TRANSPARENCY IN THE ERA OF GDPR

InfoSecurity PROFESSIONAL

(ISC)² InfoSecurity PROFESSIONAL 10 YEARS

A Publication for the (ISC)²® Membership

JULY/AUGUST 2018

GET READY TO RUMBLE

Go red or go blue

EMV® 3-D SECURE REVIEWED

Is this the right solution to e-commerce authentication?

PATCH PROFUSION

Continual updating may be creating more vulnerabilities

isc2.org community.isc2.org

3 DAYS

24 CPES

7 TRACKS

75 SESSIONS

90 SPEAKERS

CANADA'S PREMIER IT SECURITY CONFERENCE

SECTOR

Security Education Conference

OCTOBER 1-3, 2018
MTCC TORONTO ONTARIO

DON'T MISS OUT, LIMITED TICKETS AVAILABLE

REGISTER TODAY AT SECTOR.CA/REGISTER

- LEARN FROM THE WORLD'S LEADING INDUSTRY EXPERTS
- ENGAGE IN CANADA'S LARGEST IT SECURITY EXPO
- ADD THE OPTIONAL **(ISC)² SECURE SUMMIT** AT SECTOR
- EARN UP TO 24 CPE CREDITS

SECTOR IS THE EVENT FOR IT SECURITY PROFESSIONALS TO CONNECT, LEARN, NETWORK & ENGAGE.

(ISC)² MEMBERS **SAVE 10%** WITH CODE ***ISC22018***.
CAN'T MAKE THE FULL CONFERENCE? GET A **FREE** EXPO PASS WITH CODE ***ISC22018expo***.

@sectorca /SecTorCa sector.ca/blog

/SecTorConference /SecTorConference

contents

VOLUME 11 • ISSUE 4

A look at stronger risk-based authentication of payment cards used for online purchases. PAGE 24

features

INCIDENT RESPONSE & FORENSICS

18 **Red vs. Blue**
Why pen testing teams are increasingly popular among all types of organizations.
BY PAUL SOUTH

CUTTING EDGE

24 **Chipping In**
A member reviews EMV® 3-D Secure, the newest solution to e-commerce authentication.
BY DAVID L. DANN, CISSP

POLICIES & PROCESSES

26 **First, Do No Harm**
Defending our systems with continual patching may be creating more vulnerabilities than we know.
BY BARRY DOWELL, CISSP

Cover image: JOHN KUCZALA Illustration above: ENRICO VARRASSO

departments

4 EDITOR'S NOTE
Pushing Buttons
BY ANNE SAITA

6 EXECUTIVE LETTER
How We're Meeting GDPR Compliance
BY WES SIMPSON

8 FIELD NOTES
More than 100 speakers and sessions at upcoming (ISC)² Security Congress; recommended reading; (ISC)² study results on multicultural workforce; easy framework for IT security; (ISC)² ISLA Government winners

14 #NEXTCHAPTER
(ISC)² Middle Georgia Chapter

16 ADVOCATE'S CORNER
Helping Legislators Better Understand Our World
BY JOHN McCUMBER

30 CENTER POINTS
Garfield More Popular Than Ever at 40
BY PAT CRAVEN

32 COMMUNITY
Sharing Insights from Buzz-Worthy Threads
Highlights from recent discussions on the (ISC)² online forum for cybersecurity professionals

4 AD INDEX

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

editor's note

BY ANNE SAITA

Pushing Buttons

MY PARENTS recently passed away and, among many other things, I am now raising a disabled nephew they had adopted. It's a lifelong commitment, but one that my husband and I wholeheartedly accept.

My nephew likes to push buttons, literally and figuratively. In his own way, he's reacting to a series of tragic incidents in his short life. He's also testing his new family through a number of self-induced "incidents." On his first visit to San Diego, he managed to jack up all of our home electronics by randomly pushing buttons on any console, keyboard or remote he could find. Our response then: repeatedly telling him to stop. It didn't work. So, we tried to see the situation from his perspective, which involved deeper research into his disabilities, rearranging rooms and creating our own version of an incident response plan to greatly reduce both material and mental meltdowns going forward.

That's why I was so struck by the opening of our cover story by Paul South on creating red teams and blue teams to improve incident responses. Caroline Wong, CISSP, who's also a new parent, compares the popular pen testing practice to childproofing a home: Sometimes it takes an incident or an outsider to help us see previously unknown vulnerabilities.

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

We all "live" within our organizations and dedicate a great many waking hours to keeping them safe from cyberattacks. But over time, we sometimes fail to see when our current environment or tactics are no longer effective. This is reinforced by another feature by member Barry Dowell that shows a different perspective on patching policies. Another member, David Dann, brings us up to speed on the new EMV® 3-D Secure messaging protocol.

May each of you learn how best to handle the unexpected, whether it's from impersonating an attacker or improvising during a major life change. Always remember: The rough times eventually smooth out if we intelligently respond in a timely manner, rather than instinctively react all too late. ■

advertiser index

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

SecTor 2
(ISC)² Security Congress 5
CCSP 7
LATAM Perks 9
SecureSummits UK 13
Alibaba 15
(ISC)² APAC Security Congress 17
Black Hat 23
NTT Security 28
TechTarget 29
The Center for Cyber Safety and Education 31
Twirling Tiger Media 33

InfoSecurity PROFESSIONAL

(ISC)² MANAGEMENT TEAM

DIRECTOR, CUSTOMER EXPERIENCE
Jessica Hardy
727-493-3566 | jhardy@isc2.org

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

SENIOR MANAGER, CORPORATE COMMUNICATIONS
Jarred LeFebvre
727-316-8129 | jlefebvre@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 TEAM

EVENTS SALES MANAGER
Jennifer Hunt
781-685-4667 | jhunt@isc2.org

REGIONAL SALES MANAGER
Lisa O'Connell
781-460-2105 | loconnell@isc2.org

EDITORIAL ADVISORY BOARD

Kaity Eagle, (ISC)²

Jarred LeFebvre, (ISC)²

Yves Le Roux, EMEA

Cesar Olivera, Brazil and Canada

TWIRLING TIGER MEDIA EDITORIAL TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

MANAGING EDITOR
Deborah Johnson

EDITOR
Paul South

PROOFREADER
Ken Krause

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

(ISC)²

SECURITY CONGRESS 2018

Keynotes Announced

Earn up to 46 CPEs.

Congressman Cedric Richmond (LA-02)

Congressman Richmond currently serves on the House Committee on Homeland Security and is the ranking member of the committee's Cybersecurity and Infrastructure Protection Subcommittee. He is also a member of several other Homeland Security subcommittees including: Crime, Terrorism, Homeland Security, and Investigations; Courts, Intellectual Property and the Internet; and Oversight and Management Efficiency.

Dr. Jessica Barker

Dr. Jessica Barker is a leader in the human nature of cybersecurity. She has been named one of the UK's Top 20 most influential women in cybersecurity and awarded among the Tech Women 50. Equipped with years of experience running her own consultancy, she recently co-founded Redacted Firm, working with a variety of organizations from small creative agencies to multi-national banks.

Theresa Payton

Theresa Payton is one of the nation's leading experts on internet security, data breaches and fraud mitigation. She was first female to serve as White House CIO and was named #4 on IFSEC Global's list of Top 50 Influencers in Security & Fire 2017. She currently runs her successful and rapidly-growing security consulting company, Fortalice Solutions, and stars on CBS's TV show, "Hunted."

Early Bird Pricing through July 31

Register Today

SAVE $50 OFF All Access Pass with code: **INFOSEC18**

(ISC)² Members Save $300

congress.isc2.org #ISC2Congress

THE LATEST FROM (ISC)²'S LEADERSHIP

executive letter

BY WES SIMPSON

How We're Meeting GDPR Compliance

THAT COLLECTIVE SIGH you heard around the world the other month was everyone taking a moment to basically exhale after months and years of work to become compliant with the European Union's General Data Protection Regulation, which went into effect May 25.

The EU GDPR is sweeping in both scope and reach and represents one of the highest standards for data privacy. Although it applies directly to any EU citizen both at leisure and at work, we at (ISC)² decided to apply these same standards to all contacts in all regions. It's a tall order, given our global membership includes more than 130,000 members in more than 170 countries.

If you've been on our website, then you likely noticed our updated privacy policy and pop-ups alerting you to our use of cookies. Data protection and privacy are as important to us as they are to you, and we view GDPR compliance as an opportunity to provide our members more transparency into how we use your data.

Like many other organizations, reaching GDPR compliance began shortly after the sweeping legislation was passed two years ago. First, we established a cross-functional team to examine how data flows through the organization. We asked a lot of data hygiene questions to determine precisely what data we captured, when and from where. Then we consolidated systems that collect and store that data.

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

We also committed to ensure compliance for all members and candidates—not just those in the EU. Many other organizations have made a similar decision, given that similar data privacy regulations are expected to take hold in other regions. It just makes more sense to hold everyone's data to the same, stricter standards.

Of course, with our members now having more control over that data, some actions are required of them too. If you want to stay in touch and not miss out on what is happening at (ISC)², we need you to update your communications preferences. This includes timely communications essential to helping you grow professionally and maximize the value of your membership.

> **If you want to stay in touch and not miss out on what is happening at (ISC)², we need you to update your communications preferences.**

If you visit https://www.isc2.org/preferences, you'll see we've broken down select communications channels by categories. You can now decide if you want to be kept informed on any or all of the following: certifications and educational resources; continuing education and professional development opportunities; (ISC)² news and resources; and the latest from our nonprofit Center for Cyber Safety and Education, which provides the popular Safe and Secure Online program as well as research studies.

We know many of you now are more involved in managing your own organization's data protection policies as a result of GDPR, but we do hope you'll take a moment to ensure you continue to receive the information and resources you need to maintain your credential and continue your career as a certified cybersecurity professional. ■

IT'S YOUR TIME.

LEARN AT YOUR PACE.

CCSP®

Certified Cloud Security Professional

An (ISC)² Certification

CCSP Online Self-Paced Training

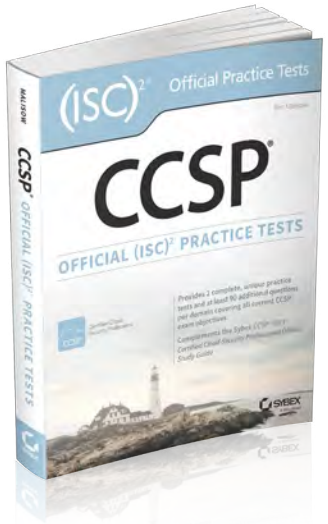
$1,995
(was $2,795)

It's your time to be recognized as a globally respected cloud security expert. Confidently prepare for the CCSP exam - on your own schedule - at a new low price of $1,995.

Through July 31, we'll bundle Practice Tests eBooks for FREE!

The CCSP Online Self-Paced Course includes:

- Access to recordings and official courseware
- Official (ISC)² Student Workbook
- Post-assessment practice questions
- And more!



(ISC)² Members Earn 40 CPEs

Start your training

field notes

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

EDITED BY DEBORAH JOHNSON

2018 (ISC)² SECURITY CONGRESS

The Big Easy Awaits

Early registration ends soon for our annual North American conference in New Orleans

Photograph by iStock

LAST YEAR'S CONFERENCE SOLD OUT, which should be a good reason to register early for the 2018 (ISC)² Security Congress, October 8 to 10 at the New Orleans Marriott in Louisiana.

The reasons for attending are many. There will be more than 100 speakers and sessions that connect with every aspect of the information security world. And with more than 2,000 industry colleagues on hand, the opportunities for sharing ideas, learning the latest innovations and networking are endless.

Here's a sample of the exciting sessions on tap:

- "Achieving GDPR Compliance with the CSA Code of Conduct" – Daniele Catteddu, CTO, Cloud Security Alliance
- "Migrating to the Cloud…What I Wish I Knew Ahead of Time" – Cory Deeter, CISSP, CISA, CIA; Director, Cyber Security and IT Compliance, The Finish Line
- "Viruses, Trojans, Worms, Malware, and Ransomware—What's Next and Are We Prepared?" – William "Tony" Cole, CISSP, Board of Directors, (ISC)²

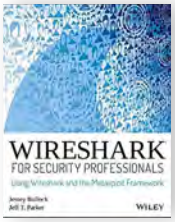
Not to mention the unique, New Orleans experience is not to be missed. Save $200 through July 31 with Early Bird Pricing.
Learn more at http://congress.isc2.org. ■

RECOMMENDED READING

Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework

By Jessey Bullock and Jeff T. Parker (Wiley, March 20, 2017)

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



Wireshark is a free and open source packet analyzer software used for network and protocol analysis and troubleshooting by security professionals, network admins and other IT personnel. It runs on many platforms including Linux, MacOS, Solaris and Windows. Wireshark is used by pen testers, ethical hackers and members of security operations groups.

Wireshark for Security Professionals exposes the security professional to its use and demonstrates how the software works with real-life scenarios. The authors provide the initial background of the tool, its objective and a set of use cases. Rather than being a technical implementation guide, the book gives the professional the background needed to expand the set of use cases for further implementation.

The authors Bullock and Parker use Zillow.com as an example of how Wireshark listings display source and destination IP, time, length and packet contents. This book demonstrates that Wireshark can be extended by using the Lua scripting language to read USB traffic, with potential for mobile as well.

There are several prerequisites needed before diving into this book, including a basic understanding of networking and access to download GitHub's repository of the lab code. *Wireshark for Security Professionals* is intended as a hands-on book to read and implement. ■

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

(ISC)² | MEMBER PERKS

NOW IN LATIN AMERICA!

GET THE PERKS YOU DESERVE

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

Additional discounts include:

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

NOW IN LATIN AMERICA!

JOIN MEMBER PERKS

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

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

Available on the App Store

ANDROID APP ON Google play

Innovation Through Inclusion: The Multicultural Cybersecurity Workforce

Data are based on an (ISC)² Global Information Security Workforce Study in partnership with the Center for Cyber Safety and Education and Frost & Sullivan

Note: Although the study is global in scope, questions of race and ethnicity were asked only to U.S.-based respondents.

LEADERSHIP IN CYBERSECURITY

U.S. cybersecurity professionals in leadership positions	**29%**
Caucasian cybersecurity professionals in leadership positions	30%
People of Color* cybersecurity professionals in leadership positions	23%

**Defined in study as those who do not self-identify as White or Caucasian*

"In order to build strong, adequately staffed cybersecurity teams, employers—and the cybersecurity profession as a whole—must make cybersecurity a rewarding and welcoming career for everyone. Understanding the challenges our profession faces related to diversity is a critical first step to accomplishing that goal and ultimately addressing the widening cybersecurity workforce gap."

—David Shearer, CISSP, CEO, (ISC)²

AVERAGE ANNUAL SALARIES

Caucasian Males	**$124,000**
Males of Color	**$121,000**
Caucasian Females	**$121,000**
Females of Color	**$115,000**

MINORITY REPRESENTATION IN THE WORKFORCE*

Within the Cybersecurity Profession	**26%**
U.S. Total Workforce	**21%**

**U.S. Bureau of Labor Statistics 2015*

ON-THE-JOB DISCRIMINATION

32%

of participating cybersecurity professionals of color reported experiencing workplace discrimination

READ. QUIZ. EARN.
2
CPEs

Earn CPEs for Reading This Issue

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

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&PCAT=7777&CAT=10773

28.9 MILLION

Number of cryptominer incidents reported

Source: Comodo Cybersecurity Threat Research Labs – Q1 2018 Survey

Who's behind the data breaches?

76%	financially motivated
73%	perpetrated by outsiders
68%	took months or longer to discover
50%	carried out by organized criminal groups

Who are the victims?

58%	categorized as small business
24%	healthcare organizations
15%	accommodation & food services
14%	public sector entities

Top action varieties in breaches

- Use of stolen credentials (hacking)
- RAM scraper (malware)
- Phishing (social)
- Privilege abuse (misuse)

Source: 2018 Verizon Data Breach Investigations Report

A Security Framework that Anyone—and Everyone—Can Follow

BY SHAHIN KAMRUZZAMAN, CISSP

This is excerpted from the April Insights, *the companion e-newsletter to* InfoSecurity Professional. *You can read a lot more detail about each component of the framework at https://www.isc2.org/News-and-Events/Infosecurity-Professional-Insights.*

IN A BUSINESS START-UP, the entrepreneur usually is a one-person band, taking on all kinds of work, including IT. As the business grows and becomes increasingly dependent on IT infrastructure, the entrepreneur may not be able—or willing—to handle the challenges of IT security, vulnerability, risk management framework and privacy law.

To provide the new business owner guidance on security needs, I've created a simple approach to basic IT security. It's a five-step framework to manage vulnerabilities and reduce risks as related to IT security. It works for any organization, but is targeted for independent/privately held organizations with 500 to 5,000 employees that struggle with implementing information security into their existing IT infrastructures, whether done in-house or using outside consultants.

This framework for a basic IT security plan can be broken into five groups:

- Asset Management
- Asset Behavior
- Vulnerability Management
- Threat Detection
- Incident Response

Each section has requirements and measures to ensure the end result: security for the organization's infrastructure. ■

Framework Step	What to Know and Do
Asset Management	• How many assets do I have? • Is my inventory current? • Do all assets have security tools installed, configured and maintained? • Are there any exceptions in my configuration? • Do I have an inventory of my service accounts? • Do I have an asset decommission policy and is it enforced?
Asset Behavior	• Where are my assets? • Are they in my perimeter or inside? • Are they configured as per secure guidelines? • Are they being monitored for their utilization? • Does the organization have maintenance for all assets with vendors for support? • Does the organization know each asset's best-case and worst-case scenarios? • Does the organization have an expert or managed service for each IT asset?
Vulnerability Management	• Are my organization's assets vulnerability free? • Do my organization's assets get updates from vendors? • Does my organization's product get scanned at least monthly for known vulnerabilities? • Is the patching up to date? • Do I have a vendor security newsletter subscription? • Does my vendor comply with US-CERT vulnerability discloser policy? • Does my organization have a red team? • Does my organization engage a professional hacker to find vulnerabilities in the system or on my perimeter network?
Threat Detection	• Does my organization have an IDS/IPS is place? • Is the IDS/IPS properly configured and monitored? • Does the organization have the SIEM solution in place for all assets? • Is the SIEM solution properly monitored and investigated? • Does the organization have a weekly threat-detecting meeting or discussion? • Does the organization rely on vendors or have its own honeypot to detect new threats?
Incident Response	• Does my organization have a formal Incident Response Plan in place? • Does the organization do a quarterly tabletop exercise for incident response? • Does the organization do mock incident response exercises? • Is the incident response team member contact list up-to-date? • Does the incident response team have multiple ways to communicate? • Does everyone know what to do when people see an incident?

(ISC)² ISLA Government Winners Announced

Master of ceremonies Dr. Earl Crane, CEO and founder, Emergynt; (ISC)² Board of Directors

CONGRATULATIONS to this year's (ISC)² ISLA Government recipients, selected from an outstanding field of exceptional individuals and teams. This program recognizes the ongoing commitment of individuals whose initiatives, processes and projects have led to significant improvements in the security posture of a department, agency or the government (local, state, or federal).

The following were officially recognized for cyber excellence on May 8 during an awards ceremony luncheon at Secure Summit DC.

Workforce Improvement
Aung Htein
Administrator, Office of Information Systems and Technology, Employment and Training Administration, U.S. Department of Labor

Technology Improvement
Michael Sherwood
Director of Technology and Innovation, City of Las Vegas

Process/Policy Improvement
Glenn Hernandez, CISSP
Captain, U.S. Coast Guard (Retired) and Chief Information Security Officer

Up-and-Coming Information Security Professional
Mark Bacharach, CISSP
Innovation Fellow, Environmental Protection Agency, Office of Environmental Information, Office of Information Security and Privacy

Community Awareness Team
Matt Goodrich, J.D.
FedRAMP Director, Technology Transformation Service, U.S. General Services Administration
Supporting team: Ashley Mahan, Claudio Belloli, John Hamilton, Betsy Steele and Ryan Hoesing

Most Valuable Industry Partner (MVIP) Team
Nicholas Andersen, CISSP
Vice President of Corporate Strategy, Invictus International Consulting
Supporting team: Sean Hensen; Cornelius Roberts, CISSP; Erin Clemens, CISSP; Mike Bernert, CISSP; and Jimmy Jay, CISSP

Raytheon Women's Cyber Security Scholarship Awards
Sophia Hu, Princeton University
Aileen Ma, California Institute of Technology

Engility CyberWarrior™ Scholarship Awards
Leonardo Bastidas
Magdalena Seitz

The (ISC)² President's Award
Kevin L. Jackson, CCSP
Founder and CEO of GovCloud Network

F. Lynn McNulty Award
Essye B. Miller
Acting Principal Deputy, Department of Defense Chief Information Officer

Learn more about the (ISC)² ISLA Government program at https://www.isc2.org/About/Award-Programs. ■

(ISC)²

SECURE SUMMITS / UK

#ISC2Summits

ENRICH. ENABLE. EXCEL.

Can't attend?
Watch the live stream broadcast for free from the convenience of your computer.

Join us at the (ISC)² Secure Summit UK

19 - 20 September | THE KIA OVAL, London

(ISC)² Secure Summit UK is back for another year bringing together over 400 industry colleagues.

Hosted at the iconic KIA OVAL, home of Surrey County Cricket Club, the event features over 14 educational and thought provoking sessions.

16 cpes **Earn your CPEs!**

Register Now
securesummits.isc2.org

SAVE THE DATE

(ISC)² Secure Summit EMEA | 15 - 16 April, 2019 | World Forum, The Hague

#nextchapter

EDITED BY DEBORAH JOHNSON

(ISC)² MIDDLE GEORGIA CHAPTER

Forging a Stronger Bond Between Cyber Education and Tech

Bringing cybersecurity education together with the latest in technology has been an ongoing mission for the (ISC)² Middle Georgia Chapter. Since 2014, the chapter has organized technology expos and cyber forums held at the Museum of Aviation in Warner Robins, Ga. Initially, this was an event aimed solely at providing local certified professionals affordable (free) continuing education opportunities.

Starting in 2015, the events were expanded to include a technology expo to bring industry and the military together in a convenient location to network and collaborate on mission requirements and new technologies.

Speakers are recruited through networking and by encouraging chapter members to volunteer to speak at the forums. Vendors displaying their technologies at the expo are also approached for presentations. The chapter partners with the local Armed Forces Communications and Electronics Association (AFCEA) chapter and National Conference Services Inc. (NCSI) to help cast a larger net for potential speakers for the cyber forum and to solicit vendors to participate in the tech expos.

The theme for a recent event was "360 Degrees of Information/Cybersecurity." The nearly 300 attendees engaged with high-quality speakers from multiple disciplines including technology providers, industry practitioners and academia. In addition, the expo included 23 vendors who shared technologies and resources with attendees. The event was highlighted by a cyber forum, which gave cybersecurity professionals the opportunity to earn CPEs.

The chapter's next technology forum and cyber expo will be another partnership with the local AFCEA chapter featuring a presentation by Dr. Ron Ross, a fellow at the National Institute of Standards and Technology. Ross leads the Federal Information Security Modernization Act (FISMA) Implementation Project, which includes the development of security standards and guidelines for the federal government, contractors and the United States' critical infrastructure. ■

(ISC)² MIDDLE GEORGIA CHAPTER

Contact: Todd Davenport, President

Email: president@isc2chapter-middlega.org

Website: http://isc2chapter-middlega.org

Q&A

Todd Davenport, President, (ISC)² Middle Georgia Chapter

When it comes to cybersecurity, what do you think are the challenges facing practitioners in educating the public?

The biggest challenge is time. As a society, we are moving at a pretty hectic pace; technology has made it possible to do more, faster than ever before. You would think that if we can do more, faster then we'd have more 'free' time to do other things, but as we all know that isn't the case. Doing more faster just frees up time to do more. Today, cybersecurity education is an ancillary type of activity, and since there is a premium on time, that makes it difficult. Somehow, cybersecurity education needs to be integrated into the day-to-day activities of the workforce, becoming part of the culture and not an ancillary activity.

Does the average user of social media understand the privacy risks that are out there? And what can (ISC)² members do to help them understand?

Thanks to the many highly publicized breaches that have taken place over the past few years, I absolutely believe they understand the privacy risks. The challenge is getting them to change the behaviors that put their information at risk.

The current trends of social media use point to a community obsessed with "sharing information." Ten to 15 years ago we didn't have programs like Safe and Secure Online to educate kids on the risks before they started using these social media platforms. We must continue the emphasis on educating the public on how their

information is mined, the type of information being mined and, most importantly, why it's being mined.

My experience has shown me that if we can't communicate the "why" most in what we tell folks, the "how" and "what" will be ignored. As (ISC)^2 members we need to really emphasize the importance of reaching the 6- to 10-year-olds now before they develop bad habits.

How has your chapter grown and what do you think is the biggest attraction to potential members?

Our chapter has grown at a pretty steady pace, about five new members a year. We are in our sixth year as a chapter and we've used a "crawl, walk, run" approach. Initially, we focused on the networking and continuing education benefits of membership in a local chapter. Over the past two years we've added more emphasis on the community outreach.

When your members get together, what are the most popular issues in discussion? And how do you capitalize on that to gain new members?

Lately it's been whatever is in the headlines: ransomware attacks, data breaches, election hacking, etc. Our approach is to attract members who are interested in continuous improvement and have the self-awareness to understand no one is an expert in everything. As a chapter, we strive to help fill each individual's knowledge gap by providing speakers who are experts on a variety of interesting and relevant topics.

What do you think is the biggest challenge facing cybersecurity professionals today?

We live in a time where technology and innovation are moving faster than we can keep up with. Historically, the cyber and information security professionals have been perceived as the folks who put the "n-o" in innovation or the Chicken Little "the sky is falling" folks. We need to rebrand ourselves and make the business see us as a value-added part of their team.

If we can't effectively communicate our value to the business, we will be marginalized and ignored. We must always emphasize our goal is to make sure the solutions are operationally secure, ensuring needs are met without introducing undue risks.

MUSINGS ON SECURITY ISSUES THAT IMPACT MEMBERS

advocate's corner

BY JOHN McCUMBER

Helping Legislators Better Understand Our World

IT WAS AN AMAZING DAY to be on Capitol Hill. First and foremost, it was the peak of the cherry blossoms. These wonderful gifts from the Japanese people bless Washington each spring with their exuberant yet ephemeral beauty.

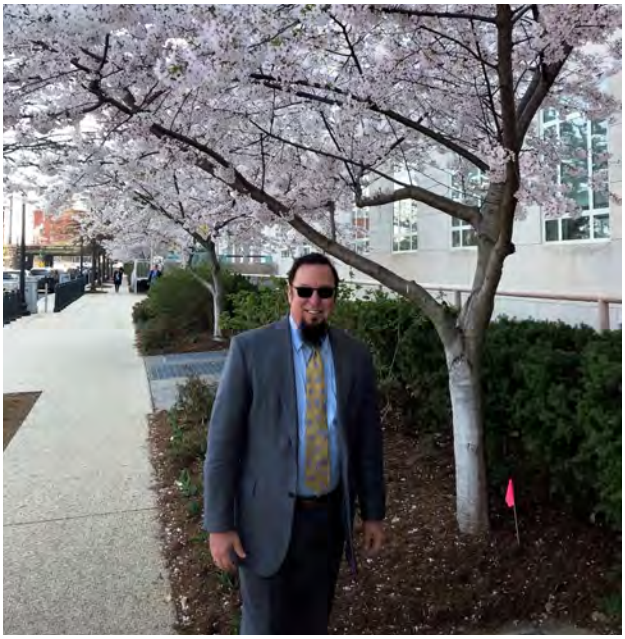
This was also when Mark Zuckerberg testified before the Senate on his company's use and alleged misuse of his subscribers' personal information. I was wandering the halls of Congress that day, and every congressperson's and senator's office was showing the spectacle on the ubiquitous televisions. The CEO of Facebook looked like I did when I got my first adult suit of clothes to be confirmed by the bishop at our huge Gothic church back in the Midwest.

One of the key observations to come from the hearings was just how little our elected representatives know about how this newfangled internet thingy works. Even with hordes of staffers and experts writing up comments and questions, the verbal exchanges were awkward and far from enlightening. Of course, even the words used were often incorrect and/or misleading. It was a brutal display of just how little valuable information can be elicited from groups of people speaking two different languages.

Part of my mission on this beautiful day was dropping off copies of the (ISC)² Cybersecurity Lexicon we developed in response to the last time I visited the hallowed halls of Congress.

During my January meetings, I had determined a missing component of existing and pending legislation was the misuse of key terms of cybersecurity and risk management. We needed to start with a common understanding of basic terminology.

I have had the privilege of being a small part or this profession for 30 years. I never thought producing basic primers would be so important at this stage. We went through the first 1,000 copies in two days. Technology companies, legislators and their committees, universities and lawyers have been asking for thousands more copies to distribute. It's a start.



One of the early principles of the internet I shared with friends and family as well as professional colleagues was that if the game/app is free, you're the game. In other words, using free software meant your information was scraped from your use of the software for a variety of purposes, but mostly simple directed advertising in the early years.

That caveat has become even more ominous now that our technology surrounds us, listening to nearly everything we say while recording nearly everything we type on our devices. There has never been a more critical time to be a part of the active and diverse cybersecurity profession. ■

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

(ISC)²

SECURITY CONGRESS | APAC 2018

09 - 10 July
Conrad Hong Kong Hotel

ENRICH. ENABLE. EXCEL.

At (ISC)² Security Congress APAC 2018, you'll get to engage with over 400 security-minded individuals, discover solutions to the latest cybersecurity threats, and gain insight from international industry experts.

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

Tracks Include:

- Cloud Security
- Critical Infrastructure
- Emerging Technologies & Security
- Governance, Risk & Compliance
- Professional Development
- Security Operations

Keynote Speakers:

Jason Pun, Assistant Government Chief Information Officer (Cyber Security & Digital Identity), The Government of the HKSAR

Hon. Charles Mok, JP
Legislative Councillor (IT)
The Government of the HKSAR

Dr. Kevin Charest, CISSP
Chairperson, Board of Directors, (ISC)²

David Shearer, CISSP
Chief Executive Officer, (ISC)²

Dr. Frank Law, CISSP
Senior Superintendent of Police,
Cyber Security & Technology
Crime Bureau, Hong Kong Police Force,
The Government of the HKSAR

Register Today & Save!

(ISC)² Member Price: US$ **324**

Standard Price: US$ 432

5% additional discount for group purchase.

For inquiries: (852) 2850 6953
securitycongressapac@isc2.org

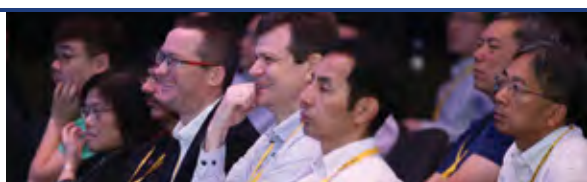
Visit apaccongress.isc2.org | #ISC2congressAPAC

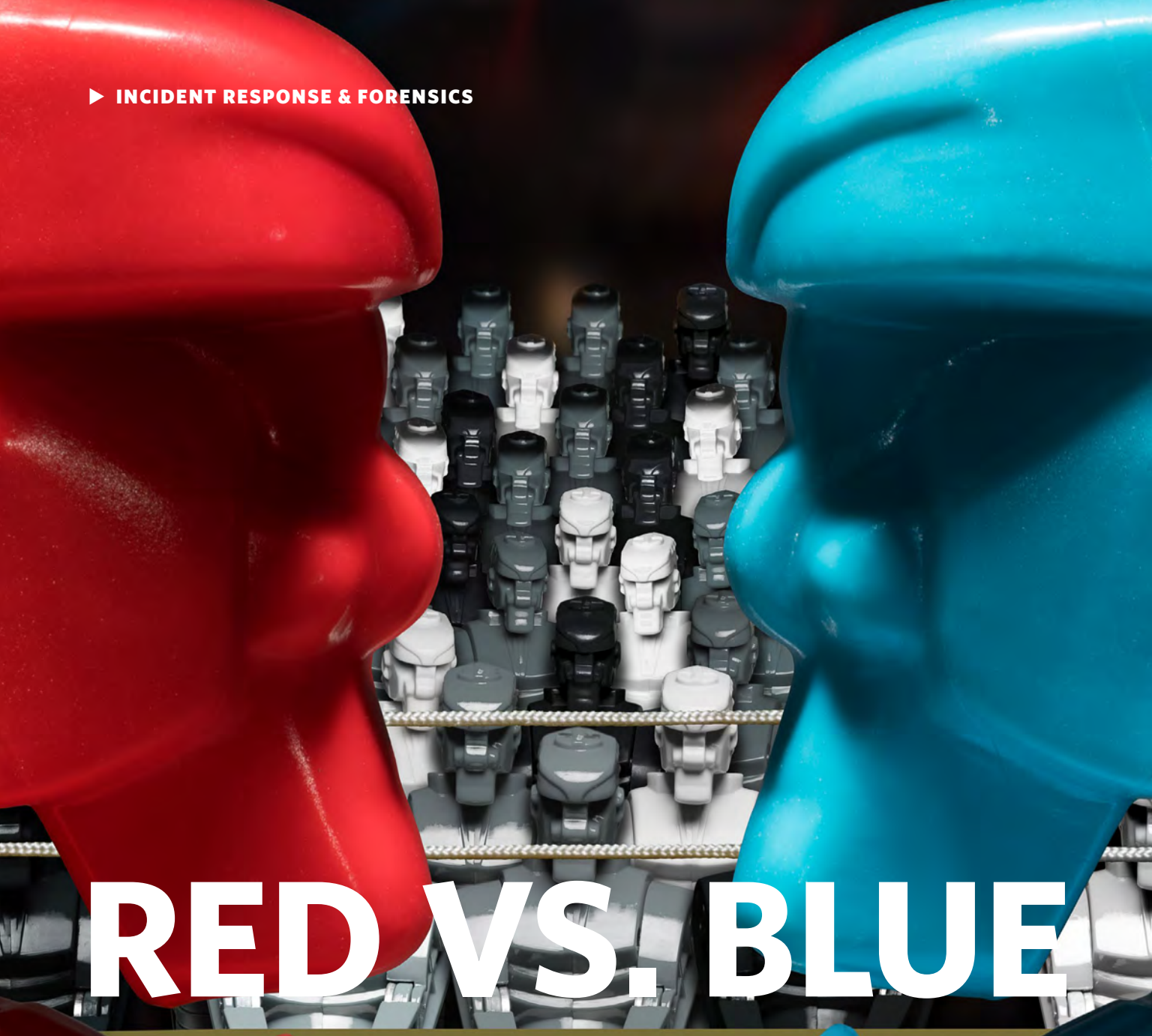
In Partnership with: image engine

Supported by: GovCERT.HK 政府電腦保安事故協調中心 | CSA cloud security alliance

Platinum Sponsors: 阿里安全 ALIBABA SECURITY | NTT Security

Gold Sponsor: ST Engineering Electronics





RED VS. BLUE

WHY PEN TESTING IS INCREASINGLY POPULAR AMONG ALL TYPES OF ORGANIZATIONS

BY PAUL SOUTH | With a toddler and a new baby at home, it's understandable that veteran cybersecurity professional Caroline Wong, CISSP, would draw an analogy from parenting when it comes to penetration testing. Wong is vice president for security strategy at San Francisco-based Cobalt.io and has worked in cybersecurity for eBay, Zynga and other firms.

IMAGE BY JOHN KUCZALA

"Three years ago, penetration testing was one out of every 20 engagements that we did. As of December, it's one of every three, or one out of every two."

—MICHAEL D'AREZZO, CISSP, CISA,
director of security services - GRC, SLAIT Consulting

"It's kind of like hiring a professional baby-proofer for your home when your kid develops from infant to toddler," Wong says. "Some parents do it themselves, others choose to outsource this activity to a professional. A professional will come into your home and examine it from top to bottom, identifying areas of weakness—accessible window on a second- or third-story floor, stairs without a baby gate, kitchen drawers that aren't locked, etc. They'll provide the parents with a list of vulnerabilities and a set of recommendations for how to take action."

In the cybersecurity community, the debate over how to pen test—internally or externally—is a hot topic, with the case for internal versus external testing drawing pros and cons from both camps. What makes this all the more intriguing is that the growth in the number of organizations to undergo such testing is a relatively recent phenomenon. But now retailers, banks and other organizations in fear of a widely publicized data breach are embracing penetration testing.

"At least now people are thinking about it," says Michael D'Arezzo, CISSP, CISA, a 20-year IT professional who has worked in cybersecurity for the last decade. "Ten years ago, people were like 'You want to do what? Secure my network? Why the hell would I want to do that?' It's gotten a lot better. The conversation's easier."

Still, for D'Arezzo, director of security services - GRC at Virginia Beach, Va.-based SLAIT Consulting, and partner Don Murdoch, GSE, MSISE, MBA, director of security services, the growth in pen testing has exploded.

"Three years ago, penetration testing was one out of every 20 engagements that we did. As of December, it's one of every three, or one out of every two," D'Arezzo says. "It's definitely made a lot of inroads. As such, we have a lot of competition, which is good. I appreciate the competition."

MORE ORGANIZATIONS SEEING RED

The reason for the growth? Organizations seem to grasp the correlation between network and application invasions and the bottom line. CEOs, CFOs and other executives now understand that major security breaches can impact jobs and profit.

First, a bit of background. Aside from red teams (attackers) vs. blue teams (defenders), there are other variations in the pen testing rainbow: black, white and gray testing. In black testing, the external pen tester is flying blind, with no prior knowledge of the organization being tested.

Black testing for networks is not uncommon. But for web applications, it is rare, D'Arezzo says. "It's almost like an unethical hacker, basically attacking some firm, but with their permission," D'Arezzo says.

White team testers work with an organization's network security team and its ins and outs, almost as if the tester had administrative-level knowledge to go after the network or application.

A gray level test fits somewhere in between.

"Gray level, I like to say, is a cross between black and white testing—'I know a little bit about your company, I know your IP address, meaning it's very easy to find your IP addresses based on your domain name,'" he says. "And once I find one IP address, I can find other IP addresses associated with that. Plus, I might have done a phishing campaign for that client. So, I might be able to come back to that client and say my phishing campaign was 15 percent successful, so I've established a capability for me to get a username credential and password credential.

"They'll give me a baseline username and password credential," he continues. "They'll create a test account, so I can monitor it. Then I use that to get in and test it. Gray pen testing is about 75 to 80 percent of all the testing I do."

For Dave Tyson, MBA, CISSP, CPP, the chief executive officer of CISO Insights, a global security firm with offices in the United States, Canada and the United Kingdom, pen testers are part of the cybersecurity equation. Organizations generally fit into two categories:

- Those with good security programs seeking flaws or testing the readiness of an incident response program
- Those that don't understand how bad a shape they are in.

Red vs. blue team exercises, Tyson believes, benefit an organization in three key ways.

First, they help build team skills and capabilities. They also provide a "real-world training ground" to test and measure individual development, which in turn assists in crafting employee development plans. And, they provide real threat information to build both general and specific awareness for executives.

FAILURE, AS APPLIED TO PEN TESTING

Make no mistake, pen tests fail. And the reasons for such failures are many.

"They have all failed," Tyson says. "No one has kept my

Continued on page 21

PEN TEST POINTERS

BY PAUL SOUTH | When it comes to penetration testing, one of the best ways an organization or pen testing firm can boost its red and blue capabilities is to build a quality squad. First-rate tech talent is a no-brainer, but what else does it take besides mad cyber skills to craft an effective team, either working internally or using an external provider?

WHAT ABOUT INTANGIBLES?

At its heart, obviously, is a commitment to teamwork. Dave Tyson, CEO of CISO Insights, says there are common threads in building successful defenses and in crafting the team dynamic for both defenders and attackers.

"It's about teamwork and personal responsibility," Tyson says. "Every team member has a role. Leaders must lead. Incident response teams must execute their plan. The infrastructure team must provide data to understand the anomaly detected to determine if it's an in-process intrusion."

For organizations with the size and financial muscle to do so, Tyson suggests a taste of real life.

"Consider starting in a 'live fire range' that is set up with your configurations and work multiple exercises until you get the basics down. Then, bring in multiple red teams to see how you react to different attack types."

Tyson has deployed red teams composed of former law enforcement and military cybersecurity pros, academic researchers and "hard-core pen testers; that's all they do," Tyson says. "All three [fields] have value and take different approaches to the problem, and have different tools and tradecraft to get in."

DO YOU NEED A READY-MADE PEN TESTING SUPERSTAR?

Caroline Wong, CISSP and CEO of Cobalt.io says, "Consider hiring someone who might not be your ideal candidate right now, but whom you believe you can grow into being your ideal candidate. This might be an engineer with limited security experience or knowledge, or a more junior pen tester that wants to grow. Given the difficulty of hiring experienced, already employed, expensive talent by pulling them from somewhere else, consider 'growing' your own internal pen test team in-house by hiring smart, curious, hard-working, fast learners and providing them with the tools they need to be successful (training, etc.)."

WHAT ARE THE CRITICAL QUALITIES?

Across the board, passion and integrity are critical, whether your team wears a red or blue jersey. The ability to unflinchingly and diplomatically speak truth to power—even if it involves hard truths about network and app vulnerabilities—is a pen tester's most valuable attribute.

"You always want to be known for your integrity," Michael D'Arezzo, CISSP, CISA, of SLAIT Consulting says. "Integrity is key. Our currency is integrity and information. Information is something that you can gain more of, but once you spend your integrity, you're all done."

ARE BLUE TEAMS NECESSARY?

Don Murdoch, GSE, MSISE, MBA, chief security architect at SLAIT Consulting, thinks they are a must. An effective blue team must possess "lateral thinking, the ability to pivot from one data source to another and strong ability to research what the source events mean, and just as strong an ability to connect the dots of one data source to another data source and why."

Wong agrees: "Blue teams are important. Today there's a recognition that attacks will happen, and are happening, all the time regardless of whether they're known and planned by security teams as in a red teaming exercise or if they're an actual attack by a malicious party. It's critical that teams are prepared to respond and practicing their responses processes."

AND DON'T FORGET PREPARATION

As the old saying goes, luck happens when preparation meets opportunity. Wong and colleague Mike Shema, vice president of security operations and research at Cobalt.io offer these thoughts on how to prepare:

- **Define goals.** What's being tested? Whether a red team can find an exploit that works? Or

whether they can escalate privileges across trust zones? What controls might be involved that should be helping the blue team?

- **Define success criteria.** What makes the red team effective in this case? Is it access, or time taken to gain access? When can they stop?
- **Budget time for a postmortem.** Review the gaps that the red team exposed. But also take time to discuss surprises or unanticipated events that may challenge your expectations about where you thought risk was in your organization. In the modern world of shadow IT and ubiquitous adoption of various types of cloud services, you may discover data exposures that weren't even on your radar at the beginning of the exercise.

REMEMBER THE POWER OF SURPRISE

Don Murdoch says that unannounced attacks are most effective in maintaining blue team preparation and vigilance.

"Multi-factor authentication is a powerful tool, not tremendously expensive, and provides significant protection. If you go with 'announced tests,' the vigilance gets pumped up and the bad guy is often caught. I favor no prior announcement; rather, I favor a set of practices that should find an attacker," he says.

AFTER THE SMOKE CLEARS, THEN WHAT?

Regardless of team rosters, what's important is how attacked organizations respond to pen test results.

"There are almost always failures. This kind of data generally evokes a strong response to closing the holes found," Tyson says. "The question is, does it evoke a response to change the process that allowed the hole in the first place."

Consider Murdoch's words when examining how firms generally respond to exposed weaknesses in the wake of a red vs. blue test, a last point worth pondering.

"For the engagements I've done, it's a 50-50 proposition. Some clients take the recommendations to heart and we don't see them again. Some do not." ■

From page 19

red teams out, but it depends on the scope (of the tests). The best tests are black box, where there's no previous knowledge of the tests, no internal knowledge of the environment to the testers. These are true live fire."

Most of the intrusions, he adds, come from unpatched technical flaws, such as a backdoor in a web-facing technology left open, or human weakness.

D'Arezzo agrees that not understanding the scope of the test, or an organization not having thorough knowledge of its infrastructure, can impact success or failure. But overconfidence can also play a role in pen test outcomes.

"Those people who are overly confident probably don't understand how things work, like the permeability of a network. Just in sending a phishing campaign, they have this, 'You can't get past my perimeter' attitude," D'Arezzo says. "I tell them, 'You don't have security, you have yourself an armored Jell-O mold.'

"You may be confident about the external side of your network, but the inside of it is just butter. It's just warm butter. And I'm going to be a hot knife going right through it, because you don't have layered defenses. You don't have a firewall separating your internal network from your data center. You don't have IDS or IPS. You have antivirus and you barely keep that up-to-date."

Overconfident clients also are common. "Those are usually the ones where you find the critical findings, or you find the cross-site or SQL injection issues."

D'Arezzo's colleague at SLAIT Consulting, Don Murdoch, points to structural weaknesses when defensive failures happen.

"More often than not, we get in due to a configuration issue or a weak password," he said.

PEN TEST PREPARATION

On the other side of the coin, D'Arezzo says, organizations that worry about pen tests are generally better prepared.

"Those are the guys who are very secure. A lot of it is because they are worried about everything; because they're worried about different parts of the network; because they get that you can't boil the ocean."

Wong and colleague Mike Shema point out that how a red team enters a network or app is not as critical as what the attacker does once penetration is achieved.

"Just getting in isn't necessarily a measure of failure for the blue team. I usually try to focus on aspects like whether the blue team can retrospectively re-create the attack chain, whether they had visibility into the compromised

systems, and whether monitoring and alerts were effective or could be made more effective," Wong says.

Shema, vice president of security operations and research at Cobalt.io, adds, "The caution with that approach is that you want to avoid over-correcting for a specific technique used by a red team to gain that initial foothold. For example, it's probably not going to be helpful to watch for a specific exploit payload or just send phishing awareness reminders to employees. Instead, review how the blue team is able to find malicious and anomalous activity across systems—especially since the best exploit is having valid user credentials. Or set up a mechanism for employees to report and respond to phishing—including setting positive encouragement that if they've clicked on a link and then reported the phishing after-the-fact that such notifications will help security without incurring undue blame."

"I see red team and blue team exercises as friendly competition, where they're trying to test controls that the blue team has in place, as well as find out what they may be missing."

—CAROLINE WONG, CISSP,
vice president for security strategy, Cobalt.io

That brings us to a key question: Is it best to bring in an outside service provider, or to build a team from within?

Obviously, the size of an organization and budget are major factors. D'Arezzo, who has worked with organizations ranging from five to 20,000 employees, offers this advice for internal teams: Make sure members come with diverse skills and responsibilities.

"When I first started this practice three or four years ago, we just had network pen testers. I had no web application pen testers," he notes. "And at that point I was a mediocre web developer, so my skill level with web application pen testing was very, very low. I had to reach outside our team and hire a subcontractor at times."

From an internal company perspective, to build a red team, discern the skills members have and fill in where needed, especially to cover when someone is out on vacation. That means having members who are fluent in different IT areas—network, web applications, Windows, Linux, etc. Additionally, you need people who are truly committed to this kind of work.

"You've got to have a diverse team. You've got to have people who are passionate about different things and [have a] want and desire to keep everybody together," D'Arezzo explains. "The most difficult thing that I think about a red team is keeping cohesion. In my experience I've seen a lot of alpha personalities when it comes to pen testing. There are a few people who are modest and humble about their skills, and those guys are really, really sharp in my experience. It's hard to tie everybody together if they have very strong personality types."

Beyond technical prowess and passion there are other key attributes: integrity, communication skills and the ability to document thoroughly and clearly, both in speech and in writing.

"You have to find a way to say, 'There are some challenges here. There are some opportunities here. We were able to do this, this and this.' … Just telling somebody, 'Good luck with that' is not very helpful."

And while writing end-of-exercise reports may not be fun, it's vital, D'Arezzo says.

"At the end of the day, regardless of if you are an internal red team or a third-party red team, no matter what you found on the network or within a web application, it only matters what the report says. Report writing for a pen tester is probably the most important thing."

He adds: "The ability to communicate to chief executives is important, but only for your lead communicators and your project managers. But report writing is the most difficult thing for most people to do. It's the least sexy part of the game. It's the end result that nobody wants to do. But if you become good at it, you will be very successful."

In a world where both white hat and black hat hackers are in demand, sanctioned pen testing can be among the most useful gauges of an organization's security posture.

"An organization that isn't testing itself is nonetheless already being, or soon to be, tested by others, with or without that [organization's] knowledge," Mike Shema says. "Doing some sort of testing is a baseline necessity. Maturity comes into the equation in the way blue teams and the organization is able to detect and respond to compromises. Maturity for red teams can come from testing fundamental security stances and architecture improvements."

Wong sees pen testing as preparation for when not-so-friendly forces appear on the cyber horizon.

"I see red team and blue team exercises as friendly competition, where they're trying to test controls that the blue team has in place, as well as find out what they may be missing," she says. "They're more competing against the internet and whatever threats are coming against the organization. It's a way to stay in practice and stay in shape so that when an incident does occur, the blue team can better respond, and the red team can better learn an attacker's techniques." ■

PAUL SOUTH *is an editor for* InfoSecurity Professional *magazine.*

chipping in

A member reviews EMV® 3-D Secure, the newest solution to e-commerce authentication

BY DAVID L. DANN, CISSP

ILLUSTRATION BY ENRICO VARRASSO

ACCORDING TO RSA's Anti-Fraud Command Center, global losses from e-commerce fraud in 2017 amounted to $660,000 every hour. The problem has worsened, rather than improved, in the United States since credit and debit card providers introduced "the chip" or EMV payment cards, which on Oct. 1, 2015 shifted liability for fraudulent point-of-sale transactions from a merchant's bank to the merchant itself.

That e-commerce fraud worsened after the migration to EMV was predictable; Europe and Asia experienced similar increases in card-not-present fraud after their adoption of chip cards and point-of-sale terminals. Since they were first introduced in France in 1993, so-called chip cards, unlike payment cards with magnetic stripes, have proven extremely difficult to counterfeit, given someone would need to crack the cryptographic secret stored in the chip. That makes for excellent authentication at the point of sale. And those point-of-sale transactions where the cardholder must enter a PIN and not a signature helps verify that the cards have not been stolen.

But online purchases—which continue to grow exponentially worldwide—are done without such devices or authentication mechanisms. Therefore, fraudulent purchases remain a major concern.

There are several solutions to this authentication problem, and one of them is EMV 3-D Secure. Version 2.0 of this XML-based messaging protocol provides for stronger risk-based authentication of payment cards used for online purchases. The intellectual property rights to the protocol are owned by EMVCo, a company jointly owned by the major payment card brands and the owner of the specification for EMV cards and terminals. Both Visa and Mastercard have implemented EMV 3-D Secure in their services, Verified by Visa and Mastercard's SecureCode.

Version 1.0 of the protocol had serious drawbacks. The most serious was that it resulted in a high rate of false declines. A false decline is when a customer's transaction is rejected because of inaccurate and incomplete information about the cardholder. False declines for merchants can result in revenue losses greater than those from fraud.

To date, no online authentication mechanism is foolproof, but version 2.0 of EMV 3-D Secure is a step in the right direction.

Another concern for merchants is cart abandonment, which occurs when a customer finds the checkout and payment process too onerous and never completes the sale. Version 2.0 is much improved and addresses these problems. In addition to expanding support to mobile apps and not just web browsers, it provides real risk-based authentication that results in the easy, elegant and frictionless transactions that users expect in e-commerce.

To that end version 2.0 has an expanded dataset that includes the customer's IP address, codes that describe product or service types, and length of time that the cardholder has had the account. These data elements combine card issuer and merchant knowledge of a customer to provide a more accurate risk measurement that reduces the rate of fraud, cart abandonment and false declines.

The architecture of EMV 3-D Secure consists of three domains: the card issuer; the acquirer or merchant domain; and the interoperability domain, which is the infrastructure that supports the payment system and includes the ACS (access control server).

To illustrate how this works, let's create two personas: Buyer Alice and Merchant Bob. Alice, a frequent shopper at Bob's online shop, Widgets R Us, makes a purchase. The card issuer's data on Alice's usage of her payment card, together with data from the merchant domain on Alice's shopping history at Bob's store, is all used to produce a holistic risk assessment metric. Alice might only be prompted on-screen for a onetime password if that risk rating was high for an anomalous situation, such as an IP address showing her purchase is being made from a location that would be unusual for her or if the dollar amount of her purchase at Bob's was unusually high.

EMV 3-D Secure also offers a benefit for merchants in meeting regulatory compliance. For instance, the European Commission Second Payment Services Directive (PSD2) mandates strong customer authentication (SCA) be implemented for electronic transactions. Merchants are not mandated by the card brands to enroll in EMV 3-D secure; however, failing to do so means they may miss out on a key inducement: the fraud liability for transactions that travel across the 3DS environment shifts from the merchant to the card issuer.

To date, no online authentication mechanism is foolproof, but version 2.0 of EMV 3-D Secure is a step in the right direction. As more consumers and businesses purchase goods and services online and particularly while using mobile apps, the risks associated with fraud will also rise. EMV 3-D Secure is worth investigating as a possible solution for anyone seeking more secure online sales while reducing the risk of fraud-related financial losses. ■

DAVID L. DANN, CISSP, *works on payment card and payment system security for private and public sector clients in Washington, D.C. He wrote about web security for the magazine in 2015.*

LEARN THE LATEST ON EMV 3-D SECURE

The Official EMVCo Site

Gain a better overview as well as detailed SDKs for the latest specifications to support secure new payment channels.

https://www.emvco.com/emv-technologies/3d-secure/

RSA Explainer on the Protocol

This blog post from RSA explains what's new with EMV 3-D Secure and why merchants should consider using it for online transactions.

https://www.rsa.com/en-us/blog/2018-04/3-d-secure-2-what-the-protocol-means-for-merchants

First, Do No Harm

Defending our systems with continual patching may be creating more vulnerabilities than we know

BY BARRY DOWELL, CISSP

"First, do no harm" is one of the guiding tenets of the medical profession. But it is a phrase that we as IT security professionals should fully follow in our work.

Over the last several years, the IT security world has become exceedingly familiar with the concept of "zero-day vulnerabilities" and a never-ending cycle of patching and updating systems to protect against those vulnerabilities and mitigate against other potential risks to our systems. The problem is that we frequently forget to practice what we should preach—completely weighing the risk of the patching against the potential for a compromise of the systems we are patching.

PHOTOGRAPH BY JOHN KUCZALA

PREPARING FOR THE WORST

In April 2014, the security bug Heartbleed became known to the world. In response to a furor in the IT arena, vendors and software manufacturers rushed to push out patches that would address that vulnerability. C-level management became aware of the vulnerability thanks to industry news sources and even non-industry news sources including newspaper, TV and radio reports. Of course, having heard the alerts about the serious nature of that bug, orders came in from the security operations centers and vulnerability management teams that patches needed to be deployed as soon as possible.

Within the organization where I work, vulnerabilities are rated by risk and criticality for patching purposes. Critical vulnerabilities are required to be patched within a relatively short window of calendar days. While mission-critical systems may be able to defer patching for a short period of time, the expectation of the C-level individuals or the system owners whose names are directly associated with the risk for these systems is that patches will be applied as soon as possible, oftentimes forgoing a testing cycle that would allow for confirmation that the patches and updates are not bringing more problems than they were supposed to fix.

Even with appropriate time for patching, organizational budgetary concerns may limit a validation environment that adequately supports a production environment. Such was the case within the organization where I work. The development/testing environment was closed off from, and not exactly like, the production environment.

We had the luxury of having a production system that was replicated on a scheduled basis to an alternate system, but the equipment in use in the production environment was not the same as it was in the dev/test environment. Within the production environment the replication between the primary and alternate systems was expected to mean that patching either of those systems *should* have been a non-issue. Worst case, a recovery copy was always available.

Of course, not many organizations have the funds to pay for an exact replica of their systems, so you may wind up having to use equipment to create a reasonable facsimile for your testing purposes. For example, you may not have the same storage technology in use in your development and testing environment as you have in your production environment, though in most circumstances it would be close enough to allow you to test a "typical" system update or patch for potential negative impact.

THE PRICE OF SPEED

In a series of events that somewhat mimic the plot of the book and film *The Perfect Storm*, orders came down to patch systems against the "critical" rated Heartbleed bug. That perfect storm included a mix of VMware and a storage array and data access that can only be described as "touchy." VMware published a patch that was expected to mitigate the Heartbleed bug. When it was first available, there was no expectation of any bad results for customers that were using the combination that my team used within the environment we were responsible for managing and supporting.

Unfortunately, within just a few days of deployment of the VMware patches, VMware discovered problems with the patch that had become evident under specific circumstances. (We later learned that specific storage access methods were the primary culprit.) Even more unfortunately, VMware discovered this problem after my team had to try to determine why our production environment was suddenly completely out of service, with a serious data corruption problem having become evident.

As noted previously, this was a perfect storm event. Even the best-laid plans can be fouled by not exercising sufficient caution and due care. There was a replica system available and in use that had not yet been patched with the buggy update. But the data corruption that had been occurring meant corrupted files had been replicating between the primary system and the alternate system, making data recovery a more complex task. Thankfully, snapshots from the days prior to the deployment of the patch were available and were used to help return to normal operation.

In the end, hundreds of hours of labor were expended and days of operational time were lost. All of which may have been avoided if a "Go, go, go!" mentality hadn't been in effect at the higher levels in the vulnerability management and security operations center.

A NEVER-ENDING CHALLENGE

You may be reading this and thinking, "Gee, Heartbleed was a long time ago. Why are we reading about this topic now?" Besides the "first, do no harm" mantra, most of us are also familiar with the proposition that history often repeats itself. Take Meltdown and Spectre, for example.

In early 2018, Intel and its partner vendors, including Microsoft, VMware and others, as well as Intel competitor AMD, blasted out a round of patches and updates to address Meltdown/Spectre that called into question just how much quality assurance was going into the development of those patches. Patches and updates were made available, then were recalled or replaced with new patches when random reboots, blue screens and other negative results including serious impacts upon system performance were experienced after applying those updates.

These issues don't just occur with system-level patching and updating, though an update to a VMware system most certainly is a much higher risk than an update to an application such as Microsoft Word. Some of us may be very familiar with application updates that have resulted in unintended consequences on our systems. For example, updates to anti-malware applications such as Symantec Endpoint Protection or Malwarebytes have been known to falsely identify critical system files as compromised with those files quarantined or removed from the system. Upon

reboot, the systems become inaccessible and hours of effort may be needed to recover the system from backup or a previous system restoration point.

While that problem sounds small, in an environment where hundreds of systems are updated and rebooted before the problem is identified and stopped, many hours of manual effort may be needed to get everything back to normal (and of course fighting with the vendor for reimbursement for those efforts is not likely to result in any satisfaction).

Equally important: communicating the difference in risk for patching a typical workstation, which is likely an interchangeable item in your environment, as compared to the risk of patching a system that your entire organization may be dependent upon (a VM environment, for example). While patching a workstation is fairly trivial and in a worst case you would probably easily be able to replace a workstation with a newly imaged system, replacing an entire organization's VM environment and especially the data within may be a monumental task.

SETTING BEST PRACTICES

As security engineers, systems administrators, or even as information system security officials, we owe a duty to the systems under our care to make sure that we don't cast aside the best practices we would otherwise be using. Insisting on leaving adequate time in patching cycles to fully research and test patches that we are about to deploy must be something we communicate to the people that make the decisions about the risks they are willing to accept. Without explicit communications among all participants there can be disastrous results and worse—over time it gives the users we support reasons to fear patching and updating that we should be doing.

We need to make sure that from the C-level down we are balancing the risk of harm from buggy updates and patches against the risk of compromises and exploits of the systems we are managing. Should we ignore patching and updating or put off patches indefinitely?

We all may be aware of systems that may be operating under those circumstances, but the answer is most definitely and enthusiastically "NO!" Patching certainly needs to be done, but taking a little longer to make sure that we are not harming systems and negatively impacting operations is a goal we should all be meeting. ■

BARRY DOWELL *is an information systems security official working as a contractor for a U.S. government agency. He has worked for that agency for more than 15 years, the majority of which were as a systems engineer and information systems security official. Barry obtained his CISSP in 2015.*

TechTarget | SearchSecurity

It takes minutes to compromise a system.

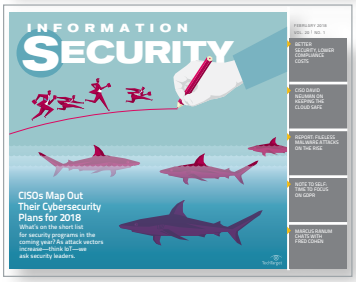
Only seconds to be better prepared.

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

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

- Remaining compliant with new **GDPR requirements**
- Using **machine learning** and **AI** to detect threats
- Regaining control of **data protection** in the cloud
- Emerging **security threats** from every which way
- Strategies for **perimeter network security**

Get Free Membership



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

* 2016 Verizon Data Breach Investigation Report

FOCUSING ON EDUCATION AND RESEARCH INITIATIVES

center points

BY PAT CRAVEN

Garfield More Popular Than Ever at 40

IF YOU'VE PASSED THE MILESTONE, then you know turning 40 years old can be traumatic. "Over the hill" is the common expression. People tell you that you are "on the backside of life" or other depressing things that conjure images to make you believe your life is nearly over. But if you're a lazy cat turning 40, the typical things might not faze you. If you had nine lives, I guess you could live the charmed life of our old friend, Garfield, the cartoon cat.

Since Garfield joined our team at the Center for Cyber Safety and Education (here is the video of how it came about if you missed it), some people have asked about Garfield's relevance and popularity today. "Is he still as big today as he was when I was kid?" is a common question. The answer is "Absolutely YES!" And I don't mean just his waist size. In fact, with so many new media outlets, he could be bigger today than ever.

Growing up, you only found him on the Saturday morning cartoons and in the Sunday comic strip in the newspaper. Today, he is all over social media, with 20 million followers and 5.6 million page views a month on his website. People have downloaded his games and apps more than 85 million times. There is even a new app available in Dubai called Garfield Eats, where you can order Garfield-inspired food like lasagna and have it delivered to you. He's been in two major motion pictures and is working on a third. An accomplished author, he has sold more than 200 million books. Not bad for someone that likes to sleep and eat his days away.

Garfield's popularity is international. His comic strip is the most popular in the world, with some 200 million readers a day in 80 countries and 40 languages. So, he may just be hitting his stride.

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

It was this kind of worldwide popularity that drew the Center to select Garfield as the face of our children's internet safety program. Every teacher I speak with is in awe of how attracted the students are to him. When they start the cartoon, the room falls silent. Who wouldn't want to watch a Garfield cartoon at school? One teacher recently sent us a letter that read, "I have never had a group of students this age be so engaged in an extracurricular program the way they were engaged in this one. Thank you and thanks to Jim Davis for the effort you have made to keep our children safe."

What all this boils down to is we have a rare opportunity before us to make a difference in the world, to make it a better place for children and to keep them safe, all thanks to a crazy, lazy cat who has been entertaining us for 40 years.

As adults, we love Garfield because we can relate to him—he's honest (and wise) about the very human topics of everyday life. Children love Garfield because he is like them—smart, funny, mischievous. What all this boils down to is we have a rare opportunity before us to make a difference in the world, to make it a better place for children and to keep them safe, all thanks to a crazy, lazy cat who has been entertaining us for 40 years. Now is the time for us to use Garfield's nine lives to make someone else's life better.

Learn how you can get involved now at www.iamcybersafe.org/get-involved. ■

Center Celebration Riverboat Cruise

Tuesday, Oct. 9 • City of New Orleans Riverboat • 6pm

Add **The Center Celebration** to your Congress registration or purchase separately.

JOIN US to CELEBRATE

CRUISE THE MISSISSIPPI

LIVE MUSIC GREAT FOOD

PLENTIFUL LIBATIONS

$100 Early Bird (through July 31st)

$125 Regular (after August 1st)

congress.isc2.org

CENTER FOR CYBER SAFETY AND EDUCATION

iamcybersafe.org

All proceeds benefit the Center for Cyber Safety and Education's children & adult cyber safety programs.

Highlights from recent discussions on the (ISC)² online forum for cybersecurity professionals

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

QUESTION:

Why is security the last to know?

Why is it that security professionals are not engaged at the start of new initiatives either internally by their own organizations or via clients? Is it because we frighten people? Don't want to spend money on security? [All of] which normally results in a high-intensity catch-up…. Security is a business (business, people and technology) problem, adding additional technology, which does not integrate with the organizational security framework and how it operates, just exasperates the situation as we all know. Answers and points of view would be appreciated.

—*Submitted by Caute_cautim*

SELECTED REPLIES:

- It is easier to ask for forgiveness later than to get permission first.
- I didn't want to be told no.
- You guys always kill or slow down our projects.
- Oh. I forgot.

Those four excuses are what I hear the most. So we have to get away from being known as the department of "No!" You have to start becoming an innovative security practitioner and finding ways to get invited to the early meetings. Make yourself available. Ask that you be brought in early and if you are not needed you can bow out gracefully.

—*Posted by CISOScott*

Ultimately whether you are talking a small business or a multi-national conglomerate, we love to leap before looking. But the issue isn't that developers or executives don't come to "us" earlier. It is that our skill set is not part of their training and experience.

—*Posted by JoePete*

I have been doing a lot of third-party assessments/due diligence projects, and people were always complaining that I needed documentation rather than just signing off on a purchase. A few years later, and some bad apples weeded out among third parties, they now understand that the additional two weeks of prep work will save a lot of headaches later on.

—*Posted by kratzy11*

Find this complete and updated thread here.

QUESTION:

New NIST Password Standards

I wanted to see how members feel about the NIST new draft of password policy suggestions. [NIST draft recommendations include 8-character minimum/64-character maximum; elimination of forced character combinations such as requirements of capital letters, numbers, etc.; no mandatory expiration.]

—*Submitted by Matthew*

SELECTED REPLIES:

I got rid of password aging seven years ago. I have been telling auditors I don't make passwords expire because doing so decreases security. It's good to see NIST coming out with advice that passwords should not be changed every 90 days and that longer is better.

—*Posted by n5rmj*

No matter how much we talk about changing passwords, or minimum/maximum lengths, or using passphrases instead of passwords, etc., without enabling multi-factor authentication, passwords will always be weak.

—*Posted by RaymondFrangie*

If you are going to abide by the recommendations made by NIST to jettison expiration and outdated password complexity rules in favor of user-friendliness—it requires that you introduce new password encryption standards and require multi-factor authentication for any service involving sensitive information. Industry will have to layer up.

—*Posted by canLG0501*

I'm in favor of forcing users to periodically change their password. Some users will quite openly volunteer their password with the littlest of encouragement. In areas that have high staff turnover or take on students for temporary assignments, changing passwords is essential, even if it is an incremental change. That's better than the alternative.

—*Posted by Wolf*

Find this complete and updated thread here.

CONTENT CREATION SERVICES FOR MARKETERS

Are you short on time or in-house talent and need help?

Get expert white paper writing and design services

Boost your credibility and establish yourself as an authority on cybersecurity using words and images unique to your brand.

Twirling Tiger Media can help you create engaging white papers—on time and on budget.

We can help you get started today. **I'm ready!**

TWIRLING TIGER™ *media*

creators of content you can sink your teeth into

Contact Gordon Hunt at ghunt@twirlingtiger.com or call (919) 816-6876

Twirling Tiger Media is a WBENC-certified Women's Business Enterprise