TIPS FOR HARDENING MULTI-CLOUD ENVIRONMENTS

InfoSecurity PROFESSIONAL

MARCH/APRIL 2021

Reining in IoT Risks

Securing Cloud Endpoints

Dialing in Smishing

(ISC)² A Publication for the (ISC)² Membership

TAKE YOUR CHILD TO WORK DAY
with GARFIELD VIRTUAL

Even in this new work environment you can still have Garfield join in your company's Take Your Child to Work Day activities. Garfield Virtual is a fun way to entertain and educate your employees' children on how to be safe and secure online.

10 YEARS 2011- 2021

CENTER FOR CYBER SAFETY AND EDUCATION

IAmCyberSafe.org/GarfieldVirtual
or email at Center@isc2.org

CONTENTS ▪ MARCH/APRIL 2021 ▪ VOLUME 14 - ISSUE 2

Managing cloud endpoints can be difficult but is doable with the right approach.

PAGE 26

FEATURES

Cover illustration by Jeff Mangiat

Illustration (above) by Raul Allen

DEPARTMENTS

LEARN HOW TO EARN FREE CPE CREDITS

Cybersecurity is Only as **STRONG** as its WEAKEST Link

The cybersecurity of your organization can be thought of as a chain. And every chain is only as strong as its weakest link. How strong are the links in your organization's cybersecurity?

Stronger Cybersecurity Starts with CISSP

CISSP certification arms your employees with the expertise to design, engineer, implement and run a premier information security program. Make your people your greatest strength and protection. Certify them with CISSP.

(ISC)² Why It Is Important to Have Qualified Cybersecurity Professionals On Your Team

The Definitive Guide for Cybersecurity and Business Prosperity

More than 50% of the world's population is now online[1]. Approximately one million people join the internet[2] each day, while two-thirds of humanity own a mobile device[3]. What is known as the Fourth Industrial Revolution (4IR), is already bringing tremendous economic and societal benefits.

Smart technologies have enormous potential to improve both human life and the health of the planet. For example, satellite-based applications can aid rural farmers to irrigate their crops efficiently[4]. Prosthetics can be 3D printed. Autonomous vehicles can be employed by the elderly to support better mobility. The Internet of Things (IoT) can even help to lower CO2 emissions[5] by optimizing energy consumption and reducing traffic congestion.

However, many new challenges and risks have also surfaced. Cyberattacks have become a common hazard for individuals and businesses. The World Economic Forum Global Risks Report 2020[6] ranks them as the seventh most likely and eighth most impactful risk, and the second most concerning risk for doing business globally over the next 10 years.

The need for strong cybersecurity is apparent.

CISSP® Certified Information Systems Security Professional

An (ISC)² Certification

Get The Definitive Guide for Cybersecurity and Business Prosperity

Become CISSP Strong

EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

Don't Call Us; We'll Call You

IF YOU OWN A PHONE—any phone—eventually you start getting vished. These phone calls and voice messages appear to come from trusted numbers in an attempt to gain sensitive information. These scams really ramped up once we all were at home and felt compelled to answer unknown or local numbers that may belong to co-workers, clients or prospective employers.

One of this issue's features takes on this topic. While reading it, I keyed in on a warning that any new policy or protocol to curb vishing and number spoofing could also impact legitimate business operations. I immediately thought of such a staple: cold calling.

No one likes cold calling. No one. But if you work in certain fields, like sales and marketing, you know it's a part of the job. And if you work in IT, you should know how sales and marketing functions influence your security posture. Know too that an inability for sales to do comprehensive outreach limits efforts and, ultimately, revenues, which eventually trickles down to resource reductions.

We're now so conditioned to expect robocalls that we usually let any unsolicited or unanticipated call go to voicemail as a screen. But that hasn't stopped Google Business from hounding me daily about lost opportunities (despite call blocks) or to hear a live voice allegedly from Microsoft alerting our all-Mac shop that they've detected serious issues with our operating systems.

I unlisted a landline years ago after discovering the number's previous owner had absconded with a lot of people's money and everyone thought I was her just using a new alias. I now alert people ahead of time, regardless of which phone number I use, when to expect a call from me no matter how it shows up on caller ID.

Many of us now ignore calls from all but select family, friends, co-workers and service providers. That strategy worked for me until one day a phone number from my old area code popped up on my personal phone and I let it go to voicemail. The caller hung up and tried once more. This time I picked it up, heard initial silence and hung up believing it was another voice-activated vishing call. I thought nothing of it until months later when an old friend I hadn't talked to in years died. That mysterious call had been him wanting to say goodbye. He died thinking I didn't want to hear from him, when, really, quite the opposite was true. Yes, unsolicited phone calls can be annoying, even dangerous. Sometimes, though, they carry unintended yet painful consequences. ●

Photograph by Louise Roup

Anne Saita lives and works in San Diego. She can be reached at asaita@isc2.org.

CONTRIBUTORS

Matt Gillespie is an independent technology writer working out of Chicago. In addition to cybersecurity, he's most recently focused on multi-cloud computing, machine learning, IoT, IT Ops, analytics, HPC and software-defined infrastructure. He can be found at www.linkedin.com/in/mgillespie1/.

Óscar Monge España, CISSP, CCSP, is a seasoned information security professional with more than 17 years of experience. He currently works as a security solutions architect for Rabobank, helping shape the security monitoring direction for both on-premises and cloud and its technology integration.

A trio of CISSPs from Grand Canyon Education in Phoenix round out our roster of authors this issue. CISO **Mike Manrod**, IT Security Manager **Daniel Addington** and Senior Telecommunications Engineer **Ryan Mauldin** collectively have decades of strategic and operational IT experience that they are eager to share with colleagues.

Did the 1980s toy and cartoon series Transformers once capture your imagination? This month's cover illustrator, **Jeff Mangiat**, created the original box art for toymaker Hasbro. Mangiat has illustrated in a photo realism style for national magazines, advertising, book and product art industries. His new graphic style depicts a cowboy reining in IoT icons—all with a nod to Western-style art. Mangiat was also the illustrator for our 2019 award-winning article "Beyond Blockchain Hype."

CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

EXPERT SECURITY

to Command the Cloud

Gain more credibility, recognition and versatility with the CCSP certification. Considered the industry's premier cloud security certification, the CCSP broadens your operational knowledge beyond vendor-specific platforms, differentiating you as a leader in cloud security architecture, data security and infrastructure. As a CISSP, you meet all CCSP experience requirements and are immediately eligible to sit for the exam. Elevate your skill set to realize…

- **Instant differentiation** as an authority figure on cloud security, proving proficiency to keep up with new technologies, developments and threats.
- **Unique recognition** for achieving the highest standard of cloud security expertise.
- **Enhanced acumen** to stay ahead of cloud security best practices, evolving technologies and mitigation strategies.
- **Versatility** to apply knowledge and skills across a variety of cloud platforms.
- **Career advancement opportunities** by expanding into cloud services or moving into more strategic roles.

CCSP was just named **"The Next Big Thing"** by Certification Magazine!

CERTIFICATION MAGAZINE

2021 TOP CERT

CCSP

(ISC)²

THE NEXT BIG THING

The cloud allows businesses of all sizes to increase efficiency, agility and deployment speed. But security concerns remain high, especially with the accelerated shift to remote work environments. Now, more than ever, companies need expert security professionals, like you, to command the cloud. Dive in now.

Lead the Way ⊳

InfoSecurity PROFESSIONAL

A Publication for the (ISC)^2 Membership

(ISC)^2® INSPIRING A SAFE AND SECURE CYBER WORLD

isc2.org community.isc2.org

READ. QUIZ. EARN.

Earn Two CPE Credits for Reading This Issue and Taking the Online Quiz

In order to earn the two CPE credits, you must pass the issue quiz. Please provide your name and (ISC)^2 member number so that we can award the two CPE credits to your account. This typically takes up to 15 business days to be added to your account.

https://www.isc2.org/InfoSecurity-Professional/Magazine-Archive/Quiz/March-April-2021

Learn about more opportunities to earn CPE credits.

ADVERTISER INDEX

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

InfoSecurity Professional is produced by Twirling Tiger® Media, 10 Brassie Way, Mashpee, MA 02649. 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. ©2021 (ISC)^2 Incorporated. All rights reserved.

(ISC)^2 MANAGEMENT TEAM

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

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

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

MANAGER, MEMBER COMMUNICATIONS
Kaity Pursino
727-683-0146
kpursino@isc2.org

COMMUNICATIONS COORDINATOR
Dimitra Schuler
727-316-9395
dschuler@isc2.org

EDITORIAL ADVISORY BOARD

Brian Alberti, (ISC)^2

Anita Bateman, U.S.

Felipe Castro, Latin America

Brandon Dunlap, U.S.

Rob Lee, EMEA

Jarred LeFebvre, (ISC)^2

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

TWIRLING TIGER MEDIA MAGAZINE TEAM

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

ART DIRECTOR, PRODUCTION
Maureen Joyce
mjoyce@isc2.org

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

How Did Continuing Cybersecurity Education Stand Up to the Pandemic Pressure Test?

BY DR. CASEY MARKS, CHIEF PRODUCT OFFICER AND VICE PRESIDENT, (ISC)²

To say that last year was unexpected would be an understatement of generous proportions. Almost overnight, organizations migrated their operations to remote work environments and canceled travel budgets for their staff. Cybersecurity professionals were faced with the task of seeking out continuing education opportunities online in the wake of event cancellations throughout the year.

Dr. Casey Marks is chief product officer and vice president of (ISC)². He can be reached at cmarks@isc2.org.

Looking back at how our own continuing education processes and offerings withstood the unique challenges of a global pandemic, we are now better prepared for whatever comes in the future.

Fortunately, the shift from in-person to online learning did not catch us unprepared. While we did need to make some changes to accommodate remote activities, many of the tools were already in place to do so. (ISC)² had foreseen a globalized world in which much of its educational product catalog would eventually be delivered virtually, and we had been gradually moving that way already.

The launch of the Professional Development Institute (PDI) in 2019 meant that we already had a library of more than 30 on-demand courses available to support our members' continuing professional education needs at a time when in-person events and other learning opportunities were not accessible. Throughout 2020, we added more course material and to date more than 75,000 courses have been completed, with a value in excess of U.S. $20 million.

Additionally, our official training courses were available digitally through our Official Training Providers all around the globe, enabling exam candidates to continue their preparation throughout the year. Many of our members are now pursuing additional certifications, including the increasingly popular CCSP and CSSLP.

Throughout 2020, we added more course material and to date more than 75,000 courses have been completed, with a value in excess of U.S. $20 million.

One of the biggest continuing education opportunities we offer each year is our annual (ISC)² Security Congress. When it became clear that holding a physical event would not be possible in 2020, we examined some of the informal learning elements of our award-winning webinar program in order to transform our event to a fully virtual one. It took a lot of ingenuity to reimagine the event, stand up a brand new online platform and deliver the type of conference our members are accustomed to, but the end result was wildly successful. Attendance more than doubled from the previous year, and the engagement and feedback were outstanding.

If anything, 2020 highlighted the robust capacity of (ISC)² learning opportunities and showed us that we are on the right path for continuous delivery now and in the future. ●

(ISC)²

40+ Courses
120+ CPE Credits
FREE
Member Benefit

Seeking more accessible ways to keep cybersecurity skills sharp and knowledge refreshed? (ISC)² Professional Development Institute (PDI) has you covered with the flexibility of online, self-paced courses. Dive into our portfolio of more than 40 online courses – **FREE for (ISC)² members** and available for purchase by non-members. Build skills and earn CPE credits, no travel required.

Stay on top of your craft with…

- Express learning courses on emerging topics and trends in 2 hours or less
- Immersive courses covering a variety of cybersecurity and IT security topics
- Lab courses that put specific technical skills to the test

Explore FREE Courses

To receive communications when new courses are released, add *Continuing Education and Professional Development* to your preferred communications at isc2.org/connect.

FIELD NOTES

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

5 TIPS FOR HARDENING MULTI-CLOUD ENVIRONMENTS

BY PAUL SOUTH

Jeremy Snyder of DivvyCloud traveled the globe for several years learning how companies large and small secure their multi-cloud environments. The result is a list of recommendations, which were broadcast in an (ISC)² webcast, for how to improve your multi-cloud security posture. That goal is now more important than ever with the mass shift to remote work and bad actors seeking novel ways to infiltrate public, private and hybrid cloud infrastructures accessed from so many more entry points.

1. Gain visibility and define workloads

We've all heard it before, but it's worth repeating: If you don't know an asset exists, you can't secure it. This is why Snyder ranks gaining visibility as a top priority. "There's no way that you can't have that visibility, know whether it's in a secure state, whether it's properly configured, properly secured, etc.," he said. "So, you really have to have visibility in order to gain security around it."

2. Focus on password policies, MFA and logs

Just as with on-premises data centers, all cloud environments demand established and enforced identity and access management systems that incorporate strong passwords, multi-factor authentication and auditable logs. Despite being a best practice, it's one that often gets overlooked.

3. Clean up attack surfaces

While he acknowledged that he has sometimes received pushback about how hygiene impacts cloud security, Snyder points out that when larger firms go to the cloud, they sometimes tend to open their clouds more broadly. For example, a website is established to generate leads during a 30- or 60-day marketing campaign. But when the campaign ends, the site is now an "orphan," a workload no longer serving a useful purpose while spreading an organization's attack surface.

4. Pay close attention to perimeter security

More multi-cloud mistakes come from failing to properly follow the aforementioned recommendations. Once better cyber hygiene is established, along with better visibility and inventory building, it's time to tighten your cloud security perimeter just as you would an on-premises data center. This means closing buckets and locking down ports.

5. Encrypt where needed

While the complexity of a cloud environment can make previously mentioned recommendations difficult, one suggestion that is actually easier in the cloud is encryption. All cloud providers now offer multiple encryption options, depending on workloads and the location of key data assets. This harkens back to earlier points about defining workloads and knowing a firm's data assets. •

Paul South is an Alabama-based freelance writer and regular contributor. An expanded version with more tips appeared in the November *Cloud Security Insights* newsletter. Both are based on a 2020 webcast on the same subject.

Photograph by Getty Images

Transport Layer Security, Threat Intelligence Among Top-Rated (ISC)² Webcasts

If you're curious about what your peers were most interested in last year, we've compiled the top-rated/attended (ISC)^2 webinars for North America and the EMEA regions. All are available on demand through the BrightTALK platform and qualify for CPE credits.

Top Ten Rated 2020 North American (ISC)² Webcasts

Gigamon #1: Transport Layer Security (TLS) 1.3: A New Private World
https://www.isc2.org/News-and-Events/Webinars/Security-Briefing?commid=382117

Gigamon #2: Encrypted Things – Finding Threats in an Obscure World
https://www.isc2.org/News-and-Events/Webinars/Security-Briefing?commid=385629

Gamechanger! What We've Learned (So Far) from the COVID-19 Outbreak
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=398917

Key Insights from CyberEdge's 2020 Cyberthreat Defense Report
https://www.isc2.org/News-and-Events/Webinars/Security-Briefing?commid=397069

Imperva #1: How Automated Attacks Can Derail Your Company's Business
https://www.isc2.org/News-and-Events/Webinars/Security-Briefing?commid=410529

Navigating the Career Maze – Where Do I Go Next?
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=421421

Gigamon #2: What Zero Trust Networking Means for Network Visibility
https://www.isc2.org/News-and-Events/Webinars/Security-Briefing?commid=430277

Gigamon #3: Network Visibility in Today's Complex World
https://www.isc2.org/News-and-Events/Webinars/Security-Briefing?commid=433506

Earn your cybersecurity degree online

Strengthen your skills and gain expertise to help you succeed.

worldcampus.psu.edu/isc2

BEST ONLINE PROGRAMS
U.S.News & WORLD REPORT
GRAD COMPUTER INFORMATION TECHNOLOGY
2021

PennState World Campus

A world of possibilities. Online.

Your Data Held Hostage: Understanding the Extensive Ransomware Threat
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=443840

The Infinite Variety of Phishing Attacks and the Security Controls to Address Them
https://www.isc2.org/en/News-and-Events/Webinars/ThinkTank?commid=451089

Top Ten Rated 2020 EMEA (ISC)² Webcasts

Maximizing the Value of Threat Intelligence
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=450938

Ransomware: New Variants and Better Tactics to Defend and Defeat These Threats
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=440633

Is Encrypting Everything a Good Idea?
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=436867

Managing Shadow IT Realities with a Remote Workforce
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=425016

TLS1.3: Two Years On
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=405854

Minimizing Security Impacts of a Growing Remote Workforce
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=396642

Encrypted DNS: Friend or Frenemy?
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=388560

10 Ways to Harden Your Multi-Cloud Security Posture
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=431552

How to Get the Most Out of Your Security Investments
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=433272

The Industrialization of Cybercrime and Evolution of Cybercrime Syndicates
https://www.isc2.org/News-and-Events/Webinars/EMEA-Webinars?commid=446997

If you trust a third party with your end-of-life data, be prepared to pay the (staggering) cost.

Organizations are liable for data breaches caused by their third party ITAD vendors. There have been countless instances of third party negligence with regard to data disposal, and the resulting costs are staggering — millions of dollars in lawsuits and fines, as well as legal fees, administrative costs, and lost consumer confidence.

NSA EPL LISTED
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA
FOR CLASSIFIED DESTRUCTION

The answer is to destroy end-of-life data in-house using high security data destruction equipment. ***In business since 1967, SEM has earned a distinctive reputation as the industry leader and trusted source for all things data destruction***. Our paper and IT shredders, disintegrators, crushers, and degaussers can be found throughout the DoD and Intelligence Community, US Embassies, US Treasury, and countless other government agencies, as well as in security-focused commercial organizations and data centers worldwide.

SEM®

NSA/CSS Listed | NIST 800-88 Compliant
Low to High Volume | Office or Industrial
Custom Solutions for Complex Environments

800.225.9293 | www.semshred.com

Q&A

HOW I GOT HERE

A MID-COURSE CORRECTION LEADS TO NEW GOALS

INTERVIEWED BY DEBORAH JOHNSON

Katia Dean, system engineer and career coach, received the 2020 (ISC)² Rising Star Professional Award

What were your earliest interests that led you to the tech world?

When I was younger, my mom always had me in some kind of engineering or educational program in the summer. I knew that I was very analytical, structured, and liked to work on projects to stimulate my mind. However, in college, I was weak in math and science. I had a professor tell me that I needed to give up. Despite that advice, I was able to graduate with my engineering degree.

What led you to shift your career focus from electronic engineering to cybersecurity?

I had moved from Cleveland, Ohio, to Lexington Park, Md., where my dad lived and obtained my first job as a system test engineer. I volunteered at a STEM-ING (STEM-Inspiring the Next Generation) event for middle school and high school girls. The workshops on cybersecurity sparked my interest, so I searched out master's programs. A friend recommended the University of Maryland University College; I went there and earned my master's degree.

What were/are some of the struggles you faced in your career that led you to write your book and start your website?

The main struggle was being laid off for nine months. Despite having six years of experience and two STEM degrees, it was difficult finding employment again. I started to blog about my job-searching experience, what I learned from dealing with various recruiters, documenting the interview process and writing down goals. Even though I was going through a storm of my own, I was assisting other people in their careers. That kept me sane and helped me turn my negative situation into a positive experience.

You talk about the strong mentors you've had. How did they help you?

Having a mentor in your field will help you build confidence. During my graduate studies, I had a professor, a Black woman. This was the first time in my career that I saw someone who looked like me. She instilled in me that I had transferable skills to get into cybersecurity. Another mentor has assisted me throughout my career with various speaking engagements and building my personal brand.

What's next for you in both your cybersecurity and coaching endeavors?

Whatever the universe has for me will be a major blessing. ●

KATIA DEAN

With a 2013 bachelor's degree in electronic engineering from Cleveland State University, and a position as a system engineer, Katia Dean decided to shift focus to cybersecurity. She earned a master's degree in cybersecurity technology 4.0 from University of Maryland University College in 2017 and is currently a system engineer at AnaVation LLC. She founded a website and blog, www.Katiascylife.tech, and has written *The Struggle is Real: A Blueprint to Excelling into the Cybersecurity Discipline* to help others build their careers.

CONTENTS

RECOMMENDED READING

Suggested by **LARRY MARKS**, CISSP, CISA, CISM, CFE, PMP, CRVPM, CRISC, CGEIT, ITIL, CDPSE

Third Party Risk Management: Complete Self-Assessment Toolkit

BY GERARDUS BLOKDYK
(The Art of Service, 2020)

To promote best practices, the authors have created a useful tool to ensure that a user has evaluated the KPIs and risks of their program.

TO ASSIST ORGANIZATIONS in developing a third-party risk prevention program, The Art of Service, an Australia-based management consulting firm, has produced a comprehensive guide. *Third Party Risk Management: Complete Self-Assessment Toolkit* identifies the tools needed to implement a third-party vendor risk program. It includes a detailed checklist and a self-assessment tool scorecard. The checklist is organized by listing the key steps of identifying and controlling risk: recognize, define, measure, analyze, improve, control and sustain.

Firms that already have a risk management system will benefit from the detailed tactics that can prompt further evaluation of a third party or project. The 665 questions offered in the checklist can be expanded to help a firm evaluate the maturity of its third-party program. Not covered are contract and other legal issues involving business with third parties. But the book provides the guidance to find the answers to these questions.

Third Party Risk Management is high level and may be supplemented with other guidance such as onboarding a cloud provider. The controls and processes are the same, it's the tactics and implementation that will differ. To promote best practices, the authors have created a useful tool to ensure that a user has evaluated the KPIs and risks of their program. This is a hefty book with a hefty price tag. However, this is one of the most unique and valuable tools that I have seen. ●

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.

CISSP RECEIVES 2020 DOD DIGITAL MODERNIZATION AWARD

Mark Santaw honored for creating criminal data automation tool

Mark Santaw, CISSP, Chief Information Officer, U.S. Army Criminal Investigation Command

Photograph by Ronna Weyland, U.S. Army

MARK SANTAW, CISSP, recently received one of three individual 2020 Department of Defense CIO Awards for creating a tool to automate the importation of electronic criminal disposition data from military, state and federal law enforcement agencies to the FBI. That data currently is used as part of nationwide federal criminal history and weapons prohibition background checks.

Santaw, who earned his CISSP in 2003, is the Chief Information Officer for the U.S. Army Criminal Investigation Command. He was commended for developing a DOD cybersecurity-compliant 1MB system-agnostic tool that enables law enforcement agencies to easily convert 10,000 offender entries at a time into the proper format—within seconds. The same task previous took 15 minutes per offender. This more modern process has saved more than 20,000 manual processing hours across DoD Law Enforcement thus far. ●

CONTENTS

CHAPTER SPOTLIGHT

(ISC)² SINGAPORE AND JAPAN CHAPTERS ORGANIZE SUCCESSFUL VIRTUAL SUMMITS

Secure Singapore draws 130 attendees to Saturday half-day event

(ISC)² SECURE SINGAPORE, which in the past was held in conjunction with Singapore's GovWare conference during the Singapore International Cyber Week, went from a sponsored in-person event to an all-virtual, standalone one on a shoestring budget. The (ISC)² Singapore Chapter's executive committee and organizing team were up to the challenge.

The half-day Saturday date let members attend without taking time from their busy schedules. The program was compressed to a half day and funded only by a small fee collected from each registration.

The conference kicked off with opening addresses by (ISC)² CEO Clar Rosso; Singapore Chapter president Victor Yeo; and guest of honor Melvin Yong, Assistant Secretary-General of National Trades Union Congress (NTUC) and a member of Parliament for Radin Mas SMC. The remainder of time was spent in town hall–style panel discussion segments.

Although this meant members couldn't interact and catch up in person, the virtual event also meant more members could attend since there were no physical constraints. In the end, 130 people attended the chapter's first major virtual event.

(ISC)² CEO Clar Rosso (below) was among those to open the Singapore Chapter's virtual summit.

Secure Singapore 2020

Welcome Address

Clar Rosso, (ISC)² CEO

Among the panel discussions:

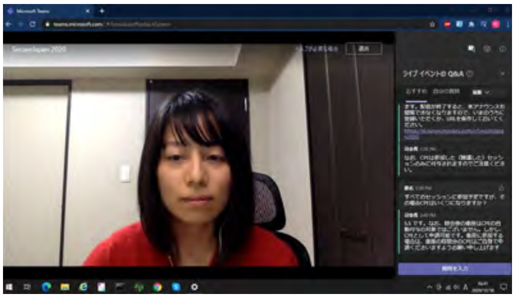
- *Quantification, Measurement and Prioritization of Technology Risks and Investment*, facilitated by Paolo Miranda, the Singapore Chapter's Volunteers Director and Associate Director at KPMG. The panel members consisted of Keyaan Williams, Founder and Managing Director, Cyber Leadership & Strategy Solutions, LLC; Dr. Meng-Chow Kang, Head of Security Assurance, Asia Pacific and Japan, Amazon Web Services; and Neha Malhotra, VP, Cybersecurity Program Manager, Credit Suisse. She's also the Communications Director of the Singapore Chapter.
- *Safer Cyberspace Masterplan 2020* from the Cybersecurity Agency of Singapore (CSA) was facilitated by the Singapore Chapter's Vice President, Garion Kong. The panel members consisted of Gwenda Fong, Assistant Chief Executive, Cybersecurity Agency of Singapore (CSA); Huang Shaofei, CISO, Land Transport Authority (LTA) of Singapore; and Victor Yeo, Regional Director/GM (international government) at BAE Systems Applied Intelligence.

Overall, the town hall format worked well for the attendees, based on the positive feedback the chapter received in post-event surveys.

Japan Chapter acquires 17 new members through its virtual event

The (ISC)² Japan Chapter's biggest event, Secure Japan 2020, drew 300 attendees to the eight-hour virtual event in mid-December. The

CONTENTS



Fumiko Noma, CISSP, (ISC)² Japan Chapter President, moderating Secure Japan 2020.

chapter also acquired 17 new chapter members from the free event, which was sponsored by Tokio Marine & Nichido Risk Consulting, NTT Security, Global Security Experts (GSX) and NRI Secure Technologies.

The video conferencing infrastructure was operated by Yurika Kakiuchi, CISSP; Hiroyuki Komachi, CISSP; Hiroko Oogane, CISSP; and Rui Kanazawa, CISSP. Because of so much support, the event was successful at a minimum cost.

Secure Japan 2020 kicked off with opening addresses by new (ISC)² board member Eiji Kuwana, CISSP, and (ISC)² CEO Clar Rosso, whose speech and some of the other presentations were delivered with Japanese subtitles.

Presentations included:

- International Cyber Crime Investigation - The Days of Distressing, presented by Naruomi Ebitani, CISSP
- Overview of U.K. Cyber Essentials Scheme by Emma Philpott MBE
- Cyber-Physical Fusion and Cyber Security by Junpei Watase
- Japan Cyber Security: Protecting the FinTech Epicenter before the Olympics, a roundtable discussion led by Felix Beatty, CISSP, CCSP, and colleagues Amit Ranjan and John Ghanotakis
- Cyber Risks that Japanese Companies May Face in the Future and Trends in Visualization - The Cyber Insurance Developer Speaks Out, delivered by Daisuke Kyogaku
- Observing the Movements of Cyber Criminals - Anti-Ransomware by Yu Arai, CISSP
- The Future of Familiar Problems Everywhere, led by Hiroshi Aido, CISSP

Secure Japan 2020 was voluntarily supported and operated by numerous team members. The chapter is grateful to all the volunteers who helped to ensure this virtual event was well attended and valuable for attendees. ●

Naruomi Ebitani, CISSP, American Express International, during his live studio presentation.

Keiichiro Oguma, CISSP, (ISC)² Director of Business Development, Japan, during his live studio presentation.

Yu Arai, CISSP, NTT Data, during his live studio presentation.

MEMBER'S CORNER

BUILD TRUST IN PRODUCTS THE RIGHT WAY—THE SECURE WAY

BY WILL RAINWATER, CISSP

In my 31 years in IT across multiple verticals including government/military, financial services and healthcare, I have seen a similar pattern following a massive data breach. First comes the headlines and then an email or letter from a company's CEO expressing a commitment to do better by its customers.

We don't have to keep repeating this pattern. We could shore up a lot of these ongoing issues by having a company's leadership and management provide more than lip service to creating tamper-free solutions by making cybersecurity a top priority across the entire corporate spectrum.

Let's first recognize that a cornerstone of capitalism is filling a need, but that need also comes with the expectation that the solution to that need does not cause harm or facilitate harm to the consumer. I think that concept sometimes gets lost, or is at least less visible, in this era of globalism, immediate gratification, and intense pressure to generate profits quickly and frequently.

I believe we are on the precipice of an incredibly scary time where individual privacy is suffering despite the rise of regulation or government intervention. From my vantage point, too many companies appear to still not understand the cost savings in relation to bad press and class-action lawsuits when products are built securely.

Deadlines put into place at every step of the systems development process are the biggest barrier to secure software and hardware, hands down. If deadlines were dropped and security was truly a focus, where full spectrum vulnerability testing was performed at every step in the lifecycle, we would not be having the issues we do. Time could be spent covering all aspects of both functionality *and* security instead of just functionality alone. Developers must get past this "get it done so we can get to market ASAP" (and make a profit sooner) mindset and instead embrace the "it will be released when it is ready" mindset. Doing so means we, as a society, would see fewer issues with privacy, fewer data breaches, and less cybercrime because it would no longer be profitable for the criminals.

Will Rainwater, CISSP, is an Information Technology Director. He can be reached at wrainwater@levihospital.com.

Sure, there are costs associated with that, especially in the short term. But if your product is truly secure, can protect the data it is designed to protect, and perform the functions to solve the need *and* the expectation, then the profits will come.

Everyone who buys a product (consumer- or enterprise-grade) expects the product to work as advertised, as well as protect them from harm. What no one should expect is for it to *remain* secure forever. I don't know of anyone in the IT community who has that expectation. Security vulnerabilities pop up by the second. You have to adapt, and that also costs money. But the ongoing costs of maintenance would be greatly reduced if software makers did it right the first time, so you only have to cover changes in the security environment moving forward, not vulnerabilities known two decades ago.

Deadlines put into place at every step of the systems development process are the biggest barrier to secure software and hardware, hands down.

"Do it right the first time" should be the new mantra, and it should be spoken and honored and extended to everyone in the company, especially management. The systems development lifecycle does not just include programmers, testers and quality assurance personnel. Your entire management infrastructure has a hand in the responsibility of ensuring that their product does no harm or does not facilitate harm.

Moving forward, remember that customer loyalty is a two-way street. We, as customers, will remain loyal to a company if we feel that that loyalty is valued and reciprocated. Transparency and an ethical approach to development are two aspects that have a huge impact on long-term loyalty. I cannot speak for everyone, but I have to believe that my opinions are shared by more than just me. You cannot be ethical if you put profits first. You just can't. ●

CONTENTS

SEARCHMORE

Find Threats that are Already in Your Environment

With Long-Term Search, organizations can reduce the time needed to investigate and find threats that are already in their environment.

www.securonix.com
Copyright ©2021 Securonix Inc. All rights reserved. 0121

SECURONIX™

Lights! Camera! Interview!

HOW TO GET THE MOST OUT OF YOUR VIRTUAL NEW JOB DISCUSSION. BY DEBORAH JOHNSON

Interviewing a candidate for your cybersecurity team now relies on virtual communications technology more than ever, primarily thanks to the pandemic. In an April 2020 report, Gartner reported that 86% of 334 human resource leaders surveyed were "incorporating new virtual technology to interview candidates." Cybersecurity pros, while familiar with Zoom meetings and online presentations, may need some guidance to get the most out of a virtual candidate interview.

The nuts and bolts of the candidate's skills can be determined through a resume. But what is the person really like? Will they fit in with the current team? Will they mesh with corporate culture? The camera can make these intangible attributes more difficult to assess.

First, make sure you have the "right technology that's fully functional," says Dan Schawbel, managing partner of Workplace Intelligence, an HR research and advisory firm, in an email exchange. "You should plan for a remote interview the same as you would in person. The interviewer should present themselves the same as in-person. If you don't take the interview seriously, then [the candidate] won't either."

And don't let your environment distract you, he advises. "Look at the camera and not at your phone, which should be turned off. Make sure you're in a quiet place with good lighting."

Next: Get a good "read" on your candidate. "One of the biggest issues we see now that everything's gone remote—we're missing the rapport-building part," says Kris Rides, co-founder and CEO of Tiro Security, a cybersecurity staffing and services organization. "Because, in person, we're better at just talking, a little bit of small talk," he said in a phone interview.

Don't forget traditional interviewing techniques. "Big, open questions can draw out their feelings," Rides advises. "Big questions like 'Where have you found you've been most successful?' 'What did you enjoy most about your job?' [and] 'What do you want from your next place?'"

Rides warns: "Passion is something that a lot of people ask for, but it's an intangible. If their passion is cybersecurity and they've made a job out of it, then they're probably doing bug bounties, they're doing webinars, joining the Cloud Security Alliance, the local (ISC)² chapter, and they're working on a certification they don't need for their job. They are just genuinely interested in it."

The successful remote interview is a combination of reliable technology and positive personal interaction. Robert Half Business offers these tips on its blog:

- Be prepared. Don't try to wing it.
- Test your video conferencing platform (i.e., Zoom, Skype, WebEx, etc.) in advance.
- Have a backup plan to your platform in case there is a problem on either end.
- Find a quiet, well-lit space and minimize distractions (e.g., silence mobile phones).
- Look professional.
- Pay attention to facial expressions and tone of voice.

A good interview is successful whether it's in person or remote. Just because the candidate isn't in the same room doesn't mean you can't discover if they are the right person for your team. ●

Deborah Johnson lives and works in San Diego. She can be reached at djohnson@twirlingtigermedia.com.

CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

Make This Your Year for CCSP CERTIFICATION

Here's Everything You Need to Succeed

You know that preparing for an (ISC)² certification is a BIG commitment. You also know that CCSP will help you stay on top of growing cloud security demands and build critical skills. Maybe you've started studying, but unforeseen challenges interrupted your progress… We get it!

We're here to help you get back on track for success.

Get back on track for success.

(ISC)² Exam Action Plan ▶

(ISC)² | Inspiring a Safe and Secure Cyber World

REINING IN THE Risk

What's at stake in securing IoT's massive attack surface, made up mostly of lightweight devices with few security protections. **BY MATT GILLESPIE**

IoT creates nooks and crannies in your network where the light never reaches. You can't easily see the vulnerabilities there, and it may be impossible to know where to look. →

ILLUSTRATIONS BY JEFF MANGIAT

“Segmentation between IoT and OT is an absolute best practice. They should never be on the same network.”

—John Powell, principal consultant, Optiv

The IoT universe comprises billions of small-footprint devices that are not designed or manufactured to enterprise-grade security standards. Understanding and mitigating the risk requires revisiting what’s on the network, what it’s doing, and whether it should be there at all, for a start.

Devices may appear unannounced and stay hidden, resisting conventional attempts at discovery and monitoring. In its immature state, IoT lacks standardized protocols, which can make a unified view difficult or impossible. Global bodies are developing standards, but finalization and widespread adoption are still far off.

Even when familiar IT best practices are followed, securing environments in the face of these complexities poses new challenges.

IoT DEVICES CAN BE LIKE SNEAKY, SPOILED CHILDREN

The threat associated with IoT devices is often made worse by inappropriate levels of elevated privilege and a lack of control. Those devices may make their way onto the network without notice by IT, especially when they are implemented by business units that don’t suspect the danger.

As with any technology, the potential exists for security to be relegated to the status of an afterthought or ancillary concern. Part of the issue is that IoT devices are often deployed without recognizing that they are network endpoints.

Ken Munro, a partner at Pen Test Partners, describes one such case involving wireless screencasters, which are small-footprint devices that let users cast the displays of their personal mobile devices to large presentation screens. Munro recalls, “We found these little devices also have network ports, and the installers have been going into firms and not just putting in a standalone screencaster; they connected it to the network, too.”

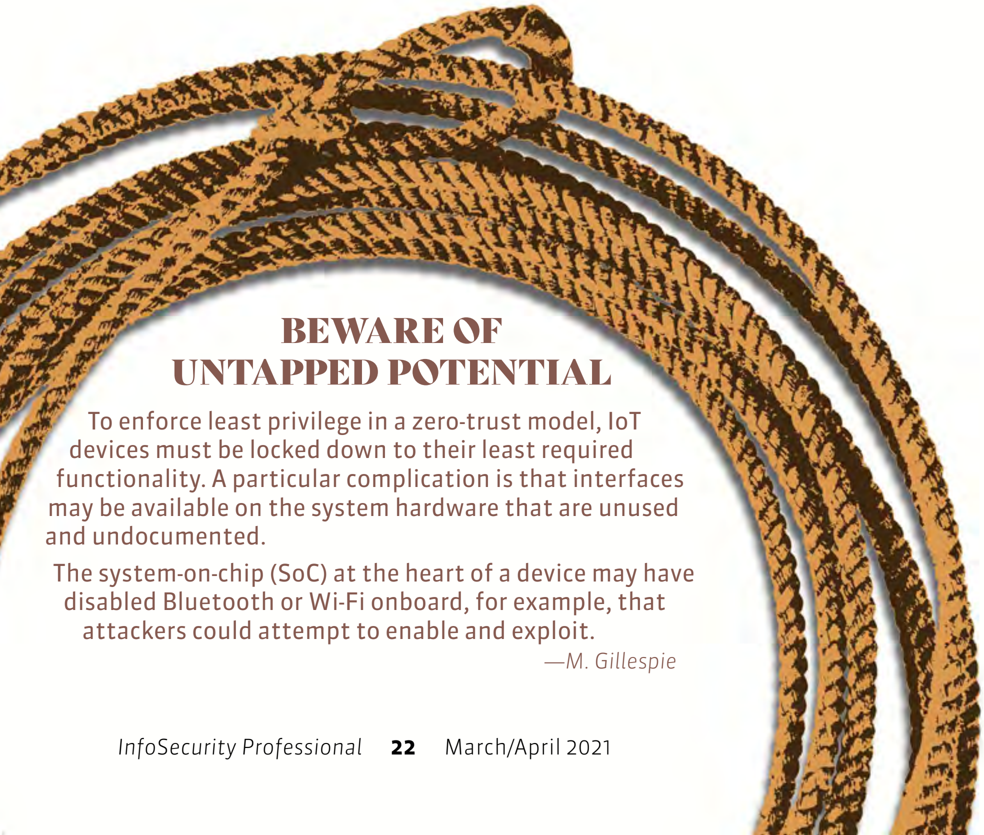
While these screencasters are directly connected to the network, they don’t conform to the firms’ security requirements for network endpoints, and they are typically not manageable by IT. Making matters worse, they may host wireless networks for the devices used with them, offering WiFi that is often left open or minimally secured using intentionally weak passwords for convenience.

A similar example concerns digital signage that displays information such as meeting room schedules drawn from the corporate network. These low-end, rebadged consumer Android tablets often appear in public areas, where an interested party could steal them and make off with a device that potentially has discoverable Active Directory credentials cached on it.

This inadvertent, side-door installation onto the network highlights the necessity of isolating IoT devices, with physical separation or at least on a separate subnetwork. As Munro said, “The first thing to do is keep them off your network to start with.”

John Powell, principal consultant with Optiv, concurs: “Segmentation between IoT and OT is an absolute best practice. They should never be on the same network.”

That necessity is largely because of the limited capabilities of many



BEWARE OF UNTAPPED POTENTIAL

To enforce least privilege in a zero-trust model, IoT devices must be locked down to their least required functionality. A particular complication is that interfaces may be available on the system hardware that are unused and undocumented.

The system-on-chip (SoC) at the heart of a device may have disabled Bluetooth or Wi-Fi onboard, for example, that attackers could attempt to enable and exploit.

—M. Gillespie

IoT devices themselves. Security agents or antivirus, for example, can't typically be installed on an IP camera. So how do you safely allow such a thing onto the network? One source advises, "Don't trust the thing in the first place. This is kind of a glaring poster child for the zero-trust model."

One aspect of that zero trust is to have an intermediary such as a router or gateway between IoT devices and the network. The intermediary acts as the endpoint, and the devices themselves are not on the network. Security controls are applied to the intermediary, which has sufficient resources such as compute and memory that it can conform to the organization's cyber standards.

Another best practice is to lock down the types of traffic allowed to devices. For example, an IoT camera only needs to receive commands such as pan up, pan down, and zoom; only that data should be allowed to flow into it.

Those traffic restrictions are a reflection of the very limited role that the device should play on the broader network.

Rather than using persistent sessions, IoT devices should also be treated as untrusted and potentially hostile entities, with every access request verified and authorized individually. This is particularly true in the large proportion of IoT implementations where the device is physically located in an uncontrolled remote location.

In sum, unlike actual spoiled children, the proper course for IoT devices is to keep them in an environment of zero trust and isolation.

"A lot of the IoT devices that are out there right now have hard-coded passwords, usernames, all of that stuff. The only way that you can really check ... is when you're ready to deploy it."

—Penny McKenzie, cybersecurity engineer, Pacific Northwest National Laboratory

SECURING ELEMENTS THAT AREN'T BUILT THAT WAY

Shortcomings in the security of many IoT devices is baked in at the time of manufacture. "The biggest issue is that these little, small devices are programmed at a factory and shipped. If they're not built with security in mind, then it's impossible to change them later," Powell says.

Indeed, cost constraints and the need to get a revenue-producing offering out the door can lead to corners being cut in security during product development. Many are built without even rudimentary access-control measures.

Penny McKenzie, a cybersecurity engineer at Pacific Northwest National Laboratory, suggests: "The first thing that I would consider before purchasing any IoT device is whether or not ... admin credentials have the capability of being changed. A lot of the IoT devices that are out there right now have hard-coded passwords, usernames, all of that stuff. The only way that you can really check ... is when you're ready to deploy it."

Likewise, many small, inexpensive IoT devices lack the ability to be updated with security patches or other necessary changes. Checking for that capability and understanding how updates are performed is important pre-planning for how future vulnerabilities can be addressed.

Keeping track of these devices and their security states requires mapping their presence and function on the network, a task that is made more complex by the tangle of communication protocols involved. Likewise, detecting Bluetooth communication or RFID tags can be of limited value; they are unlikely to identify the broadcasting device.

Operators are often left with patchy understandings of their IoT environments that can make it impossible to identify and track threats.

In cases where the functionality of IoT devices is limited by not being on the main corporate network, business needs may be at odds with security requirements. In others, the main requirement may be cloud connectivity, either through a gateway to the corporate network or directly to a third party using means such as 5G.

Emerging capabilities for private 5G networks may play into secure IoT deployments, especially for widely dispersed ones such as utility infrastructure or oil fields. On the other hand, the cost and complexity of hosting these networks make it untenable for any but the largest enterprises.

In terms of outside connectivity, McKenzie points out potential differences between passing data to one of the top-tier cloud providers for processing versus a point solution vendor. The latter case most likely has less rigorous security measures in place than the former.

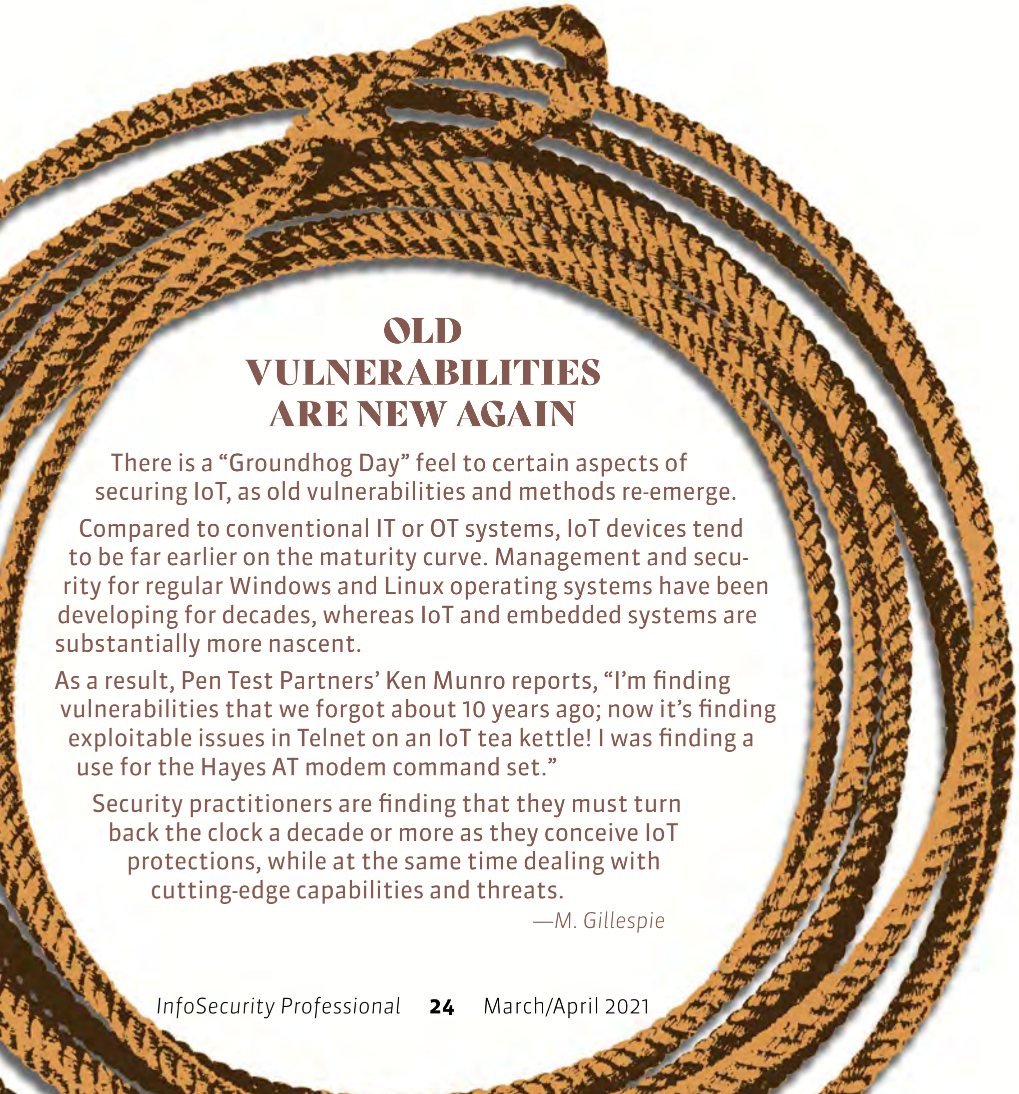
In particular, the major cloud vendors provide integrated sets of solutions that protect data from the device to the edge to the cloud. By contrast, the capabilities offered by smaller vendors may be less comprehensive.

This exposure can have implications for both the privacy and the integrity of the data. And as McKenzie notes, "You get all that information, but the vendor also gets that information … There are no regulations out there to say that it has to be secure."

The need for these data-protection assurances emphasizes the criticality of due diligence, vetting vendors for security readiness. They should be able to provide a detailed description of how they lock down their embedded systems, for example. They should be able to produce (and willing to share) penetration testing reports. They should also be able to discuss security issues they've had in the past and how they handled them.

Ken Munro points out the value of discussing security weaknesses as well as strengths with a vendor: "The companies I respect the most [are the ones] who are honest and admit that they haven't got it completely nailed in the couple of areas they're worried about, but they've got a plan."

Establishing how the vendor positions itself in conversations such as this lends insight about what level of support they can be expected to provide if vulnerabilities or other problems arise. Likewise, building in security considerations at the outset of a project is always preferable to trying to bolt them on later.



OLD VULNERABILITIES ARE NEW AGAIN

There is a "Groundhog Day" feel to certain aspects of securing IoT, as old vulnerabilities and methods re-emerge.

Compared to conventional IT or OT systems, IoT devices tend to be far earlier on the maturity curve. Management and security for regular Windows and Linux operating systems have been developing for decades, whereas IoT and embedded systems are substantially more nascent.

As a result, Pen Test Partners' Ken Munro reports, "I'm finding vulnerabilities that we forgot about 10 years ago; now it's finding exploitable issues in Telnet on an IoT tea kettle! I was finding a use for the Hayes AT modem command set."

Security practitioners are finding that they must turn back the clock a decade or more as they conceive IoT protections, while at the same time dealing with cutting-edge capabilities and threats.

—M. Gillespie

THE IoT SECURITY LANDSCAPE BEYOND DEVICES

The most tangible and distinct part of an IoT implementation is its array of devices, and most discussions of IoT security (including this one) begin there. Notwithstanding their potential vulnerabilities, and the need to isolate them from the rest of the network, compromise of devices themselves is likely not the primary area of concern.

Working outward from the device level, the vast majority are connected wirelessly. Verifying simple measures such as Wi-Fi security and use of the latest versions of drivers and Bluetooth technology should not be overlooked.

The platforms that are used to access data from IoT platforms are a specific locus for vulnerabilities and potential compromise of a broad swath of the environment. The APIs used by those platforms

CONTENTS

to access devices are key components to consider.

For example, some platforms do better than others at enforcing strong passwords, preventing reuse and so on. Trying out your favorite weak password can be illuminating. If the platform accepts “pass1234,” that’s a pretty good indication that additional security concerns will emerge upon deeper inspection.

Beyond enforcing good password hygiene, platform vendors should enforce two-factor authentication for API connections.

Standards and regulatory frameworks are working to catch up with the unmet security needs of IoT as well. California Senate Bill 327 went into effect on the first day of 2020, mandating “reasonable” security features. While this statute is limited in scope, it is part of a larger trend of legislation that is also taking place in the United Kingdom and the European Union, for example.

In conjunction with those legal advances, industry standards are also being developed by entities such as the National Institute of Standards and Technology (NIST) and European Telecommunications Standards Institute (ETSI), among others.

These advances are part of the solution to overcome either unsecure IoT implementations or delay of widespread commercial adoption by businesses because of security concerns. Regulation and assured conformance to industry standards is a necessary step in the maturation of secure IoT.

Munro takes the position that “there is now a strong commercial motivation for IoT vendors to prove that they’re following some third-party standards. And if they don’t, then that’s what we need some regulation for.”

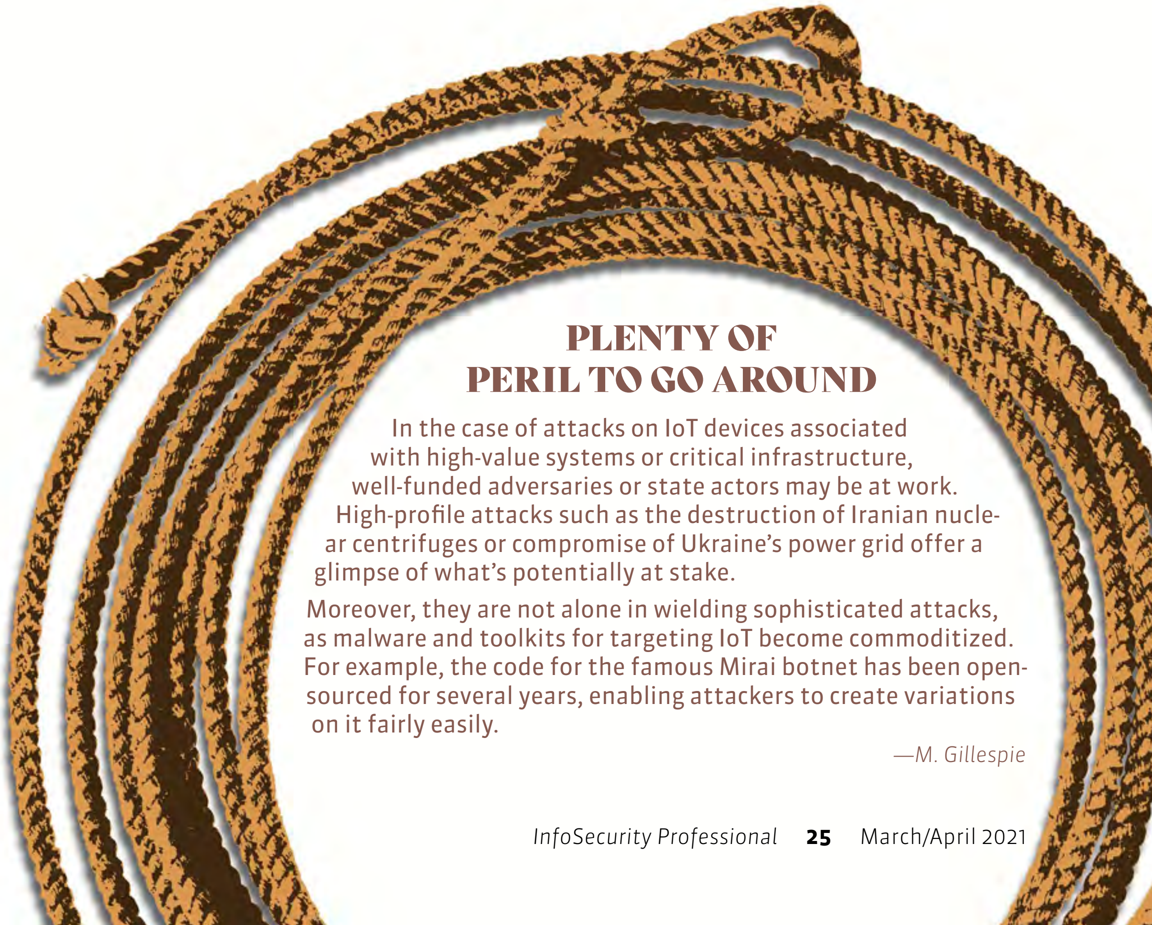
A great deal is at stake, from direct financial losses to opportunity costs from delayed adoption to potential injury or loss of life if the wrong systems are breached.

The good news is that maturing tools, techniques and standards are combining with market forces and regulation to move the industry toward increased hardening of IoT solutions. And not a moment too soon. ●

MATT GILLESPIE is a technology writer based in Chicago. He can be found at www.linkedin.com/in/mgillespie1.

“There is now a strong commercial motivation for IoT vendors to prove that they’re following some third-party standards. And if they don’t, then that’s what we need some regulation for.”

—Ken Munro, partner, Pen Test Partners



PLENTY OF PERIL TO GO AROUND

In the case of attacks on IoT devices associated with high-value systems or critical infrastructure, well-funded adversaries or state actors may be at work. High-profile attacks such as the destruction of Iranian nuclear centrifuges or compromise of Ukraine’s power grid offer a glimpse of what’s potentially at stake.

Moreover, they are not alone in wielding sophisticated attacks, as malware and toolkits for targeting IoT become commoditized. For example, the code for the famous Mirai botnet has been open-sourced for several years, enabling attackers to create variations on it fairly easily.

—M. Gillespie

Virtual Reality

TIPS FOR MANAGING VULNERABILITIES ON CLOUD ENDPOINTS

BY ÓSCAR MONGE ESPAÑA, CISSP, CCSP

ILLUSTRATION BY RAUL ALLEN

ONE OF THE MOST COMMON challenges when securing the cloud is not having full visibility of all resources deployed. This exponentially increases the exposure factor, which could lead to a possible breach.

Six to eight years ago, when organizations started moving to the cloud, the main goal was a smooth transition in order to quickly reap the benefits of cloud: to deploy workloads and reduce capital expenditures. Security came later.

Organizations tried to implement the same controls as on-premises, even the same vulnerability management technology. However, because of the cloud's unique

CONTENTS

characteristics, the technology either was not cloud-oriented, or the information was not as reliable as the technology used traditionally to identify endpoints (IP address or hostname-based). In the cloud were other unique identifiers such as instanceID (AWS), UUID (Azure), Instance ID (Google) and instance-id (Alibaba).

A typical vulnerability management process runs on a recurrent basis within the organization; depending on the criticality of the systems, it can happen weekly, biweekly or even monthly. This would feed the first stage of the VM lifecycle: the vulnerability and configuration assessment. Cloud endpoints' lifespans could be totally different. One could spin a VM for a few minutes/hours/days and terminate it, although if the organization followed the traditional *lift-and-shift* it is most likely following the same rule of thumb as on-premises: a virtual system that lives forever in the cloud and gets patched on a regular basis.

THE DYNAMIC NATURE OF CLOUD NETWORKS

Usually, on-prem vulnerability assessments involve a network vulnerability scanning solution. This approach we're all familiar with. But cloud networks could be very dynamic and carry restrictions, such as cloud vendors that do not allow a network scan without prior approval.

Organizations started considering creative ways to tackle the vulnerability management problem. Some created hub-and-spoke connections between virtual private clouds or virtual networks and would request permission from the cloud service provider to perform their security activities. Others sought industry-leading solution providers to ease the security burden while allowing rapid adaptation of internal processes. This approach alleviated a common pain point: the lack of cloud security specialists on staff as the business defined its cloud vision and built out increasingly complex cloud infrastructures.

As with any other IT activity, there was—and still is—a cost associated with this level of outsourcing. For those that eventually decided they'd get a better return on their investments by building their own clouds, professionals were trained to consume cloud native infrastructure to fulfill the business needs.

VENDOR-BASED VM SOLUTIONS

Lately, we've seen how multiple cloud providers have either come out with their own vulnerability management solution or have partnered with strategic vendors to provide this service as part of their offerings. Such changes in the way vulnerability management is performed in the cloud means:

- More visibility is provided to the business unit and the organization
- Proactive measures can be taken and automated, instead of manually patching or assessing and patching on a regular basis
- A holistic view of information security–related issues can be gained, such as of security events and vulnerabilities

Because we're talking about a multi-cloud strategy, the integration of vulnerability data might be a challenge. There could be a risk of vendor lock-in or differences in how data is consumed and correlated between endpoints. Enabling a cloud data lake might be a good option to centralize overall visibility, and enable the business to act upon collected data while feeding other sections of the vulnerability management process like enforcement, reporting and tracking of issues in an automated fashion. The same goes for other information security areas like incident response, in which, having a background on the vulnerabilities affecting an endpoint could greatly enhance the possibility of a positive outcome of an investigation.

Here are some suggested steps to gain greater visibility.

- Start by identifying which vulnerability management services exist per cloud service provider and the output provided; differences will exist depending on the vendor. Ask yourself: Can it be exported?
- Identify requirements to enable the capability on endpoints. Are agents or specific roles necessary? Both?
- Define the vulnerability information destination bucket and format (if necessary, for consistency).
- Validate overarching vulnerability visibility against reporting endpoints.
- Integrate with organizational processes to act upon collected data.
- Enrich the incident response process with vulnerability information to increase the scope of investigation on incidents.

CREATING A SOUND STRATEGY

Defining a solid vulnerability management strategy enables the organization to adapt its processes faster to disruptive technologies like containers, on which vulnerability management can be performed at the guest OS, container image and code deployed.

How do we tackle vulnerability management container issues?

- Standardize the utilization of images used to develop applications.

- Control which images can be pushed into the container registry and that do not contain either medium nor high vulnerabilities.
- Perform continuous vulnerability assessments when the containerized application moves from development to pre-production.
- Vulnerability management should continue as part of the lifecycle of the application in the production environment.

IoT devices do not fall far from the OS tree. The organization should focus on a baseline to harden these devices (changing default account passwords, for example) and aim to monitor the activities these devices exhibit in the network and its deviation. Cloud-native integrations are being offered by major cloud service providers to ease the burden on the organization and provide visibility on such activity.

Following similar practices as those performed on-premises, it is recommended that the vulnerability management process foresees enabling the organization to identify reactively if their cloud instances are relevant to a vulnerability related to a zero-day based on CVE (Common Vulnerability Exposure) identifiers obtained from open- or closed-source intelligence reports.

Vulnerability management is a ubiquitous process that will continue evolving. It is our job as information security professionals to ensure that processes and people evolve nearly as fast as technology does, while enabling the organization to react in a more agile manner while still maintaining the security posture all along.

How can we do that? Understand that visibility is everything, and the same technology might not be suitable for all use cases. Think beyond vulnerability management and be vigilant about costs and budgets. Finally, never forget that any technology, any vulnerability management system, will fail if you disregard your people and processes. ●

ÓSCAR MONGE ESPAÑA, CISSP, CCSP, is a security solutions architect for Rabobank with a passion for information security and technology alignment to IT business needs. Another version of this appeared in *Cloud Security Insights*.

Galvanize

Focus on the cyber risks that matter most.

ITRMBond streamlines IT and cyber risk assessment activities so you have more insight into your IT risk and compliance posture.

Use automated workflows and harmonized content to quickly start rationalizing IT compliance risk and control environments. Then quantify risk with real-time dashboards and ultimately ensure compliance.

Ready to get more clarity with ITRMBond? wegalvanize.com/infosec

HOW TO DIAL IN VISHING AND 'SMISHING' ATTACKS

BY DANIEL ADDINGTON, CISSP,
MIKE MANROD, CISSP,
AND RYAN MAULDIN, CISSP

Have you la
Confirm your ATM card code
Lose 30 pounds while you sleep
Redeem your complimentar coupon
Rep free
You must act now to redeem this special offer
Urgent Special Alert
Click to update your account information
IRS needs your updated information
Your account has been compromised
Download this free app today

FOR MOST OF US, it's now more difficult than ever to get through a day or week without receiving—let alone screening—one phone call or text message impersonating numbers we are likely to trust. These "callers" may go as far as leveraging open source information to impersonate a trusted number to conduct their phishing or 'smishing' (SMS-based) attacks. Or, they select an area code with direct inward dialing or a prefix that appears local.

Why is this possible? What allows those with nefarious intentions to game the telecom system? And, for organizations, how can these attacks be reined in while allowing legitimate sales and marketing phone calls to continue?

ILLUSTRATION BY RICHARD MIA

Spoofing: So Easy a Manager Can Do It!

OUR INITIAL IMPRESSION when first investigating attacks using spoofed phone numbers was that these were attacks involving some technical complexity. Unfortunately, we could not have been further off base.

Setting up a working POC for spoofing voice calls or SMS text messages is something you can accomplish during a lunch break. For a simple POC, go to https://www.spoofcard.com/ and select a plan for as little as U.S. $10 and simply follow the steps to get up and running.

Once you have a valid account, to make spoofed calls or text messages, you input the number you want to impersonate and it will return a code and a number to dial (many other options are available also, including selecting a voice disguise or a desired background noise). If you want to spoof calls or text messages at scale as attackers do, it may be more economical to setup your own environment.

The best way to prove the importance of protecting against this threat vector is probably to buy a burner phone and prepaid credit card, set up a POC and demo it live in a meeting with executive decision-makers if there is any lingering skepticism. A robocall from a key exec, leaving everyone speechless, may be worth a thousand words.

—D. Addington, M. Manrod and R. Mauldin

In the simplest terms, the issue comes down to a lack of universal validation of the caller source, the "From" header field value, which is fundamentally arbitrary and user-supplied (see RFC 7340).

Voice communication, whether wired or wireless, has a rich history with a legacy extending back much farther than many of the communication frameworks we rely upon today, including the internet and numerous derivative protocols of transmission and trust. Granted, these more evolved frameworks are far from perfect—websites are impersonated, certificates are compromised and the DNS (Domain Name System) is sometimes hijacked. And, this does not even include the myriad ways a legitimate site can be compromised to send users somewhere malicious (e.g., XSS).

That said, their infancy as it relates to the overarching clock of human-capability advancement would presuppose a disadvantage to such technologies. Why is it that one of the more fundamental communication technologies with roots back to the esteemed first phone call in 1876 should be one of the least secure, trusted or evolved trust models of our modern age? Can we trust that "Mr. Watson! Come here, I want to see you" were really the words of Alexander Graham Bell—or, did someone intercept and manipulate that communication?

Of course, it is laughable to think this first communication was manipulated—at that time, there were only two endpoints and one local point-to-point transmission (not to mention, practically nobody else had such capability yet). And, for a long time the voice infrastructure remained relatively trusted, with relatively limited interference.

While the technical barriers to intercept and impersonate communications were low by today's standards, it definitely occurred; however, the relative frequency seemed to be very low. Moreover, such intercepts and impersonations were often sanctioned and authorized. That is not to infer they were always just; instead, it is to suggest that the capability was not ubiquitous and universally exploited on a level with broad societal impact.

A fundamental flaw within telecommunications trust is that the identity of the originator of any specific communication can be self-authenticated, either directly or indirectly.

Eventually, the art and science of exploiting voice communications dawned as a new frontier for the masses with the phreaking revolution started in the 1960s, which later evolved into the substantial problem of telephonic trust we all face each day in our modern age. *(See "Spoofing: So Easy a Manager Can Do It," above left.)*

FUNDAMENTAL FLAWS EASILY EXPLOITED

A fundamental flaw within telecommunications trust is that the identity of the originator of any specific communication can be self-authenticated, either directly or

CONTENTS

indirectly. It is relatively easy to impersonate the number of a caller, for communications delivered via voice or SMS/text. On a larger scale, there are issues with a massive, distributed network of implicit trust, resulting in the ability for large-scale actors with malicious intentions to join the party, so to speak, as a new company with a range of legitimate numbers to use for illegitimate purposes. That said, another implication of this implicit trust required to make the existing blended PSTN, TDM and SIP networks work is the ability for a threat actor to simply lie about the "From" header value to impersonate a number that is not really theirs. This is similar in concept to MAC address spoofing within IP-based networks.

Calling Use Cases and Associated Complexity

THE PRINCIPAL PROBLEM for implementing a trust hierarchy for voice and SMS communications comes down to the complexity and technical debt of the infrastructure, combined with the wide range of use cases that must be accommodated.

For example, it is necessary to account for calls among and between VoIP and PSTN infrastructure following a range of patterns, including pure VoIP, strictly PSTN, and scenarios going from PSTN to VoIP to PSTN and even vice versa. This makes a pure inline/end-to-end trust model difficult, if not impossible.

It seems like it is necessary to have a trust model that exists outside of, and maintaining authority over, the complex range of possible communication scenarios. A useful comparison may be what has been implemented with DMARC for email—if entities are required to declare, own and take responsibility for numbers in a manner that is binding, certified and externally maintained, it would reduce the impersonation risk.

—D. Addington, M. Manrod and R. Mauldin

BUILDING A TRUST HIERARCHY

Upon initial examination, we thought it sufficiently possible to introduce a trust hierarchy similar to one for internet resources. While flaws exist within these systems—vulnerabilities still frequently exploited—billions of users maintain a relative level of trust that allows them to confidently execute web transactions with a certain degree of confidence, from internet posts to high-dollar purchases. Despite persistent problems like phishing, consumers' level of trust in top eCommerce sites seems to be far higher than the trust we have in an unknown inbound phone call or text message.

Of course, we are continuously fixated on the times these internet trust systems fail. It is our job to do so, and the number of opportunities to find flaws seem to be limitless. In any paradigm of security, there is no absolute protection; instead, it is a matter of percentages and relative confidence levels. When a new call comes in, our confidence level (collectively, at least) is very low, compared to the knowledge that if thousands of web transactions are placed, eventually one may result in compromise or some form of inconvenience due to third-party manipulation.

> While individual providers and platforms offer options for end users—and, point solutions have addressed symptoms of this problem—a root cause remains elusive.

While much of our effort in cybersecurity is to elevate our internet trust levels, it is worth focusing some dedicated attention on how to improve voice and SMS communications to reduce the attack surface for this proverbial panacea of exploitation of the most vulnerable users/interactions.

STIR AND SHAKEN

Many solutions have been tried over the years, with varying degrees of success. While individual providers and platforms offer options for end users—and, point solutions have addressed symptoms of this problem—a root cause remains elusive. As a result, at present we still cannot trust the unrecognized numbers that show up on caller ID, given how rampant robocalls and mass vishing remain. Of all of the resources available, RFC7340 (Secure Telephone Identity Problem Statement and Requirements) seems to provide one of the most comprehensive overviews of the problem we all face for voice communications. This influential publication, released in September 2014, outlines problems ranging from voice and text trust to telephony denial of service attacks along with prior solutions and their practical shortcomings.

RFC7340 outlines requirements for what could

How Can We Protect Ourselves Now?

WE ARE ALL TIRED of receiving unwanted / malicious calls and text messages—and, as companies we have a hidden cost of threat actors or spammers impersonating our ranges—either to prospects, customers or even back to our own employees as part of social engineering attacks.

For users, help is on the way with the implementation of STIR/SHAKEN. In addition, many apps and services are available to help with this, although evaluating and recommending options is beyond the scope of this article.

For companies wanting to mitigate social engineering, the most critical step is to block inbound calls from your defined DID range, from the outside. If an attacker can impersonate your numbers when calling internal employees, their pretext will seem significantly more believable. This absolutely must be guarded against—if someone calls accounting claiming to be the CFO and the internal name and number show on caller ID as that person, the attack is very believable.

—D. Addington, M. Manrod and R. Mauldin

become a successful telecommunications trust model, introducing the foundations of what would become STIR and SHAKEN. STIR, or Secure Telephony Identity Revisited, applies to SIP and VOIP but does not impact TDM/SS7, which has become increasingly important due to the multi-faceted nature of mobile communications, among other use cases. SHAKEN, or Signature-based Handling of Asserted Information via Tokens, provides PSTN infrastructure with standards for how to handle calls that do not provide valid STIR metadata for a communication.

FCC MANDATE FOR STIR/SHAKEN

The FCC has mandated adoption of STIR/SHAKEN by June 30 for IP networks, which represents a monumental step forward, although it may introduce complexity for organizations during the transition period.

While this may not entirely address the PSTN side of the equation, it is a key step in the right direction. That said, it's not yet completely clear how this will play out. Security and telecommunications leaders would be wise to enthusiastically champion this movement. They should consider taking an active role in promoting STIR/SHAKEN and helping shape its adoption. It's also recommended that a business examine its own sales and marketing processes, including cold calling. At the end of the day, robocalls and vishing erode both trust and answer rates for legitimate sales calls, so this really is best for everyone in the long run.

Remember: Transition periods are difficult, and nobody wants to be caught off guard with catastrophic results in trust levels of legitimate outbound calls. We recommend you do some homework to understand its potential impact on your organization.

Simply put, it is useless to have information for a call that may not comply with predefined standards if the user endpoints are not looking for, and meaningfully enforcing, those standards that prevent impersonations. This is almost the reverse, because properly implemented, SHAKEN will ensure that only communications that are STIR can be trusted. STIR applies a trust level of A, B or C—and then, SHAKEN relays these trust levels across the SS7 network for POTS enforcement. *(See "Calling Use Cases and Associated Complexity," p. 31.)*

> Simply put, it is useless to have information for a call that may not comply with predefined standards if the user endpoints are not looking for, and meaningfully enforcing, those standards that prevent impersonations.

While the applicable RFCs are well thought out and worth reviewing, the most important considerations involve gaining universal adoption of a unified standard that can actually reduce the practical efficacy of impersonating phone numbers or trusted ranges. It seems like STIR/SHAKEN are the standards to align with for actually resolving the root cause of the problem. Whatever solution is adopted by the industry, it must be practical, effective and convenient from both user and enterprise perspectives. *(See "How Can We Protect Ourselves Now?" above left.)*

Don’t Just Hang Up. Learn More.

WE’VE COMPILED A LIST of references that may be useful as you build out a strategy and tactical plan for combating the surge in vishing and texting attacks against your organization.

RFCs

https://tools.ietf.org/html/rfc7340

https://tools.ietf.org/html/rfc4904

https://tools.ietf.org/html/rfc8224

https://tools.ietf.org/html/rfc8225

https://tools.ietf.org/html/rfc8226

https://tools.ietf.org/html/rfc8588

How to Spoof Numbers

https://blog.rapid7.com/2018/05/24/how-to-build-your-own-caller-id-spoofer-part-1/

https://www.spoofcard.com/

https://appstudio.zendesk.com/hc/en-us/articles/360020399511-How-Do-I-Use-SpoofCard-

https://www.spoofcard.com/anonymous-spoof-text

https://github.com/vpn/SMSSpoof

Other Articles and Resources on STIR/SHAKEN

https://www.fcc.gov/call-authentication

https://www.fcc.gov/document/fcc-mandates-stirshaken-combat-spoofed-robocalls

https://www.home.neustar/resources/faqs/stir-shaken-for-businesses

https://nymag.com/intelligencer/2018/05/how-to-stop-spam-robocalls-with-stir-shaken.html

History of Phreaking

https://www.britannica.com/topic/phreaking#:~:text=Phone%20phreaking%20first%20began%20in,-known%20as%20the%20whistling%20phreaker

MAC Spoofing

https://en.wikipedia.org/wiki/MAC_spoofing#:~:text=MAC%20spoofing%20is%20a%20technique,MAC%20address%20to%20be%20changed

Social Engineering Key Resource

https://www.social-engineer.org/framework/se-tools/phone/caller-id-spoofing/

—D. Addington, M. Manrod and R. Mauldin

FOR PROVIDERS AND REGULATORS

At the end of the day, we need the ability to provide trust to a dedicated entity, delegate trust to appropriate outsourced organizations, and authenticate all trusted mechanisms to end users in a way that untrusted calls or text messages can be ignored. This needs to be a unified front across infrastructure providers, companies and regulatory bodies that back and enforce compliance to ensure the ongoing integrity of voice and SMS text communications.

Without such improvements, trust will continue to erode and vendor-specific solutions will create a bifurcated market where trust diminishes to a point of irrelevance, creating a market crisis where all resources are assumed hostile.

It is in the best interest of all legitimate parties to pursue a valid path to trust, to prevent a cascading failure of the reliance upon inbound voice communications for legitimate commercial or non-commercial purposes. The ability to assure and validate trust could not be more important as it relates to voice and text message communications. ●

> It is in the best interest of all legitimate parties to pursue a valid path to trust, to prevent a cascading failure of the reliance upon inbound voice communications for legitimate commercial or non-commercial purposes.

MIKE MANROD, CISSP, serves as the CISO for Grand Canyon Education, responsible for leading the security team and formulating the vision and strategy for protecting students, staff and information assets across the enterprise. **DANIEL ADDINGTON**, CISSP, provides management, leadership, and technical guidance for the security team at Grand Canyon Education. **RYAN MAULDIN**, CISSP, is a senior telecommunication engineer with Grand Canyon Education. Additionally, the authors give their colleague, CHRIS SMITH, special credit for his knowledge and his contributions to this article.

CONTENTS

Delivering On Our Mission Despite a Pandemic

HOW THE CENTER FOR CYBER SAFETY AND EDUCATION ADAPTED BY PAT CRAVEN

ONE YEAR AGO, schools, businesses and entire countries began to shut down as a strange and unknown virus spread around the world. Back then, we were told to temporarily stay home and wear masks for a couple of weeks to "flatten the curve," hoping this would quickly be behind us.

Never did we imagine we would still be facing restrictions and a continuation of remote work, and that we would have witnessed so many organizations going out of business as a result of the pandemic.

COVID-19 required us all to "pivot" and reimagine how we do business in a new world. We went from some temporary adjustments to permanently changing our business models. Your Center for Cyber Safety and Education has gone through the same transformation during the last 12 months.

Nearly all our educational programs were originally designed to be delivered in physical group settings, with a volunteer instructor or teacher leading the in-person discussion. But with no large gatherings permitted, yet a skyrocketing demand from the public to learn how to be safe and secure online, we had to look at what we were doing to fulfill our mission in a pandemic world. And we did.

The easiest adaptation was to modify our popular Safe and Secure Online program to an online environment. The presentations are PowerPoint-based, which we've learned works perfectly in this new digital world. Instead of a projector, all the volunteers needed was a good internet connection and a computer. More than 1,500 Safe and Secure Online presentations were delivered in the past year, reaching in excess of 60,000 people. That is a 40% increase over the previous year, with demand still growing! Volunteers and members quickly realized that the pandemic didn't have to stop our efforts to make it a safer cyber world; in fact, it made it easier to do from the comfort of our homes.

More than 1,500 Safe and Secure Online presentations were delivered in the past year, reaching in excess of 60,000 people.

At first, demand was driven primarily by volunteers and members who were putting on presentations for fellow chapter members and families or at their own children's school. But now, we are seeing a spike in companies and other organizations wanting to do something for their employees using the Parents' Program as a "lunch 'n learn" or as part of their security awareness training initiative. It is a great way to let employees know that you care about their families and to drive home the message that security doesn't end when the workday is over.

And now you can even bring the award-winning Garfield's Cyber Safety Adventures programs to your employees' children, thanks to our new Garfield at Home and Garfield for the Virtual Classroom programs. To bring it to your company or community, just reach out at center@isc2.org and we can help customize a program that will make everyone happy and safe. Together, let's seize this opportunity to ensure some good comes from such dark times. ●

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

Photograph by Getty Images

NEWSLETTERS WEBINARS PDI
BLOG COMMUNITY MAGAZINE
EVENTS CHAPTERS RESEARCH

WELCOME TO BUZZWORTHY, A ROUNDUP OF WHAT'S BEING SAID AND HEARD AROUND (ISC)^2 CHANNELS

"If you are a cloud-native company, you have to focus on your data. You don't have any other choice. If you are in a traditional shop, try to start thinking about things on that side. Focus on identity access and management and getting a solution that's going to cover you, no matter where you are."

—Eric Gauthier, CISSP, VP of Technical Operations at Burning Glass

Source: (ISC)^2 January edition of Cloud Security Insights

"There are some interesting aspects within this new [New Zealand] Privacy Act; for instance, they do not talk about 'data,' they refer to 'information.' There was an interesting High Court case in New Zealand, which stated that information is not confined to the written word but embraces any knowledge however gained or held and, in some circumstances, can extend to the information contained in the mind of an individual."

—John Martin, CISSP, Senior Security Architect, IBM New Zealand

Source: (ISC)^2 blog post

"You are likely to see the rise, over time, of what's called the Chief Health Officer … the CHO. That is someone who is also in the security space, who is advising the C-suite on what to anticipate in terms of not just pandemics, but healthiness generally."

—Juliette Kayyem, senior lecturer in International Security at Harvard's Kennedy School of Government and faculty chair of the Homeland Security and Security and Global Health Projects, during (ISC)^2 2020 Security Congress keynote

"One of the big pushes that we're seeing is away from the traditional VPN, where we had to own the endpoint, to the more contemporary thought of zero trust."

—CISO Michael D. Weisberg, CISSP, Garnet River, LLC, during (ISC)^2 2020 Security Congress session "How I Am Surviving the Apocalypse - Information Security In the Time of a Virus"

"To really remove the barriers to diversity in the cybersecurity profession, the community needs to start by engaging underserved students in middle school. I was in the military, industry and government, but it wasn't until I transitioned to being an adjunct professor … and participated as a lead instructor at a GenCyber Camp for middle school children that I was able to get a perspective on the challenges students face, like not having exposure to technology or having things considered basic to many professionals. Our community tends to expect that everyone has broadband access with a decent laptop, and that is nowhere near reality."

—@Frank60 during (ISC)^2 2020 Security Congress Diversity Lounge session "The Problem with Diversity and Inclusion in Cybersecurity—We Can Fix It"

SHOW OFF YOUR CREDENTIALS

SEE AND SECURE EVERY THING™

You know that every reputable cybersecurity framework starts with an understanding of the environment. This means comprehensive visibility of every thing—digital and physical, managed and unmanaged, on and off the network—with an understanding of current risks and exposures with policies and procedures to manage those risks.

Armis was born from this understanding, with an agentless device security platform designed to discover, detect, and defend—enabling you to more easily see and secure every thing.

Learn more about how Armis supports cybersecurity frameworks visit armis.com/solutions/cybersecurity-frameworks/

ARMIS®