

Scalability

One known limitation of current blockchain technology is the limited throughput, measured as transactions processed per seconds. On average, Bitcoin processes about seven transactions per second, compared to Ethereum (15 transactions per second) and Ripple (the fastest major cryptocurrency, at 1,500 transactions per second). For comparison purpose, the Visa network does around 24,000 transactions per second. The consequences of a slow transaction rate often result in a longer wait for individual transaction confirmation. Subsequently, there's less finality on the transactions due to a possible transaction rollback and, as a result, higher transaction fees.

Solutions to scaling include:

- Increasing the block size
- Separating signature from transaction data (e.g., Segregated Witness method)
- "Sharding" transactions
- Off-chaining transactions

Increasing block size makes nodes more expensive to operate, reduces the number of nodes and leads to more powerful centralized entities. Block size changes are more difficult on a public blockchain, requiring hard fork and often contested by the user community.

Sharding effectively breaks the blockchain into partitions of smaller chunks with their own independent piece of state and transaction history, allowing the throughput of transactions processed in total across all shards to be much higher than having a single shard do all the work as in a main blockchain.

Off-chaining allows for transactions to be processed off the main network and added to it later. Off-chaining violates decentralization, as the nodes performing such tasks must be explicitly trusted. While these technologies are promising in solving the scaling obstacles, they should be considered experimental at best.

SECURITY AND PRIVACY CONSIDERATIONS

From a security and privacy perspective, blockchain technology is not well understood due to the complexity of the components and infancy of the technology.

The design of the network architecture and access con-

RETURN TO CONTENTS

trol plays a crucial role in reducing insider threats to the network. Requiring a minimum number of nodes to be properly connected, designated and authorized for participating in a federated or private blockchain consensus process is a good start to strengthening the security of blockchain technology. The minimum number should be at least large enough to provide adversarial protection that matches the degree of integrity required for the network. Since public blockchains are prone to the aforementioned 51 percent attack, care should be taken to ensure the network has enough geographically dispersed nodes to prevent any collusion from any one entity, any specific country or specific region of the world.

While it does not seem like much, for practical purposes, the keyspace is essentially infinite.

The possession of the private key proves both ownership and the assigned rights to execute certain transactions. Accordingly, security depends on choosing and protecting the private key. For example, Bitcoin's security model rests on a private key that composes an integer between 1 and 10^{77}. While it does not seem like much, for practical purposes, the keyspace is essentially infinite. As the private keys contain many digits, using the Wallet Import Format (WIF) reduces the private key into a sequence of characters and numbers shown below:

5GK67bPQuYpm884wtkJNzQGaCErckhHJBGFsvd3VymHfqcXj3hS

Or, most blockchain wallets can generate a series of words as backup (e.g., *body decision painful space bloom sunlight grown father sky third mirror jump*). Given their importance, take extreme caution whenever storing or transmitting private keys or safeguarding the backup words. Most software wallets provide user-friendly PINs, passwords or passphrases to encrypt and decrypt stored private keys and keep the encrypted wallet on the main hard drive of the user's computer. However, the keyspace for the wallet's PIN, password or passphrase must be sufficiently large to prevent being reversed using rainbow tables, particularly if the hash algorithm is known—such as documented by JAXX's known weakness for using the SHA256 hash algorithm for the four-digit PIN utilized for user authentication.

As most blockchain technology is open sourced, available documentation may not be up to date and formal training on specific blockchain platforms may also be limited. As a result, most developers are likely to be self-taught through

SMART CONTRACTS: What's in That Code?

AN INDEPENDENT REVIEW of Ethereum smart contracts revealed more than 100 errors or bugs per 1,000 lines of code. That is between two and six times the industry average, depending on the coding techniques.

The top two categories of issues relate to:

- Security flaws that resulted in the loss of money or control for users or owners
- Poor performance based on the description or code comments

In a 2018 publication, *Finding the Greedy, Prodigal and Suicidal Contracts at Scale* by Ivica Nikolic, et al., the authors proposed the use of MAIAN, an automatic tool for finding three different types of trace vulnerabilities in Ethereum smart contracts:

- Greedy for contracts that lock funds indefinitely
- Prodigal for contracts that leak funds carelessly to arbitrary users
- Suicidal for contracts that can be killed by anyone

The authors analyzed nearly 1 million smart contracts on Ethereum and found 34,200 (or 3 percent) with some form of trace vulnerabilities. The authors were able to properly confirm Parity Technology's Smart Contract multi-signature library as suicidal, which locked the Parity wallet and ultimately froze $150 million in Ethereum tokens when the contract was unintentionally exploited by an inexperienced developer. The event was deemed accidental because the developer did not gain from the event.

Accordingly, a blockchain deployment should use formal verification of secure coding practices through peer code review, formal testing and code regression maintenance to improve the quality of the smart contract and reduce the likelihood of these trace vulnerabilities.

—T. Phan

RETURN TO CONTENTS

trial and error and therefore will likely make significant mistakes, which can lead to the presence of buggy code.

This makes smart contracts one of the most significant sources of weaknesses for blockchain security.

OTHER SECURITY ISSUES TIED TO BLOCKCHAIN CREATION AND MANAGEMENT

Patching security flaws on private blockchains follows best practices similar to other enterprise applications and, for the most part, only lightly impacts an enterprise. On the other hand, patching of public blockchains represents a unique challenge as significant changes may require a hard fork, as previously discussed, which may result in the creating a second blockchain and subsequent costs from reprocessing affected transactions.

Unlike public blockchains where the recovery of assets, user credentials or rollback of transactions is nearly impossible, private blockchains can be designed to provide mechanisms to facilitate these needs. As such, the loss of identification credentials may be addressed with a robust key management program. Organizations must consider the tradeoff and plan for data accuracy and correction vs. immutability of information. Also, a hard fork of codes may be expensive to implement post-event; therefore, consider installing pre-built transaction rollback mechanisms to append transactions to the rollback state, particularly for systems that manage physical or financial assets.

Unlike public blockchains where the recovery of assets, user credentials or rollback of transactions is nearly impossible, private blockchains can be designed to provide mechanisms to facilitate these needs.

Due to its inherent distributed nature, blockchain implementation must consider the rights of individuals to protect and erase their private information, particularly financial and health information. Instead of using actual data, privacy experts recommend using cryptographic hash references to provide evidence on the chain while limiting access to transaction data.

Other implementation possibilities may include the obfuscation of transaction data, additional safeguards to limit access control for the nodes and the participants, or the use of zero-knowledge proofs or “succinct arguments of knowledge” (SNARKs). SNARKs offer the greatest possibility for safeguarding privacy as they programmatically verify hidden inputs known only to the user to derive public known output that affirms the user without revealing any other information.

KEEPING AN EYE ON REGULATIONS

In many countries, regulatory focus on blockchain technology has been limited, with more focus on its promise to enable more optimal ways of doing business. As its use grows, however, expect regulators to follow as is already happening in places like Singapore and Switzerland, among others.

Positive trends are happening. Industry groups from financial services, healthcare and supply chain management to education, academia and others are rapidly forming to access blockchain technology in a legal and regulatory contest. There also are U.S.-based federal and state government working groups such as the Congressional Blockchain Caucus, Government Blockchain Association (GBA), Delaware Blockchain Initiative and Illinois Blockchain Initiative.

The 2018 Joint Economic Report released by the U.S. Congress makes the following recommendations:

- Policymakers and the public should become more familiar with the technology.
- Regulators should continue to coordinate to guarantee coherent policy frameworks, definitions and jurisdiction.
- Policymakers, regulators and entrepreneurs should continue to work together to ensure developers can deploy these new blockchain technologies quickly and in a manner that protects Americans from fraud, theft and abuse, while ensuring compliance with relevant regulations.

Several congressional bills related to blockchain and cryptocurrencies have also been proposed to protect against being leveraged for money laundering, counterfeiting, terrorist financing and tax evasion.

IS BLOCKCHAIN READY FOR PRIME TIME?

We are still at the beginning of a blockchain revolution.

The technology, while complex and technical to implement, potentially offers significant improvements to existing processes and methods. It creates new business models and corresponding opportunities.

However, blockchain technology is not a panacea to resolve issues with existing processes. Therefore, organizations need to understand their true needs prior to adopting blockchain technology.

RETURN TO CONTENTS

Popular use patterns for evaluations

When considering use cases, organizations can apply the following use patterns in their evaluations. The absence of one or more of the patterns may indicate a poor fit for blockchain applications.

The most important use pattern for an ideal blockchain is the cost of trust currently performed by the "trusted" intermediaries. In the current transaction models, these are entities that operate, safeguard, oversee and ensure transactions for banks, insurance companies, lawyers, etc. Indirectly, they serve as a quasi-central authority to support the networks. However, their participation adds unnecessary transaction costs and controls on the network, both of which conflict with the blockchain's disintermediation and lack of authority value proposition.

The type of data and the methodology for their use also is central.

Decentralization must be chosen over centralization, as the latter requires implicit trust that contradicts blockchain's trustlessness value proposition. Accordingly, managed data must be sharable or be able to exist on a public forum.

The open access serves as notice for any disputes with the claimed ownership information. For example, in the U.S., real estate properties can be readily retrieved from states' departments of tax administration because that information is considered public record. In contrast, health, income tax and financial records do not exist in the public domain. In these instances, privacy takes precedence over transparency due to the limited sharing of information. Furthermore, a certain degree of trust must be placed on the network operator who becomes the custodian and facilitator of the sensitive data.

Also central to blockchain's value proposition is the ability to provide immutability and integrity to transactions in a logistic chain. Consequently, transaction data must be available so that the nodes can compute their version of the digital ledger and confirm the transaction history. By limiting access to the data, the certainty of the ledger is diminished. Although it may be overcome by new methods such as SNARKs, more thorough testing is still needed on a larger scale to demonstrate the viability of these approaches.

Blockchain technology still has critical obstacles to overcome, such as enhancing security without compromising network performance and honoring both transparency and privacy.

Organizations wanting to adopt blockchain technology should approach with caution as there are many hidden costs to consider, including mapping and reengineering existing processes to work in a blockchain scenario. Acquiring or training staff with the specialized skills to develop, implement and maintain the technology can add significant costs too.

Do your due diligence now so that everyone in the organization thoroughly understands how a blockchain application will work and how much time, talent and effort is required. That includes working through security and privacy issues before they become problems. Doing all of this not only will help determine blockchain's viability within an organization, it will also help ensure sensitive data cannot be compromised. That is one way to realize a strong return on investment for a technology still in its infancy. ■

A RELATIVELY NEW INDUSTRY Needs New Experts

THE ADOPTION OF BLOCKCHAIN technology and smart contracts will require specialized skillsets. According to a recent study conducted by Burning Glass Technologies, an analytics software company based in Boston, the demand for blockchain expertise grew by 115 percent in 2017, with similar gains reported by many technical job search sites.

Salaries are growing as well.

The freelance job website Upwork recently showed numerous positions for blockchain developers paying upwards of $150 per hour. Many blockchain startups are also offering a combination of equity, bonuses and other perks for onboarding and retaining qualified blockchain developers. Many of those rewards are reminiscent of incentives from the late 1990s, before the dot-com bubble burst.

—T. Phan

TUAN PHAN, *CISSP, PMP, Security+, SSBB, is a partner with Caplock Security LLC, where he also serves the practice leader for blockchain technology. He is leading the development of several proofs of concept using Hyperledger Fabric and Ethereum private blockchains and implementing security audits of blockchain technology. Tuan can be reached at* tphan@caplocksecurity.com.

RETURN TO CONTENTS

IoT AT THE CELLULAR LEVEL

First responders (and the public) are at risk due to default configurations in ICS gateways.

BY SHAWNA McALEARNEY

IN THE MOVIE *The Italian Job*, a character remotely manipulates traffic lights. In *Live Free or Die Hard*, police officer John McClane attempts to stop cyberterrorists who hack into U.S. transportation and electrical grids, gas lines and other critical systems to disable key elements of the nation's infrastructure.

Unfortunately, this is no longer the stuff of film fiction, and it doesn't require a hardware or software vulnerability either. Instead, it requires only weak access control and the use of default credentials.

ILLUSTRATION BY SAM WARD

RETURN TO CONTENTS

Yes, using default passwords is *still* an issue. F5 Networks Principal Threat Researcher Justin Shattuck discovered the problem and says he can speculate as to the cause.

"We know a very common reason many organizations' IT staff are unaware of the vulnerability caused by default and weak authorization is due to their use of a third party," he says. "For example, I spoke with an oil and gas company that used a service provider and consulting company to deploy hundreds of cellular gateways. These were left online and therefore vulnerable. The company only became aware when auditing their invoices for service to those devices and observed a high quantity of SMS messages being broadcast from them."

And the manipulated traffic lights referenced above do exist. According to F5 Networks, an application delivery networking and security provider, "They are often connected back to a smart city's infrastructure through the use of VPN tunnels and other private means of communication over devices like cellular gateways." Critical infrastructure has always been a prime target for cyberattacks, but security researchers now warn of increased danger from agencies that install improperly configured devices or use insecure wireless services as part of their modernization initiatives.

"These gateways are similar to the modems and routers used by consumers at home but with an additional feature, cellular connectivity, often in the form of 4G/LTE, if available," F5 security researchers report. "Additionally, these devices are capable of providing a variety of connection options, including wireless connectivity over 802.11x, Ethernet, USB, serial, analog and digital I/O, and cellular bands ranging from 2G through 4G LTE. If the devices are not configured properly, an attacker may be able to access them and do just as Lyle did in *The Italian Job*."

In an October 2018 interview, Shattuck says more than half a million devices, likely across all cellular device manufacturers and industries that require long-range, constant connectivity, are impacted. Though only Sierra Wireless models were listed in his report, he believes "the problem to be widespread across all manufacturers of cellular IoT [Internet of Things] devices."

CRACKS IN DEFAULT CREDENTIALS

Those researchers found that a default configuration in cellular IoT devices can allow an attacker to "easily leverage remote administration for nefarious purposes. The improperly configured devices we discovered and tested had either default administration credentials (such as admin:12345) or required no authentication at all." They also warned that the absence of logging capabilities on these devices ensures that such activities cannot be tracked.

Cellular connectivity goes far beyond consumers' personal cellphone use. Shattuck and his team note that the demand for long-range, constant connection extends into many, many industries, especially organizations that operate fleet vehicles, from delivery drivers to law enforcement.

"Critical emergency services such as police, fire and medical manage their fleets with vulnerable cellular IoT devices … devices susceptible to remote attacks because of their weak access control and use of default credentials," F5 security researchers write in their paper. "Once accessed, an attacker can use the device to launch attacks, as we have seen with thingbots like Mirai and Reaper, or they can use that access for nefarious purposes to spy, redirect commands in the case of a fleet taking orders from a remote command or shut the system off, effectively disabling operations."

> **This is an urgent human-interest matter as we have moved beyond the unpleasant life impact of stolen data and into attacks that can literally cost people their lives."**
>
> *—Justin Shattuck, principal threat researcher, F5 Networks*

"The critical emergency services we depend upon are using these systems," they added. "This is an urgent human-interest matter as we have moved beyond the unpleasant life impact of stolen data and into attacks that can literally cost people their lives."

After determining that Sierra Wireless devices were among the majority of wireless devices impacted because of market share, F5 security researchers went to the company's website for case studies and found "a wealth of customer stories and details about the types of applications many customers were using Sierra devices for." They included emergency services and police and fire departments throughout the world.

When asked about a worst-case scenario, Shattuck says: "Specifically any of the items outlined in the research, [used] in coordinated warfare and terrorism attacks, [can cause] human loss of life. A substantial amount of damage can be caused by someone wanting to cause harm or [by] simply 'toying' with a device they access, causing a critical piece of infrastructure to fail. Stoplights could go down, sensitive pipeline devices could fail, police records systems could be inaccessible or compromised."

RETURN TO CONTENTS

Default password problems can run the gamut from individual consumers to large-scale enterprise or government agencies. When asked for cases in which this issue has been used to cause a problem, Shattuck says, "I cannot speak to specifics, but we've been in touch with several municipalities and different vendors about issues this vulnerability has caused."

NOT A VULNERABILITY PER SE

It's important to reiterate that this is not a vulnerability in the hardware or software sense. As such, it is not only going to affect a single vendor or a small segment, but rather, likely, most of the industry.

"There is no weakness in the software to exploit," says Shattuck. "There's no hacking of the hardware. This is a weak admin user authentication exploit—the age-old 'user didn't change the default password' story."

> **There's no hacking of the hardware. This is a weak admin user authentication exploit—the age-old 'user didn't change the default password' story."**
>
> *— Justin Shattuck, principal threat researcher, F5 Networks*

Because the gateways were deployed insecurely, for example, with configuration interfaces exposed on the public internet with only default password protection, Sierra Wireless Chief Security Engineer Larry LeBlanc says he prefers the term "default password problem."

"An analogy would be the risk you take when leaving your door unlocked, or perhaps more correctly if you lock it with a key that is the same as that used by every other lock in the city," says LeBlanc. "There is nothing wrong with your door or your lock, except that it is very easy for anyone to unlock."

CAR 54, WHERE ARE YOU?

Consider the potential ramifications of excessive information disclosure. Fleet vehicles like those for law enforcement or emergency response need to be tracked, so virtually all of them list GPS coordinates. Allowing those coordinates to be publicly accessible could allow an attacker to discover in real time the exact location of a target vehicle.

"In late 2016 and early 2017, when our research was in its early stages, it was national news that 2016 was an especially fatal year for law enforcement officers. In fact, ambush-style assassinations on police officers were up over 150 percent," F5 researchers write in their report. "With this dominating much of the national discourse at that time, it wasn't difficult to see the dangers posed by being able to track police officers in their vehicles, in real time. It is a horrifying thought, and we'll leave it at that, but a real possibility."

The team also noted a trend in terrorist attacks that has been evolving over the last two decades.

"Another horrifying, yet real, scenario involves medical help never making it to the scene or at least not in any condition to provide aid," they report. "Emergency medical personnel en route to save lives become victims themselves, increasing the time before initial victims receive help and reducing overall emergency response capacity. The same way police cruisers can be tracked, so can ambulances."

OH NO, THE SKY IS FALLING! NOT REALLY.

While this problem presents serious security issues, there are easy remediations. In fact, if you are a Sierra Wireless customer, the company will fix it for you. LeBlanc says the company offers a "concierge service users can call on to have us conduct an assessment of their deployment and execute a remediation plan—whether that means changing default passwords, upgrading firmware or fixing unsafe configurations. We've talked to over a thousand customers, but we'd like to talk to more."

Sierra Wireless Airlink gateway customers can call 1-877-552-3860 for an evaluation.

"IoT devices are increasingly being deployed in systems that manage information and controls which, if compromised, could be exploited by an adversary engaging in warfare, terrorism or targeted attacks on individuals and businesses," concludes Sierra's LeBlanc. "It is therefore critical for organizations deploying these systems to consider all the ways such systems can be compromised and implement an appropriate security framework to protect them.

"A key aspect of that framework is to make sure that IoT devices are deployed with an adequate security posture—disable all unnecessary services, make sure that necessary services are protected by cryptographically strong credentials and keep firmware up to date to address security vulnerabilities as they are discovered." ■

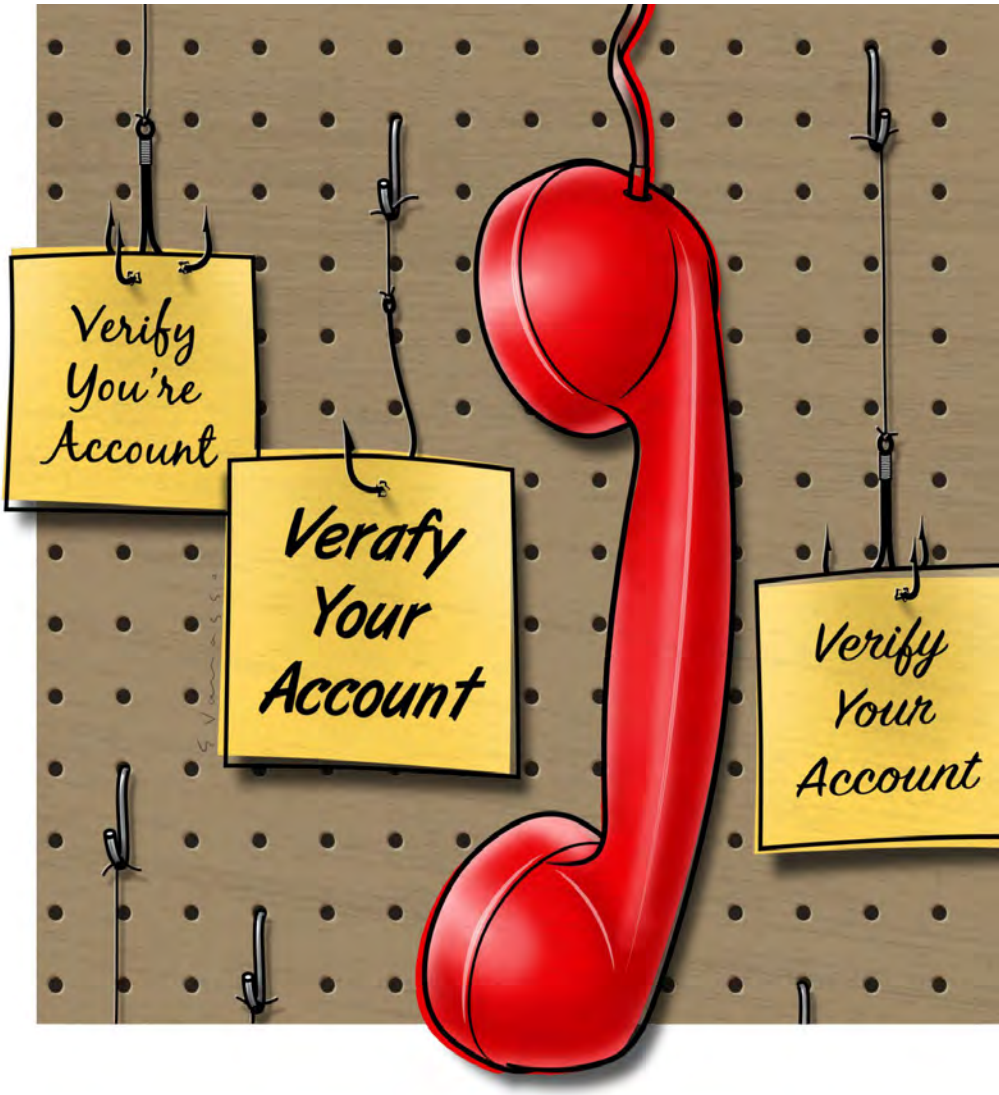
SHAWNA McALEARNEY *is a Las Vegas-based freelance writer and regular contributor to* InfoSecurity Professional *and its sister publication,* Insights.

RETURN TO CONTENTS

Phishing and Vishing

Malware developers are learning to leverage AI and other popular tech in the hunt for gullible users.

BY LEE KIM, CISSP



PHISHING AND VISHING (voice phishing) have evolved to become an advanced threat, where even the most sophisticated computer users may fall for a ploy. Tailored to targeted individuals, myriad phishing forms are no longer a labor-intensive endeavor. (Remember: Time is money.) Artificial intelligence tools now make phishing and vishing cost-effective and efficient, which can't be good news to anyone tasked with protecting an organization's virtual borders and assets.

STATE OF PLAY

Various researchers report attackers have completely automated phishing and vishing attacks on individuals. Indeed, AI techniques may also be

ILLUSTRATION BY ENRICO VARRASSO

RETURN TO CONTENTS

used to conduct (or simulate) spear phishing and vishing attacks, and without any human intervention. For example, researchers devised a fully automated spear phishing system that creates tailored tweets based on a user's interests, achieving a high click rate for links that could be malicious.[1] Yet other researchers have devised an artificial intelligence system for automated spear phishing that includes automatically constructing and communicating a spear phishing message tailored to the intended victim using information that is unique to that individual.[2]

Despite Jim's considerable efforts, his automated spear phishing and vishing attacks at Bob fail miserably. The reason: the scraped information is of poor quality.

But, those of us in the healthcare cybersecurity field know that attacks are often multi-dimensional. As an example, a phishing email may be followed by text messages and/or phone calls (i.e., vishing).[3] Accordingly, the threat may be pervasive and persistent. However, to fully appreciate the impact and significance of this threat, we need to first understand the role of intelligence gathering and analysis.

INTELLIGENCE GATHERING AND ANALYSIS

Intelligence may be used to describe the process of interpreting information to give it meaning. More specifically, the authors of *Criminal Intelligence for the 21st Century: A Guide for Intelligence Professionals* define "intelligence" as "consist[ing] of pieces of raw information that when collected, evaluated, collated, and analyzed form meaningful and useful judgments that are both accurate and timely." The step-by-step process may be described in Figure 1, below.

This analytical process may be performed by a human analyst, a machine or a human analyst with the aid of a machine. As stated previously, various researchers claim to have developed a fully automated means for doing this in the context of phishing and vishing. The degree to which this is effective and impactful depends upon the kind and quality of information sources, information gathering and intelligence analysis. No matter how sophisticated an algorithm may be for processing such information, bad data can ruin everything—garbage in, garbage out. Thus, confirming the veracity of such information is just as important as weighing its relevancy and value.

HYPOTHETICALS

When Phishing or Vishing Fails

Unsophisticated phishing and vishing attempts tend not to be believable. Something "obvious" may tip off the victim into believing that the communication is fraudulent, such as poor grammar, spelling or "too good to be true" claims. Accordingly, many of these unsophisticated phishing and vishing attempts get treated as "spam" and ignored.

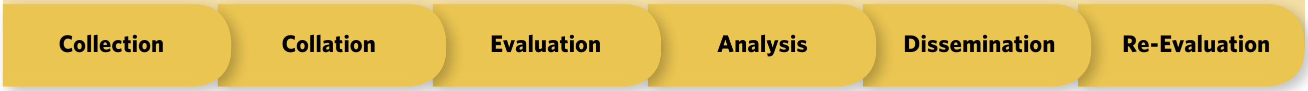
By the same token, merely using a sophisticated artificial intelligence technique, but coupled with poor quality data, may lead to a similar, faulty result.

Consider the following example: Bob is a longtime, well-respected and well-positioned employee at XYZ Corporation. Ten years ago, Bob was a manager within the finance department. But, today, Bob is the head director of the finance department.

Jim, a threat actor, decides to target Bob and others like Bob in financial positions across the country. Jim has a powerful AI tool for automating spear phishing and another to scrape social media profiles and other online sources (such as bios on company websites) for information on potential targets. When combined, these tools create a sophisticated phishing attack system.

Despite Jim's considerable efforts, his automated spear phishing and vishing attacks at Bob fail miserably. The reason: the scraped information is of poor quality. The spear phishing and vishing communications sent to Bob are within the context of his *old* title from 10 years ago. As soon as Bob receives these communications, he almost instantly disregards them.

Figure 1: **The Intelligence Process**



Source: *Criminal Intelligence for the 21st Century: A Guide for Intelligence Professionals*

RETURN TO CONTENTS

When Phishing or Vishing Succeeds

Obvious phishing mistakes can "tip off" the intended target and quickly end a malicious campaign. However, clues that may appear phony to one person can get through to someone else with a lower acceptance threshold. It's possible someone that was sent an email similar to Bob's and was intrigued or not paying close attention.

Furthermore, much like the intelligence process always involves (ideally) refining intelligence, threat actors are continuously refining their techniques based upon results and lessons learned (i.e., what works and what does not work). Part of this refinement includes some element of innovation. If it were not for a threat actor's creativity, the cybersecurity field would indeed be a boring place. But, we know how dynamic it actually is. Human ingenuity may be used for good or evil.

An email that has insider information (or other indicators of authenticity, such as references to a real person, company or brand) may fool the average recipient—or even a more sophisticated user.

Sometimes, too, the novelty in phishing and vishing attempts can be quite unique. For instance, an email message may encourage the recipient to click a link in order to view his or her spouse's divorce papers. This email communication may appear to come from a senior partner at an elite, global law firm. Indeed, the actual law firm and senior partner may all be real. But, obviously, the communication in this case is not—it is fraudulent (and with a poisoned link). Couple this type of communication with a fully automated process for targeting various high-value targets and the threat actor could indeed win.

Average Offenders and Repeat Offenders

In the healthcare sector, the average click rate for phishing victims is about 10 percent. Depending on the size of an organization, this number (a mere 10 percent) may add up to a lot of clicks. (Hypothetically, if an organization employs 30,000 individuals and 30,000 people get the same phishing communication, then it stands to reason that about 3,000 people will click on the link.) Accordingly, achieving a click rate of less than 10 percent is desirable among healthcare organizations.

A best practice, then, is to implement phishing metrics that track who is clicking on the malicious links and whether there are any patterns of behavior or users (e.g., repeat offenders)[4]. Once such a pattern is discovered, or even if it isn't, it's a good idea to examine a company's technology infrastructure or security awareness training to decrease any percentage of clicks.

BAD GUYS HAVE BEST PRACTICES TOO

Best practices are not just for the good guys. A threat actor may keep track of who falls for phishing and vishing communications and who does not. As a result, the repeat offender may be targeted repeatedly over time for all of the obvious reasons.

Phishing is not child's play, especially when AI techniques are leveraged and novel (and convincing) communications are used. An email that has insider information (or other indicators of authenticity, such as references to a real person, company or brand) may fool the average recipient—or even a more sophisticated user.

An antidote to this is to apply more human intelligence. Question and analyze what comes through, and what gets stopped at the gateway. Train your end users to better scrutinize unexpected communications, whether in email or links in social media posts. Better analysis yields better results, always. ■

LEE KIM, *BS, JD, CISSP, CIPP/US, FHIMSS, is Director of Privacy and Security and Interim Senior Counsel and Data Protection Officer for HIMSS.*

FOOTNOTES:

[1] See Future of Humanity Institute, University of Oxford, and the Centre for the *Study of Existential Risk, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, available at https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf (citing John Seymour and Philip Tully, *Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter*, available at https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf).

[2] See US Patent No. 9,882,932 to Bringsjord et al., entitled "Automated Spear Phishing System."

[3] See US Patent Appl. No. 20180124108 by Irimie et al., entitled "Systems and Methods for an Artificial Intelligence Driven Agent."

[4] Virtually every organization, no matter how big or small, has "repeat offenders"—people who are somehow more prone to phishing and vishing attempts than others.

RETURN TO CONTENTS

Want Garfield in Your Neighborhood?

by Pat Craven

TWO YEARS AGO, we released the first three lessons of our award-winning Garfield's Cyber Safety Adventures program. Since then, thanks to Garfield and Dr. Cybrina, more than 30,000 children have learned how to be safe and secure online. While that is a great start, there are over 1.9 billion children in the world, and every day, more and more kids connect to the internet for the first time, unaware of the risks. To ensure that every child is taught how to be a responsible digital citizen, it is time to take Garfield and Friends to the next level, and we need your help.

The positive results we've seen since our launch have fueled the expansion and growth of our programs. Garfield's Cyber Safety Adventures has been shown to improve a child's cyber safety knowledge by 28 percent after only a 30-minute lesson, according a recent study.

Center for Cyber Safety and Education
Garfield's S.A.F.E. Program
Students And Family Education

In addition, the series of lessons was honored with the prestigious *Learning Magazine* 2019 Teachers' Choice Award for the Classroom *(see p. 10)*, demonstrating that the program is something teachers want and love using with their students. Now we just need to get it to them.

There are several obvious hurdles in expanding the program, with money being the biggest. This is why we are launching Garfield's S.A.F.E. (Students and Family Education) Program for students and families.

No matter what part of the world you call home, funding for innovative and vital school programs like cyber safety is sparse. Schools struggle to meet their everyday needs and often don't have the money or vision to invest in a new program.

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

The S.A.F.E. program is a way for companies (like yours) to get involved and make a difference in the lives of children in your community.

I'm often asked why we charge for the Garfield program when all our other resources at www.IAmCyberSafe.org are available for free. The reason is simple: We have to pay to produce and print them. We are simply passing on that expense. The Garfield kits are *not* a fundraiser for the Center. The cost of one Educator's Kit is US$65, and it covers 30 students, meaning the cost per child is just US$2.17. *Never* has a school or teacher told me that cost is too high. In fact, their reaction is the opposite. The typical feedback we get is, "That's all it costs?!" The product is more valuable than the price, and educators know that. The problem is they often do not have any money to fund this kind of education, no matter how inexpensive, ideal and vital the program may be.

So, how do we overcome these challenges? With your creative help. Go to our website—https://iamcybersafe.org/corporate-responsibility/—to learn about ways that your company can easily get involved in the S.A.F.E. program. Then, let us know how we can help you educate and persuade your leadership by emailing us at center@isc2.org. Several (ISC)^2 members have had success securing community or corporate support. We can do the same for you and help customize a program for your specific community or organization. We'll also make sure your community or company is properly recognized. We have the mechanisms in place. We just need you to get the ball rolling in your spheres of influence. Remember—only you can make the cyber world safer for everyone. ■

RETURN TO CONTENTS

(ISC)^2® community ▮▮▮ SHARING INSIGHTS FROM BUZZWORTHY THREADS

Join the (ISC)^2 Community ›

Highlights from Recent Discussions on the (ISC)^2 Online Forum

The (ISC)^2 Community has more than 20,000 cybersecurity professionals connecting, sharing knowledge and offering solutions in the online forum. *InfoSecurity Professional*, in partnership with the Community's administrators, presents a few of the more buzzworthy threads. Note that the questions and responses may have been edited for clarity and brevity.

QUESTION:

What's the latest in blockchain security?

Does anyone have any information or some sort of nugget on blockchain security or tips on blockchain security hygiene?

—Submitted by Adesoji

SELECTED REPLIES:

Are you talking about implementing a private, public or hybrid blockchain?

If it's private, you're talking about all the standard protective measures applied to your most critical systems along with proper crypto key management.

If it's public, what you are talking about is trusting a public consensus. There is an assumption in the public blockchain implementations that the participants doing the "mining" or keeping the ledger are all altruistic. However, it's theoretically possible to attack the blockchain by overwhelming it with unaffiliated zombies (any group, such as a mining club, that can perform 51% of the transactions causes the chain to fail).

Hybrid public/private systems introduce vulnerabilities into the whole system from the vectors present in the respective parts.

—Posted by Baechle

Blockchain is still in its infancy; I am not sure which part of the technology is more vulnerable. The blockchain itself seems to be secure by default, but the reported issues are mostly related to the key security management.

—Posted by Chuxing

Blockchain lacks enterprise security frameworks and associated controls, rather like the chain of trust, including that of public key infrastructure (PKI). You need to look under the hood and simply ask the questions. Click here for more information.

—Posted by Caute_cautim

Find this complete and updated thread here.

QUESTION:

What are good cyber resume service options?

Current CISSP holder here, with a general career question. I am fortunate to be currently working within the cybersecurity field and interested in your feedback regarding resume preparation services. Not looking to make a job change; however, would like to update my resume, LinkedIn, etc.—some updating is long overdue.

Realize that many will note the best job is one done yourself and there is something to be said for this. That said, does anyone have recommendations for resume services which specialize in the cyber market?

—Submitted by RWBenoit

SELECTED REPLIES:

What most people fail to do when building a resume is to look at the job announcement, see where their experience fits and then put the required experience in their resume. "Responsible for doing scanning" doesn't always mean you performed scanning. If you did scanning and the job duties say scanning, then say so.

For executive management positions you need to show leadership and savings gains/productivity increases you were personally responsible for. How you led teams through tough times. How you accomplished much with very little resources. How you can step in, if needed, and lead your team in a direction, and then be able to get out of their way.

—Posted by CISOScott

I have four versions: a short (2 sides of A4) version that is tailored for each role applied for; a medium resume (5-6 sides) that expands on experience and training; a long version with full information (7-8 sides) that I use to jog my memory at an interview, not to hand out; and finally my LinkedIn profile, which I keep aligned to my short resume. I have produced versions for cybersecurity management, consultancy and architect when applying for specific roles.

—Posted by CEMyers

A page filled from margin to margin with dense text is just too hard to read and will likely get no more than a brief scan before getting placed in the "no" pile. The reader's eye should be drawn to the key points of your story; frame those parts with white space, use an easily-read font. And most of all, don't make the reader exert undue energy to find out why you are the right candidate for the job!

—Posted by StevenJ6052

Find this complete and updated thread here.

RETURN TO CONTENTS

(ISC)²

SECURE SUMMITS / 2019

#ISC2Summits

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

Washington Hilton Hotel
Washington, D.C.

April 23-24, 2019

Register Now

(ISC)² Secure Summit DC unites the most capable minds in cybersecurity for two days of insightful discussions, workshops and best-practices sharing. As a security leader, please join us to address the greatest challenges while learning new and effective approaches that will prepare you to protect your organization and advance your career.

WHY ATTEND?

» Secure your place among cybersecurity leaders in government, military, industry and academia

» Become a more well-rounded, focused and effective practitioner.

» Earn up to 18 CPEs

Register by **February 1**

Secure your place at (ISC)² Secure Summit DC today.
Early bird registration ends February 1, 2019

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

ENRICH. ENABLE. EXCEL.