SECURITY CONGRESS 2020 GOES ONLINE

InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

SEPTEMBER/OCTOBER 2020

IT'S TIME TO Tidy Up

How to rid IT systems of unwanted and potentially dangerous legacy OSes and dark data

+

Grappling with Election Security and Disinformation Campaigns

EPISODE 3 OF PERRY CARPENTER'S SERIES

Turning to Marketing to Change Human Behaviors

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

BE THE CYBER HERO OF OUR FUTURE GENERATIONS

DONATE

to cyber safety education

Text **CYBER** to **26989**

or visit **IAmCyberSafe.org/give**

INTERNATIONAL & CRYPTOCURRENCY DONATIONS ACCEPTED

A copy of the official registration and financial information may be obtained from the division of consumer services by calling toll-free within the state. Registration does not imply endorsement, approval or recommendation by the state. Florida License: CH37114 Call: 1-800-435-73521 www.FloridaConsumerHelp.com

contents

VOLUME 13 • ISSUE 5

... IT ALL COMES DOWN TO MESSAGE AND PRODUCT.
MAKE YOUR MESSAGE MEMORABLE ... AND REMEMBER
YOU'VE GOT A PRODUCT TO SELL.

PAGE 27

features

SYSTEMS MANAGEMENT

18 **The Career-Changing Magic of Tidying Up**
Turning to organizational experts to rid IT systems of unwanted and potentially dangerous clutter.
BY ANITA J. BATEMAN, CISSP

DATA MANAGEMENT

23 **Protecting the Unseen**
Just as dark matter makes up most of the universe, dark data is also in the majority. Protecting it depends on illumination, understanding and enlightened policy.
BY MATT GILLESPIE

SECURITY AWARENESS TRAINING

27 **A 'Fogg'y Notion and a Nudge**
A marketing executive schools the team at Acme Corporation on human behavior theory.
BY PERRY CARPENTER

Cover image: JOHN KUCZALA Illustration above: TAYLOR CALLERY

departments

4 EDITOR'S NOTE
It's Getting Really 'Stuffy' in Here
BY ANNE SAITA

6 EXECUTIVE LETTER
Crisis as a Culture Test
BY WESLEY SIMPSON

8 FIELD NOTES
Early bird pricing ends soon for Security Congress 2020; election security; disinformation and misinformation campaigns; a new way to view the CIA Triad; and much more.

16 MODERATOR'S CORNER
Just Because You Can, Doesn't Mean You Should
BY BRANDON DUNLAP

31 CENTER POINTS
Teaching Cyber Safety Post-COVID-19
BY PAT CRAVEN

32 COMMUNITY
Advice on blacklisting IP addresses, prep for the CISSP exam, effective endpoint protection

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

editor's note | *by Anne Saita*

It's Getting Really 'Stuffy' in Here

IF YOU'VE EVER RELOCATED to a new region or dramatically downsized living quarters, then you know the physical, financial and psychic toll paid for owning too much "stuff." Stuff has a way of filling in spare floor or wall space, taking over closets, cabinets, drawers, shelving and desks. It charms humans into holding on to it by pulling on sentimental strings or redirecting intentions to more immediate needs. It convinces people to rent expensive storage units instead of giving it the boot. It strains relationships when allowed to proliferate unrestrained or be dumped or donated without permission.

Then there's the "stuff" that resides within our databases and desktops and laptops and tablets and smartphones and hard drives. We're talking about all those files that we know we no longer need but keep anyways. Thousands of old email messages that sit idle for years. The cloud was to provide safe storage, so we felt less angst clicking "Delete." But cloud data sprawl is a real issue now, too.

Still, there's something almost spiritual that comes from a major purge. That's why we're devoting two of the three features in this issue to clearing IT systems of unsupported software and dark data that can cause potential harm. Finally, we return to the characters of Acme Corporation, to discover what they learn from their SVP of Marketing to get people to actually internalize security best practices. Like getting employees to properly dispose of useless data.

There's another way that we can eliminate and disallow junk to infiltrate our lives, and that's through careful consideration of what we read, listen to and watch. We touch on this in a Q&A with Theresa Payton, a former Security Congress keynote speaker who's written a book called *Manipulated: Inside the Cyberwar to Hijack Elections and Distort the Truth*. It's a good read, or one you might listen to while you clean up your space. ■

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

©Rob Andrew Photography

ADVERTISER INDEX

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

Center for Cyber Safety & Education	2
2020 Cyberthreat Defense Report	5
(ISC)² Virtual Security Congress 2020	7
Forescout	13
(ISC)² Vulnerability Central	14
Security Engineered Machinery (SEM)	15
2020 Cloud Security Report	17
(ISC)² Global Official Training Providers	22
(ISC)² CCSP Exam Action Plan	26
(ISC)² Professional Development Institute (PDI)	33

InfoSecurity PROFESSIONAL

(ISC)² MANAGEMENT TEAM

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

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

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

CORPORATE COMMUNICATIONS LEAD
Kaity Pursino
727-683-0146
kpursino@isc2.org

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

TWIRLING TIGER MEDIA MAGAZINE TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

EDITORIAL ADVISORY BOARD

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

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

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

RETURN TO CONTENTS

(ISC)²

The Latest

Trends & Insights in IT Security

The seventh annual Cyberthreat Defense Report is now available. Get an in-depth look at how IT security professionals perceive – and plan to defend against – cyberthreat.

CYBEREDGE GROUP
2020 Cyberthreat Defense Report
North America | Europe | Asia Pacific
Latin America | Middle East | Africa
« Research Sponsors »
PLATINUM
GOLD
SILVER

2020
Cyberthreat Defense Report
Sponsored by (ISC)²

The research reveals:

- A record 81% of organizations suffered from a successful cyberattack last year
- 85% of organizations are experiencing a shortfall of skilled IT security personnel
- 36% of IT security applications and services are delivered from the cloud

How do your priorities and security posture stack up against your peers? Use the 2020 findings and find out.

Get the Report

Crisis as a Culture Test

by Wesley Simpson

A STRONG CORPORATE CULTURE doesn't always show itself to be an asset when business is booming, but in times of crisis, it quickly becomes apparent whether or not your organization has such a firm foundation.

In spite of the many challenges facing organizations, business rests for no one. And investments made in building a culture of accountability, unity, collaboration, compassion and agility will pay off when serious setbacks occur. But rather than thinking about how to get through this until tomorrow, a crisis like the pandemic we're experiencing can also be an opportunity to improve processes and culture and shore up the weak spots. The COVID-19 global outbreak forced organizations everywhere to examine their communications with employees and customers, as well as their remote-work policies, and come to some conclusions about their cultures' sustainability under sudden and prolonged stress.

I've been extremely impressed by how our entire (ISC)² team responded to the pandemic, from all corners of the globe. As an organization, we were fortunate to have invested in recent years in the digital transformation of our infrastructure, which enabled us to virtually overnight shift our entire workforce to remote environments and continue to support our members with no service interruptions. Having a culture that values innovation enabled us to do that, and having an employee base that was flexible and willing to adapt to change made the process as painless as could be expected.

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

We also launched our Professional Development Institute in 2019 on a cloud-based LMS platform, because continuing education and learning is also a part of our culture. When the crisis hit and physical conferences and trainings were no longer possible, we had a portfolio of 36 world-class, on-demand digital courses available to our members at no cost to help them continue their certification and training journeys. Our team also demonstrated a culture of agility in reworking project plans in order to improve our members' online experiences. And in the midst of the pandemic, we stood up an enhanced member portal, made extensive changes to our (ISC)² online Community and created several discounted training bundles—all because our culture calls for a commitment to member satisfaction.

Culture is what guides a company before, during and after a crisis. It determines public perceptions and brand identity. In reassures employees and customers to stick with you through tough times.

> **When the crisis hit and physical conferences and trainings were no longer possible, we had a portfolio of 36 world-class, on-demand digital courses available to our members at no cost to help them continue their certification and training journeys.**

COVID-19 reminds us that corporate culture is a key factor in achieving success, as well as attracting and retaining a qualified workforce. And it's also among the most difficult tasks to take on.

By investing in developing employee and membership experiences, beliefs and actions, you can yield the long-term results you need to be resilient. When done well, an employee- and customer-centric culture will become part of your company DNA.

Like cybersecurity certifications, a strong corporate culture requires ongoing effort and maintenance, not one-and-done checklists. A crisis-hardened culture takes time, commitment, leadership and daily effort, but it can pay off when you need it most—as it certainly has in our case. ■

RETURN TO CONTENTS

field notes | EDITED BY DEBORAH JOHNSON

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

2020 (ISC)^2 Security Congress More Accessible Than Ever

The 10th annual conference is virtual this year

THE ANNUAL (ISC)^2 SECURITY CONGRESS will be held entirely online Nov. 16 to 18 in response to public health concerns related to the ongoing COVID-19 pandemic. By going virtual and greatly reducing the pricing, more (ISC)^2 members, associates and peers from around the world will be able to attend 40-plus exclusive, virtual sessions and keynotes while earning up to 45 CPEs.

"This year is bittersweet in a lot of ways, and although we're disappointed that we won't be able to see our colleagues and members from all around the world in person, we're excited to embrace this new online format for Security Congress," said Wesley Simpson, Chief Operating Officer for (ISC)^2. "All of this expert discussion, insight and peer-to-peer engagement is now more accessible than ever before to professionals around the world. As a virtual event, Security Congress will bring the global cybersecurity community together as we close out one of the most challenging years our profession has ever faced."

(ISC)^2 Security Congress 2020 is offering heavily discounted Early Bird pricing to (ISC)^2 members and associates for just $295 for an All-Access pass. Non-members also benefit with Early Bird pricing of $395. Discounted fees end Sept. 30; the price jumps $100 after that date.

That pass provides access during the three-day event to:

- All sessions and keynotes
- The popular (ISC)^2 Town Hall meeting
- (ISC)^2 Networking Lounges
- (ISC)^2 Safe and Secure Online program information

The conference also will announce winners of the 2020 (ISC)^2 Global Achievement Awards for members and chapters that have made a significant impact on the cybersecurity community. Learn more about each award and how to enter at https://www.isc2.org/About/Award-Programs/.

Attendees will have an opportunity to earn an additional 16 CPEs through pre-conference, two-day training sessions the weekend prior to the conference opening. You can learn more about pre-conference activities at https://www.isc2.org/Congress. ■

(ISC)^2 Security Congress pricing goes up after noon U.S. Eastern time on Sept. 30. Here's a breakdown of costs per category of attendee:

Member
Early Bird: $295; Standard: $395

Non-Member
Early Bird: $395; Standard: $495

(ISC)^2 Retired
Early Bird: $295; Standard: $295

Government/Military – Member
Early Bird: $295; Standard: $295

Government/Military – Non-Member
Early Bird: $395; Standard: $395

Day Pass – Member
Standard: $125

Day Pass – Non-Member
Standard: $175

Photograph: Getty Images

RETURN TO CONTENTS

ELECTION SECURITY

Ensuring Every Ballot Counts in the Digital Age

Words of warning from a member about protecting our votes

BY SAURABH GUPTA, CISSP, CCSP

AS WE APPROACH the 2020 presidential election in the United States, the reliability and safety of the process is once again under intense scrutiny. Adding to the pressure: the increasing use of computer technology in the election process. The technology has been a boon in this time of COVID-19 social distancing and self-isolation, but it's also highlighted challenges to securing elections infrastructure.

Know and Protect the Vulnerabilities

With the increase in digitization, elections have become vulnerable to new threats and intrusions, requiring organizations to strengthen their platforms.

Critical assets such as campaign websites and voter registration databases need to be protected from ransomware, malware and distributed denial of service (DDoS) attacks that could not only prevent voters from accessing vital election information, but could actually affect the outcome of an election.

Key to protecting these critical assets are:

- Selecting and implementing appropriate security controls
- Hardening systems using secure configurations
- Provisioning access only to authorized users
- Testing applications to identify software bugs

Due to the large election ecosystems and potentially huge attack surfaces, security professionals are utilizing threat intelligence to identify and mitigate various threats.

Other steps to ensure security are:

- Building in redundancies to avoid single points of failure
- Using a content delivery network (CDN) to improve response time for voters across locations
- Regularly backing up data
- Segmenting networks
- Segregating applications using VLANs to enable high availability and prevent impact in case of any exploits
- Connecting administrative systems and public-facing interfaces through different networks to prevent DDoS attacks
- Filtering requests using firewalls to allow only authorized requests

Election Challenges Caused by the COVID-19 Pandemic

The COVID-19 stay-at-home orders and social distancing requirements have created potential security vulnerabilities in the voting process.

While online voting via a website or mobile app could be a safer option, there are vulnerabilities that can weaken the legitimacy of election results. Attackers can gain access to a user's device and intercept communication between the device and application server to discover the user's identity, IP address, or even alter the individual's vote.

To provide end-to-end security and voter-verifiable ballots, security measures can be implemented, such as biometrics to authenticate voters, encrypted communication applications, blockchain technology to store votes and hardware keys to encrypt voter information.

Electronic voting machines have increased the speed of vote counting but require high-level security to prevent diverting votes through malicious hacking. Verifiable paper trails are essential, as are post-election risk-limiting audits, a statistical technique using a manual count of a sample of votes to check for software bugs or malicious attacks. Microsoft has developed a free open-source software development kit called ElectionGuard. It utilizes a homomorphic technique that counts votes while keeping the votes encrypted. Voters will be able to independently verify with certainty that their vote is counted and not altered.

As the election process becomes part of the digital world, it is crucial to ensure its integrity and security. Educate campaigners and candidates through security trainings and equip them with security tools to safeguard their campaigns from digital threats. Protection of the election infrastructure is also crucial to ensure voter trust and confidence in the electoral process. ■

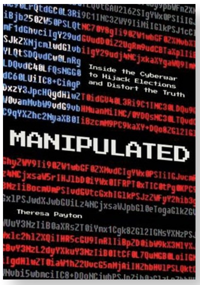
SAURABH GUPTA, *CISSP, CCSP, is a project manager at a technology company in the Seattle area. He wrote earlier this year about multi-factor authentication.*

Illustration: Getty Images

RETURN TO CONTENTS

ELECTION SECURITY

Waging War on Disinformation Campaigns


Inside the Cyberwar to Hijack Elections and Distort the Truth
MANIPULATED
Theresa Payton

Former White House CIO **THERESA PAYTON**, a keynote speaker at Security Congress in 2018, this year published her book *Manipulated: Inside the Cyberwar to Hijack Elections and Distort the Truth* (Rowman & Littlefield, 2020). The following are excerpts of a conversation with Editor-in-Chief **Anne Saita** during the book's release.

My biggest concern is that nation-states are watching, and they are going to set up fake personas on Facebook and YouTube and promote fake ballots to download and mail in.

AS: Election security remains such a radioactive topic—despite evidence in your book and elsewhere that this type of behavior is not new nor exclusive to certain countries. And now we have a pandemic sure to impact an already precarious situation.

TP: A near and present danger that wasn't really discussed coming out of 2016 and 2018 is what if Americans in record numbers decide it's not safe to stand in line on election day and want to vote by mail. Can our current processes stand up to all of the voters in a COVID-19 risk group who now prefer that option?

My biggest concern is that nation-states are watching, and they are going to set up fake personas on Facebook and YouTube and promote fake ballots to download and mail in. Then we'll need to decide: Do these ballots get counted or not?

What was among the surprises you discovered while researching *Manipulated*?

I went into this book assuming most nation-states behind misinformation and disinformation campaigns don't like democracy and want to disrupt it. That is true. But what's fascinating to me is that the more they can get you and I to argue, they more likely they make a ton of money. The more we click on things and share things, the more pennies on the click they make. So, we're actually funding the campaigns that are being used against us.

In your opinion, which is currently more dangerous: misinformation or disinformation?

Disinformation is harder to discern and disprove, which makes it very dangerous. Misinformation tends to play toward a confirmation bias and is designed to mislead you. It plays on an emotion. The challenge with disinformation is there's a kernel of truth, and it tricks you when you read something and say, 'Wow, that seems strange. But I kinda remember hearing that.' So, you go to your favorite search engine and type in a few keywords and—lo and behold—you see something close to what you're reading, only it has disinformation in it.

So, what can we do to not fall into these traps?

First, if you read something in the news, on social media, or someone texts a story and you have an extreme emotional reaction to it—like, 'I knew it and now here's proof!'—you're probably falling prey to a manipulation campaign playing to your specific confirmation biases. Go to different trusted, vetted news sources—pick something local and something international and see if they are reporting that information the same way.

If something's sent to you with a small thumbnail picture and sensational title, chances are it's a clickbait campaign. If you realize this doesn't look legitimate, first tell the person who sent it that this probably isn't true. Then report that posting to the platform involved in its dissemination, to help them train their algorithms to block such content in the future. If you're not sure, go to a website like snopes.com and see if it's been researched by anyone else. ■

RETURN TO CONTENTS

(ISC)² Urges Congressional Support of the Cyber Workforce

The proposed Cyber Leap Act of 2020, introduced in the United States Senate, calls for the establishment of national grand challenges "to achieve high-priority breakthroughs in cybersecurity by 2028." Challenges include building more resilient systems, developing improved training and digital literacy, advancing technologies such as AI and quantum science, improving cyber safety and security, and reducing cybersecurity risks to U.S. federal networks and systems.

In a letter to U.S. Sen. Jacky Rosen (D-NV), one of the bill's sponsors, (ISC)² CEO David Shearer, CISSP, encouraged passage of the legislation. Shearer cited the shortage of skilled cybersecurity professionals as a crucial challenge that the legislation would hopefully help mitigate. "As the world's largest nonprofit association of certified cybersecurity professionals, we are acutely aware of the shortage of trained cybersecurity professionals and the skills gap that exists."

For the complete proposed bill, click here. ■

Magazine Wins Twice

InfoSecurity Professional magazine received two bronze Associated Media & Publishing EXCEL Awards in July. The EXCEL Awards recognize excellence and leadership in association media, publishing, marketing and communications. ■

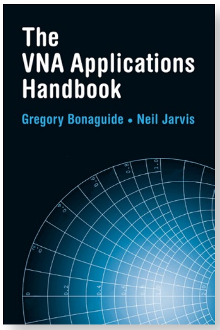
RECOMMENDED READING

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

The VNA Applications Handbook

BY GREGORY BONAGUIDE AND NEIL JARVIS

(Artech House, 2019)



THE VECTOR NETWORK ANALYZER or VNA is an important test instrument that has helped make modern wireless technologies possible. VNAs are used to test equipment and their specifications to ensure network components work together.

The authors, both engineers, have more than 30 years of experience in using VNAs. They review the various building blocks of VNAs such as measurement receivers, computers or processors, and reference receivers. They also review the calculations for frequency response transmission tracking and assess the pros and cons of bridge versus directional couplers. Additionally, Bonaguide and Jarvis look at key issues for VNA designers, such as identifying the ideal measurement system, the pros and cons of port match and size versus power handling and wide bandwidth, and the architectural boundaries and constructs of an ideal VNA.

The VNA Applications Handbook provides material that will assist a security professional in measuring the passive and active on-port devices such as radar systems for both cards and military applications, communication systems, oscillator, antenna matching or phase-matching of electrical cables—all while offering problem-solving techniques.

Bonaguide and Jarvis provide security professionals with the information they need to review documentation and process and procedures supporting the mobile wireless architectural networks. ■

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.

READ. QUIZ. EARN. READ. QUIZ. EARN.

Earn Two CPEs for Reading This Issue

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

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

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&ACTION=SI&CatRedirect=10850|10850

RETURN TO CONTENTS

MEMBER'S CORNER

(CIA)^{3D} Triad

A member makes the case that it's time to update the three pillars of information security

BY JAMES A. BATISTE, CISSP-ISSEP

AS (ISC)^2 MEMBERS, we're all familiar with the CIA Triad in which confidentiality, integrity and availability serve as guiding principles for well-structured, enterprise-wide information security programs designed to mitigate or reduce the risks of loss, disruption or corruption of information. Based on my own experiences both in the field and in the classroom, I'd argue the CIA Triad needs an update.

I teach graduate students information security concepts as they develop their information technology careers. This next generation of cybersecurity experts believes a new version of the CIA Triad should give equal consideration to areas like safety, accountability, non-repudiation, ethics, identity, preservation of life, analytics, privacy, transparency, proactivity, education, awareness and investigation.

When students first wondered aloud why the CIA Triad didn't incorporate more aspects of the cybersecurity world, I began my own analysis and discovered some shortcomings with the current version. Student responses to my queries relied heavily on the *technologies*, *controls* and *concepts* (encryption, hash, prime numbers, permutations, intrusion detection/prevention, non-repudiation, etc.) of which the CIA Triad has, over time, become the de facto symbol. In fact, the CIA Triad is at the highest abstraction level of the technologies, controls and concepts that have evolved in the battle to secure the "Information Society" (Siponen, 2001). The CIA Triad was never meant to represent all the *categories* of information, nor the *reasons* to protect them. It is a symbol of the current and ever-evolving tools we use to secure data and the systems that support the data.

What's Needed Now

The women and men entering IT today are faced with a multitude of *systemic* challenges as a result of data infrastructure (i.e., hardware, software, RFCs, etc.) that were not built with security as a primary goal. At the same time workplaces, schools, vendors and the internet provide them with a nearly infinite amount of information to combat a growing army of cybercriminals.

My proposal to combat the cybercriminals is twofold. First, update the CIA Triad to appeal to today's practitioners. Second, develop a corps of information security practitioners dedicated to incorporating best practices into this new version, which I call the (CIA)^{3D} Triad.

Figure 1: **3D CIA Triad Version 3.0**

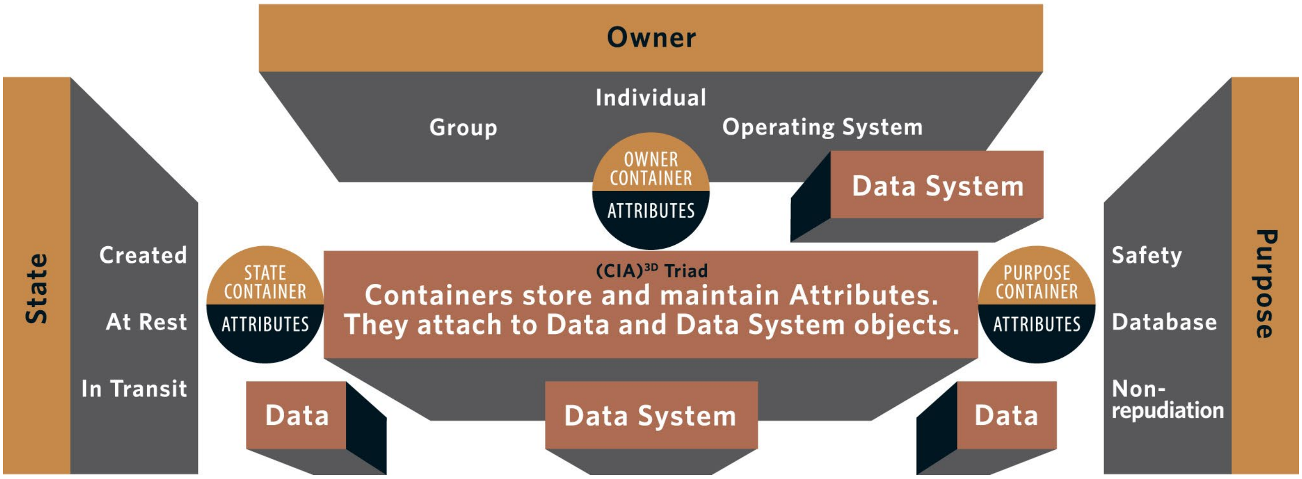


Figure 1 displays version 3.0 of the 3D CIA Triad structure. Information security practitioners utilizing the (CIA)^{3D} Triad to facilitate their discussions and collaborations are expected to develop and agree on the attributes that best suit their project. *(Request a current version.)*

RETURN TO CONTENTS

(CIA)^{3D} Triad Defined

I like to call these newfound custodians "Guardians of the Information Society" (GoTIS). They are dedicated information security practitioners representing every facet of the industry (i.e., business, hardware/software vendors, standards organizations, credential providers, etc.). They also want to fundamentally change how we, in general, protect data and data systems. One of their responsibilities is to develop and provide guidance on the best practices for the utilization of the "3-Dimensions CIA Triad," displayed as (CIA)^{3D} Triad *(see Figure 1, p. 12)*.

Three dimensions are applied to each component of the current Triad:

- Confidentiality-*State*, Confidentiality-*Owner*, Confidentiality-*Purpose*
- Integrity-*State*, Integrity-*Owner*, Integrity-*Purpose*
- Availability-*State*, Availability-*Owner*, Availability-*Purpose*

The core features of the (CIA)^{3D} Triad are:

- *State* – Refers to *Attributes* such as design, creation, at rest and in transit.
- *Owner* – Describes relevant individuals, groups, operating systems and IT departments.
- *Purpose* – Incorporates safety, database management, ethics and more.

The (CIA)^{3D} Triad distinguishes data from a data system. Data and data systems have lifecycles. At the very beginning of all lifecycles, *Attributes*—specific to each dimension—are assigned and attached to every data and data system object that comes into existence. Attributes can be changed but only deleted when the data or data system object to which they are attached is deleted.

Ground Rules and Usage

The (CIA)^{3D} Triad was developed to facilitate efficient collaboration. The following is a list of some of the considerations to ensure that happens.

FORESCOUT
Active Defense for the Enterprise of Things
The only solution that identifies, segments and enforces compliance of every connected thing
Don't just see it. Secure it.
LEARN MORE

RETURN TO CONTENTS

1. All parties agree that there is a need and room for improved *focused* communication.
2. All parties agree to a common glossary of terms.
3. All parties agree and understand that they must develop customized *Attributes* that support their project.
4. All parties agree and understand that the (CIA)^{3D} Triad is a framework to facilitate efficient collaboration and not a project checklist.

The (CIA)^{3D} Triad's facilitation role is a *success* if all parties more quickly (than not) develop and agree on the security-centric requirements needed by a project to be designed, built and operated.

A simple example of how GoTIS might leverage the (CIA)^{3D} Triad framework is in arriving at the security needs of a virtual private network (VPN). All parties come to agree:

1. The Purpose *Attribute* is a VPN.
2. Derived *Attributes* to VPN might include IPsec, L2TP and OpenVPN.
3. The determined State *Attribute* is a commercial, off-the-shelf solution.
4. The Owner *Attribute* will be the IT department.

Creating Greater Collaboration for a Common Goal

The (CIA)^{3D} Triad is vast and scalable. Its main purpose is to facilitate collaboration between stakeholders so everyone evaluates information security decisions in a similar fashion and can more quickly adopt best practices and products that stay ahead of the cybercriminals always lurking in the background. ■

JAMES A. BATISTE, *MS, CISSP-ISSEP, Security+, Linux+, CEH, owns NetWorthy Consulting and teaches at Denver University's University College and the Community College of Aurora.*

RETURN TO CONTENTS

Honors for (ISC)^2 Nigeria Chapter President

(ISC)^2 CONGRATULATES CHINATU UZUEGBU, CISSP, president of (ISC)^2 Nigeria Chapter, on being named one of the Top 50 Women in Cybersecurity Africa. She was nominated by members of the chapter. Cyber in Africa, the governing body, assembled a panel of seven judges, all business and technology leaders throughout Africa, that pored through more than 300 nominees to select their Top 50.

Uzuegbu has been an (ISC)^2 member since 2015. She led the chapter through the chartering process and has served as the Nigeria Chapter president since 2018.

"It is quite interesting and exciting to see more women coming into the cybersecurity workforce."

"It is now obvious that the internet is ruling the world and the bad guys are seriously taking advantage of vulnerabilities," Uzuegbu says. "The whole world relies on us to secure and protect their cyber space. It is important for us to consistently maintain our duty posts, advance and develop ourselves on it, and seamlessly buy the trust and confidence of the organizations we represent when it has to do with assuring a level of confidentiality, integrity and availability of their information assets."

She adds, "It is quite interesting and exciting to see more women coming into the cybersecurity workforce. We are seeing a 20% increase today, but I envisage a consistent 50% increase in no time as we keep encouraging and mentoring women into the field."

Just Because You Can, Doesn't Mean You Should

by Brandon Dunlap

THINK OF "DARK DATA" as that box you moved to your new house, but never unpacked. It's been sitting in the garage now for years, collecting dust. Do you even remember what's in it?

You haven't needed it, obviously, but you have paid to store it under lock and key. Maybe it's something sentimental, or even collectible. Maybe grandma's finest silverware. Whatever it is, it's like Schrödinger's cat—you don't know if it's worth keeping until you check inside the box.

This is dark data. It's the data that you have moved from server to server for years. You've been migrating it, backing it up, and putting controls around it, but otherwise, it hasn't been touched in years. Like grandma's silverware, you need to either use it or sell it. But first, you need to determine its value. This is where the study of infonomics, a delightful portmanteau that is the study of the economics of information, comes into play.

In researching this area, I soon learned that there isn't a generally accepted method of accounting for which side of a balance sheet a data store falls: asset or liability. But we can see if it's in use, and that's the first step.

Find it. Attribute cost, value, or both. Control it appropriately or discard it. It sounds simple. But I fell into quite a rabbit hole when I tried to solve for the first step.

Brandon Dunlap is a leadership partner for security and risk management for Gartner. He can be reached at bsdunlap@brightfly.com.

I was fortunate that on May 12, I had the privilege of hosting Steve Piper (https://www.linkedin.com/in/stevenrpiper), founder and CEO of the CyberEdge Group, on a Security Briefings webinar. CyberEdge had recently released the findings of its 2020 Cyberthreat Defense Report, a study covering 1,200 respondents across 17 countries, sponsored in part by (ISC)^2. There was a lively bit of conversation, and you can listen to the archive here (Key Insights from CyberEdge's 2020 Cyberthreat Defense Report).

Photograph: Getty Images

While I didn't catch it the first time around, in reviewing the transcript of this event, I was struck by this quote from Steve: "Of the hottest movements this year, and every year we add questions based on hot topics of the day, this is one of them. We asked about which components you're incorporating into your zero-trust architecture. Email and file encryption are at the top of the list, followed by data discovery and classification tools."

Data discovery and classification tools was No. 2, only less important than encryption! That means we are more likely to buy encryption tools, at the risk of possibly over-deploying (at great cost) to cover assets we haven't even identified yet, let alone classified. Forget about the actual accounting of the value of the data, just look at the cost to protect it.

Just think of the unforeseen liabilities that could occur either through a breach or even just regulatory exposure. And you haven't even found it yet. Dark data is either a resource to be discovered, protected and offered to the business to mine for value, or it is a liability that is going unused and untouched that must be expunged. It's either grandma's silverware, or worthless junk. You just need to find it first and start discussing its value before it gets used and you scramble to identify and apply controls to protect its newfound value. This could be the platform from which an information security professional begins to speak an emerging language of the business. ■

RETURN TO CONTENTS

What Are Your Industry Peers Saying About CLOUD SECURITY?

Organizations report that qualified staff is the **biggest** obstacle to faster adoption. And for the fourth year in a row, training and certifying IT staff ranks as the **top priority** to assure organizations evolving security needs are met.

Cloud security concerns remain high as the adoption of public cloud computing and the accelerated shift to remote work environments continue to surge.

To stay ahead of emerging trends, arm yourself with the 2020 Cloud Security Report. Sponsored by (ISC)², this comprehensive survey explores how organizations are responding to evolving threats and the ongoing shortage of qualified security staff.

Get the Report

THE CAREER-CHANGING MAGIC OF TIDYING UP

Turning to organizational experts to rid IT systems of unwanted and potentially dangerous clutter.

BY ANITA J. BATEMAN, CISSP

WE ARE ALL PLAGUED BY TECHNICAL DEBT in the form of legacy systems that can no longer be patched but must be kept up and running. Critical business processes, legacy data retention, lack of system knowledge or "pet" projects might keep us from retiring these difficult-to-maintain systems. From the very first operating system updates on the original IBM 360 to the latest Windows 10 updates today, we still struggle with this common challenge to fully patch and maintain our technical systems.

Might there be a different way to approach this perennial issue? Might we invoke some of the philosophies, principals and methodologies of organizational experts when it comes to ridding IT systems of so-called junk?

PATCHING ALONE WILL NOT SOLVE THIS

How did we end up with so many unpatchable systems in the first place? Mergers and acquisitions have brought us systems that may not conform to our standards of maintenance and lifecycle management. "Shadow IT" and our own lack of discipline may be additional sources. Ongoing challenges to "do less with more" may have forced us to make prioritization decisions to defer regular maintenance activities on lower-priority systems.

We know that we can improve the situation with well-defined processes, dedicated teams, smarter tools, more budget and better discipline—all the usual best practices. But it is rarely this simple.

Some industries, like manufacturing and healthcare, have a harder time with regular patching schedules because downtime is nearly impossible to schedule.

Dr. Marianne Winslett, computer scientist, is familiar with this. "There's a reason they [factory floor] never patch and never upgrade. It's because any time you do that, you're at significant risk of downtime. … A factory that's running 24/7 really can't afford the downtime that comes with computer system failure. So, there's an 'if it ain't broke, don't fix it' attitude."

NIST has a project underway for "patching the enterprise" in its Critical Cybersecurity Hygiene area.

The final project description, published in March 2020, says the "objective of this project is to demonstrate a proposed approach for improving patching practices for general IT systems." As this study is only addressing general IT systems, it will not help in tackling business applications or other specific topics, like Internet of Things (IoT) devices, but it may provide a useful reference guide.

Other traditional approaches to solve this problem have focused on rationalizing your business application portfolio and modernizing legacy systems. In a 2018 Gartner article titled "7 Options to Modernize Legacy Systems," Susan Moore explains how to choose between options to encapsulate, rehost, replatform, refactor, rearchitect, rebuild or replace. However, we may not know enough about a legacy system to take on a modernization project. "Not only are the people who built these systems gone, the users who asked for them to be built in the first place are also gone," writes William M. Ulrich in *Legacy Systems: Transformation Strategies*. (See sidebar on p. 21 for additional patching and legacy modernization resources.)

NEW APPROACHES

What if we approached this problem as a true cyber hygiene problem, similar to how we approach cleaning our homes, our garages and our communities? Our homes and garages accumulate "junk" just as our data centers accumulate technical debt. Similarly, a system upgrade or transformation project could be viewed as a community project with many interested individuals—including business owners, financial stakeholders, end users, IT professionals and executive leaders. What insights can be gained by approaching our unpatchable systems in this manner?

Three resources provide such an opportunity: the KonMari Method^{TM}; garage organization tips from Family Handyman; and tips for a successful community cleanup.

MARIE KONDO TO THE RESCUE

Let's consider the popular KonMari Method invented by Marie Kondo, which "encourages tidying by category—not by location—beginning with clothes, then moving on to books, papers, miscellaneous items, and finally sentimental items."

There are six basic rules:

- Rule 1: Commit yourself to tidying up
- Rule 2: Imagine your ideal lifestyle
- Rule 3: Finish discarding first
- Rule 4: Tidy by category, not by location
- Rule 5: Follow the correct order
- Rule 6: Ask yourself if it sparks joy

Rule 1: Commit yourself to tidying up

Who do we need commitments from to achieve the goal of "tidying up" our technical environments? We need to identify the commitments needed from our system technical owners, business owners, budget owners and leadership.

Rule 2: Imagine your ideal lifestyle

What do we want our technical environment to look like? Is a commitment to remove 100% of unpatchable OSes from our environment realistic? Probably not.

Maybe a commitment to remove a specific operating system or replace/retire a smaller percentage (30%?) of the technical debt in the next 12 to 24 months is more achievable. It will be easier to commit to smaller chunks and make incremental progress toward a greater goal than to fight the uphill battle to get commitment on an "all or nothing" approach.

Rule 3: Finish discarding first

What does "discard first" look like in a technical environment? We rarely throw anything away.

The biggest obstacles to discarding old systems are data retention and particularly data archival. Even if a system is no longer used for daily processes, the data may still be required for legal, regulatory or even "my pet project" reasons. We need effective data archival strategies and solu-

RETURN TO CONTENTS

tions that allow us to decommission the legacy system.

How do we stop the problem of legacy data from getting worse? We need to start thinking about data archival as part of a full lifecycle plan for a new application, and for applications inherited through acquisition.

Data Archival and System Retirement Plan should be required chapters in a support plan for a new or inherited system. I know of a small college president refusing to break ground for any new campus building unless both the construction cost and the endowment fund to care for the building were fully funded. This delayed the groundbreaking for some buildings, but this approach guaranteed that the college did not take on unmanageable debt during an eager building phase.

While we build business cases and support models to support new applications, we rarely define the useful lifecycle for an application or include the costs for data archival and system retirement with the business case.

Rule 4: Tidy by category, not by location

In IT, tidying by category might mean looking at all instances of the same operating system and tackling them in one project (e.g., all Windows 2003 OS systems). Alternatively, we could look at all business applications performing the same process/capability. This is similar to an application rationalization approach to portfolio management and provides a disciplined approach to organizing the tidying efforts.

Rule 5: Follow the correct order
and
Rule 6: Ask if it sparks joy

The KonMari Method focuses a great deal on completing your tidying/cleanup once and then maintaining it consistently going forward. This is critical so that you are not introducing "junk" into your home that does not "spark joy." Most of us have so much technical debt that it may be hard for us to envision completing the tidying process in a timely manner. We should think of unpatchable systems as a marathon and not a sprint. Mark Twain reportedly once said, "Continuous improvement is better than delayed perfection." We should take the same mindset.

ARE DATA CENTERS SIMILAR TO OUR GARAGES OR STORAGE AREAS?

If we relate organizing our garages or personal storage areas to this problem of unpatchable systems, there are some takeaways from this Family Handyman article.

Start by setting a goal to clean and separate everything into categories of must keep, want/should donate, sell or throw away. In IT, that includes an up-to-date inventory of our systems that captures the plan for each asset (e.g., keep, consolidate/merge or retire).

> Data Archival and System Retirement Plan should be required chapters in a support plan for a new or inherited system.

There is no perfect approach to doing this, but we all need an approach that works for our organization, can be sustained, and can be leveraged as a data point for strategy planning and budgetary processes.

While the article advises to "give yourself no more than one weekend and take items to the donation center before close of business that day," our inventory activities may take longer than one weekend.

The recommendations to time-box this activity, confirm our decision process and timeline, and create a way to easily see what we have (e.g., CMDB or application inventory dashboard) can be helpful to get us started.

Once we know what we have, then we can move to planning, gaining support and executing our plans. Several of the projects suggested in the article have to do with effective storage solutions. Have we considered alternative storage solutions for our legacy data? Does it have to be available real-time (e.g., sports equipment, car care products) or could it be moved off-site or archived to be available when needed less frequently (e.g., garage ceiling track storage). Can we update our storage technologies and store more in a smaller (or cheaper) way? We should review this every few years.

All of the projects in this garage organization article share a key concept with the KonMari Method—they all aim to put similar items together for best organization and visibility—or Rule 4 from Marie Kondo: tidy by category, not by location.

WE CAN'T DO THIS ALONE

Finally, what if we approach this like a community project? The University of Nebraska-Lincoln has an article with "Tips for Organizing a Successful Neighborhood Cleanup."

Two areas that stand out for our problem statement are stakeholder engagement and information research.

"Forming a neighborhood cleanup committee is a great way to get things done efficiently and build ownership at the same time," the article states. Are we leaving our infrastructure teams to tackle this problem alone or have we formed the right community of application owners, IT support, business leaders and management support? Who has pride in the current solution or would take pride in this project and should be engaged to support the effort? Who

RETURN TO CONTENTS

will be a dissenter or may try to sabotage our efforts? You may need to create a stakeholder communication plan and build support for your project. Who will organize the project tasks into a detailed plan? Have you accounted for someone to coordinate the activities or are you trying to handle it within your current workload and current staff?

"Research your 'cleanup area' to get an idea of the support you will need," the article offers. Do you have enough information about the legacy system to understand how to move forward with your objective (replace, upgrade, protect further or decommission)? Is key documentation missing or have the subject matter experts left the company? Is there an "archaeology" project you need to undertake to confirm what is required? Have there been other similar projects you can look at to understand how this effort might be advanced at your company? Are your application, cybersecurity and infrastructure teams collaborating well enough to undertake this project or does that need attention?

'IF WE CHASE PERFECTION, WE CAN CATCH EXCELLENCE'

The famous football coach Vince Lombardi wisely said, "Perfection is not attainable. But if we chase perfection, we can catch excellence."

Let's drive toward continuous improvement and reduce our threat landscapes. Let's clean out our work "houses" and "garages." It's time we tackle this problem with fresh eyes and find what "sparks joy." Along the way, we just might improve our cybersecurity risk and vulnerability posture at the same time. ■

ANITA BATEMAN, *CISSP, is an IT executive with experience in the technology, utilities, oil and gas, and automotive industries and is a past contributor to* InfoSecurity Professional.

CLEANING OUT LEGACY SYSTEMS

The following links and references may help guide your own efforts to clean out legacy systems no longer of use to an organization.

PATCHING AND SECURING LEGACY SYSTEMS

https://www.paloaltonetworks.com/resources/whitepapers/securing-the-unpatchable-in-fsi

https://www.ncsc.gov.uk/guidance/obsolete-platforms-security-guidance

https://sector.ca/wp-content/uploads/presentations14/Securing%20OS%20Legacy%20Systems%20widescreen.pdf

https://www.securityweek.com/hundreds-millions-pcs-remain-vulnerable-windows-7-reaches-end-life

https://www.rockwellautomation.com/content/rockwell-automation/www/na/us/en_US/company/news/blogs/unpacking-the-patch-management-process-for-operations.html

https://www.csoonline.com/article/3535073/basic-enterprise-security-hygiene-is-still-essential.html

https://csa.com.au/2018/02/19/the-definitive-guide-to-patch-and-release-management/

https://queue.acm.org/detail.cfm?id=1053344: March 2005, Patching the Enterprise, by George Brandman

https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/ch-pe-project-description-final.pdf

https://www.nccoe.nist.gov/projects/building-blocks/patching-enterprise

LEGACY SYSTEMS MODERNIZATION

https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-legacy-systems-and-modernization.pdf

https://www.scalefocus.com/insights/business/top-13-reasons-to-modernize-your-legacy-systems

https://www.cio.com/article/3267464/how-to-deal-with-legacy-systems-the-achilles-heel-of-digital-transformation.html

"Legacy Systems: Transformation Strategies," by William M. Ulrich, Prentice Hall, 2002

https://deloitte.wsj.com/cio/2013/10/01/when-companies-become-prisoners-of-legacy-systems/

"Working with Legacy Systems: A practical guide to looking after and maintaining the systems we inherit," by Robert Annett, 2019

"Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices," by Robert C. Seacord, Daniel Plakosh, Grace A. Lewis, 2003

—A. Bateman

DATA MANAGEMENT

PROTECTING THE UNSEEN

Just as dark matter makes up most of the universe, dark data is also in the majority. Protecting it depends on illumination, understanding and enlightened policy.

BY MATT GILLESPIE

PRIMORDIAL FEAR OF THE DARK is the fear of the unknown. And just as the dark may hide dangers, it's also hard to protect what you can't see. That reality underlies the challenge of protecting dark data.

"Dark data" refers to the lack of visibility into data that is accumulated and stored but never analyzed or used. This data, which also tends not to be properly accounted for, can create significant exposure. It can be massive in scope and be generated by systems, devices and interactions.

A survey by Splunk reports that while 81% of business and IT decision makers rate data as "very" or "extremely" valuable to their organization's success, they also estimate that 55% of their data is unknown or untapped. The volume of dark data was reported to be the No. 1 obstacle to coping with it, and the significance of these factors continues to grow as data stores expand with the ascendancy of AI and the Internet of Things.

IMAGE BY JOHN KUCZALA

System logs are a common example of information that organizations hold on to without a specific plan for it. Other sources are as diverse as email, media files, documents and customer call records. Likewise, processes such as static code analysis and penetration testing generate gobs of data that need to be addressed responsibly.

Much of that data is innocuous, but it can also sow chaos. For example, it could be used to compromise sensitive resources or intellectual property, and it could also form the basis of a slick phishing campaign.

There is a growing awareness that while "data is the new oil" and immensely valuable, today's massive uncontrolled data stores can also have negative consequences.

The remedy to this set of threats is to investigate and then protect all data that is unused, uncategorized and unknown. Not only is there a big attack surface to consider, but it's impossible to apply appropriate levels of security to information without first knowing what those levels should be.

DISCOVER AND ILLUMINATE DARK DATA TO UNDERSTAND AND PROTECT IT

The reality behind bloated unused data stores is that the default course for users or processes is often to ignore and forget information once it is no longer useful. That uncontrolled data equates to uncontrolled liability.

Before you can protect data, you need to discover and categorize it. Michael Peters, CEO at Lazarus Alliance, explains: "We do a data classification and custodial exercise; it's a process-driven, full-enterprise analysis of, 'OK, these are the types of data that we have in this organization. These are the systems that produce this information.'"

That type of audit-based approach is often accomplished using governance, risk and compliance (GRC) software, which also reveals the regulatory connection with these processes. Regulatory frameworks may specify requirements in areas such as retention periods, encryption and data sovereignty, among others, which can have direct bearing on how dark data needs to be stored and secured.

For example, Payment Card Industry (PCI) standards include a one-year retention requirement for certain sensitive data, while Sarbanes-Oxley calls for three years. The obverse of such requirements is that information should be tagged for secure deletion at the appropriate time, to avoid the continued liability of protecting it.

Discovery must proactively establish appropriate levels of confidentiality, integrity and availability (CIA Triad) for each piece of data. What are the risks if a certain body of information is exfiltrated? How important is it to be sure the organization can access it for a given period of time? And how critical is it to trust and prove that the data remains intact in its true form?

Together, these factors fuel technical analysis of data, networks and systems. This boots-on-the-ground, meticulous fieldwork begins with scanning and searching for particular types of data, such as protected health information, credit card details and trade secrets. More broadly, it is the effort to identify and classify all the information in the organization, beyond simply finding data that fits into specific classifications or types.

DARK CLOUDS DON'T INDICATE SAFETY

SOME ORGANIZATIONS may be tempted to regard cheap public cloud storage as a digital junk drawer where data can be stashed and forgotten under the watchful eye of the cloud provider. In reality, this relationship places more responsibility on the data owner, rather than less.

"Fundamentally, a company's data is a company's data, and they have a responsibility to be good stewards of it," Lazarus Alliance's Michael Peters cautions. "Just because they put it into a cloud environment doesn't remove their responsibilities or liabilities."

Contract agreements with providers are key to ensuring that protection. Organizations need assurances in terms of how the data is protected and how they will be notified in the event of a breach, for example.

—M. Gillespie

RETURN TO CONTENTS

THE SPECIAL STATUS OF EMAIL

BY ITS NATURE, email is propagated with little or no control both within and outside organizations. It also tends to persist much longer than it is needed. Some users may be cavalier about what information they include and where they send it, and they also give up control over the information after they share it.

Michael Peters of the Lazarus Alliance sums up the danger: "The best place to breach an organization ... is really through the email system. And it is such a treasure trove of information."

Indeed, one must assume that any and all information could potentially be exposed through email messages, either inadvertently or on purpose. Hunting for such threats is an ongoing area of concern and action by security teams, including technical measures and user education.

—M. Gillespie

RESEARCH THE ORGANIZATIONS AND WORKFLOWS THAT CREATE DARK DATA

Developing a rubric or taxonomy for categorizing data cannot ultimately be separated from an understanding of the people and processes that create it. The creation of data is ongoing and dynamic, which requires a collaborative mindset that embraces dialogue, rather than just prescriptive action.

Security teams and auditors must build rapport with the business and technical stakeholders involved and build insights around the data they produce from their points of view.

Peters advises teams as they wade into the organizational aspects of dark data management. "You have to learn something about the customer environment. You have to understand what it is they do, what sort of systems they have, things that they know. … You also have to know how to answer or to ask the right questions."

There is an undeniable human dimension to the process of uncovering this information, and it requires the combination of expertise and diplomacy.

"If I were to have a conversation with a customer and they think it's an interrogation, they're not going to talk to me very freely," Peters suggests. "But if they think, 'Hey, this is a collaborative experience here and I don't feel threatened,' they're going to start talking, sharing and providing better responses."

That process involves taking time to explore the functions and requirements of specific parts of the business. Peters says, "It also helps to have a good bedside manner." While investigators are expert on data considerations in the general sense, they must never forget that the business and technical people they interact with are the subject matter experts in their own realm.

Security professionals need to learn how organizations and workflows are dependent on—as well as challenged by—the specific bodies of data they produce and consume. That fuels a deeper functional understanding of the organization's data as a whole, both before and after it becomes dark.

IMPLEMENT STANDARDS AND PROCESSES FOR ONGOING GUARDIANSHIP

To guide and protect the business, the insights gathered during discovery and analysis need to be operationalized. Classifying existing and future data based on the CIA Triad is the first step of this process.

At the same time, recognize that many organizations have classification frameworks that are applied unevenly or not at all. Getting security value from classification schemes requires implementation of standards and measures to protect dark data on that basis.

A risk-versus-reward mindset may reveal that many types of data should simply be eliminated, while others should be governed and secured appropriately, perhaps only for a set period of time. Putting these standards and processes in place should build on the following dimensions:

- **Policy and governance.** Controls must be established and put into place for various subsets of data, based on factors such as its sensitivity, how long it should be retained, and what people and systems need access to it.
- **Technology stack.** Hardware and software protections will be tailored to the nature of the data, including not only the measures themselves, but whether the data is suitable for hosting in public cloud or other third-party locations.
- **Education and vigilance.** Like all parts of cybersecurity, controlling dark data carries a heavy responsibility to train users and organizations about the potential risks exposed by dark data and the measures to mitigate them.

When addressing dark data stockpiles, security and audit practitioners are well advised to remember that, in Peters' words, "Information can be your friend, but it can also be your enemy."

To discern and manage the difference, we must illuminate what lies in the shadows, take stock of what we find and take measures to protect it over the long term. ■

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

RETURN TO CONTENTS

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

A 'FOGG'Y NOTION AND A NUDGE

BY PERRY CARPENTER

EPISODE 3 (THIRD IN A SERIES):

OH, BEHAVE!

… IT ALL COMES DOWN TO MESSAGE AND PRODUCT. MAKE YOUR MESSAGE MEMORABLE … AND REMEMBER YOU'VE GOT A PRODUCT TO SELL.

ILLUSTRATION BY TAYLOR CALLERY

PREVIOUSLY IN THIS SERIES:

Three days ago, Acme Corporation had a really bad day. It suffered a data breach. During the initial investigation, Mike (an IT security manager) and his team discovered that the cause tracked back to a phishing email that slipped through their mail filters … and that their CEO, Jerry, just happened to click on it. Now, Acme's CISO, Jim, along with Mike and his team members, Katie and Krish, are on a quest to determine how that happened and what lessons they can learn from the event.

Did they already have a security awareness program in place? Of course they did. But after careful research and by looking at their program with an open mind, the team is beginning to understand the root of the problem:

- Just because people are *aware* doesn't mean they *care*.
- If you try to work *against* human nature, you will fail.
- What your people *do* is way more important than what they *know*.

Our last episode ended with Katie, an IT security analyst on Mike's team, hinting that at least part of the secret to upping effectiveness might come from meeting with their marketing department.

FRIDAY 10:00 A.M.
ACME CORPORATE HEADQUARTERS

The first thing Katie and Krish noticed as they stepped into the marketing department's area was the combined sense of play, creativity and passion. Looking to their left, they saw two employees tossing a ball back and forth over their pod walls while taking turns suggesting what seemed to be taglines for a new campaign. Artwork featuring many of Acme's most successful advertising campaigns adorned the walls. And they even noticed a few internal human resources-related campaign messages and materials enshrined in a nearby display cabinet.

This seemed to be an area that thrived on developing fun ideas and finding the best way to effectively communicate them.

"I think this is it," Katie said, gesturing to an open conference room door.

Not wanting to make the mistake of disturbing an in-progress meeting, Katie and Krish approached the

RETURN TO CONTENTS

door tentatively, slowly and cautiously peering inside … and just about jumped out of their skin when they heard a deep, booming voice behind them.

"You must be Katie and Krish! The voice came from Luke Jenkins, Acme's SVP of marketing. "Sorry. I wasn't sneaking up on you, I promise."

Luke was a big guy with a big personality. His voice seemed to consistently convey genuine enthusiasm.

"You both jumped like Scooby-Doo characters," Luke said as he stifled a laugh and ushered them into the conference room. "I was intrigued by your email."

Getting down to business, Katie and Krish brought Luke up to speed on the breach, their past security awareness program, and their recent research into learning science, communication and behavior science.

Luke listened, taking it all in, and began to speak.

"OK. So, there are a few considerations here that I know we can help with."

Krish and Katie leaned in to listen—as if Luke were a guru—and they were ready to receive some type of magical metaphysical marketing wisdom from on high.

"Scooby-Doo again."

"What?" they said in unison.

"You're acting like Scooby-Doo characters again."

"Oooooooh. Sorry," they again said in unison.

"Cute act," Luke said, shaking his head and continuing. "The way I see it, you have two things that you need to consider. The first is related to how best you can communicate the core message of the *information* you need to get out. And the second is related to the *actions* that you need people to take."

"Jeepers! How do we do that?" Katie asked in her best Daphne impersonation.

"Well, it all comes down to *message* and *product*. Your message needs to be memorable—kind of like how you just remembered 'jeepers' because I mentioned Scooby-Doo. I mean, how many of our employees can recall your last security message as easily as you recalled that obscure childhood reference? And second, you've got a product to sell. In this case your product is a behavior. You need to get your people to pick up that product—behavior—and take it to the cash register."

"OK," Krish said. "How do we do that?"

Luke leaned in, lowering his voice and beckoning Krish and Katie into a semi-huddle.

"I've got a plan…."

WELCOME to the third installment in our series about building transformational security awareness programs. Luke was able to help Katie and Krish come up with a number of strategies related to communication and behavior that will help inform a much more proactive, human-aware end-user security training program.

Luke first diagnosed the issue. He let them know that approaching security awareness training as a once-per-year compliance exercise will almost always feel extremely irrelevant to employees.

So, what was Luke's plan to address this?

He began by addressing the communication issue. Krish and Katie went into the meeting knowing that one of their problems was the disconnect between the information they were sending to employees and how well that information was received and retained. Luke encouraged them to tackle that issue head-on by finding the *why* behind the information.

Luke's advice was to always connect any piece of information with the underlying reason for why that information was important and relevant to the employee. And if they couldn't address why it was important or relevant, then reevaluate if that information should be shared at all.

Then, after deciding which information was most critical to share based on the *why*, Luke encouraged them to connect the *why* to some type of emotion or story-driven hook that would nest the information more within a human context.

And, finally, he advocated for a strong sense of imagery in branding. "After all," Luke explained, "brands have value. A brand logo and the consistency of style that they use in their communications have the effect of unlocking all of the rich history, values and experiences that customers associate with that company. Security should be the same."

Luke, Katie and Krish also did some brainstorming about the behavior science side of things. Katie explained that she'd been doing research into the Fogg Behavior Model (http://behaviormodel.org), Nudge Theory and, more generally, behavioral economics.

She concluded that most of the time people act on autopilot. This is because our minds naturally take shortcuts to conserve energy and increase our decision-making speed. After all, historically it was inaction in the face of predators that would lead to death, and inaction in the midst of a hunt might lead to a missed meal. And so, our minds are wired to make decisions extremely quickly because traditionally the payoff for the quick decision provided the greatest ROI.

If we are going to design security programs that work *with* human nature rather than *against* it, then we need to come to terms with the fact that information alone is impotent. Information with emotion is better. But the ultimate goal of an awareness training program isn't information retention—it is action. That means that we need to clearly understand the desired behavior that we want our employees to do and explicitly design for it.

The Fogg Behavior Model states that a behavior (B)

RETURN TO CONTENTS

happens when three things come together at the same time: *motivation (M)*, *ability (A)* and a *prompt (P)* to do the behavior. This can be expressed as B=MAP.

When a behavior does not occur, at least one of those three elements is missing. The model delves into whether a task is easy or hard, and whether or not it takes much or little motivation. The model looks at how to increase motivation or decrease how hard the task is to do. This drives home the point of putting a message (the prompt) out at the right time and through the right communication channel—or, preferably, through multiple communication channels to maximize the chance that employees will see the prompt.

This is also where the Fogg Behavior Model intersects with Nudge Theory.

"A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives," according to renowned economist Richard Thaler and co-author Cass Sunstein in *Nudge: Improving Decisions About Health, Wealth, and Happiness*. "To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting fruit at eye level counts as a nudge. Banning junk food does not."

WHEN YOU THINK ABOUT IT, A NUDGE AT THE RIGHT TIME IS A PROMPT THAT CAN BOTH INCREASE MOTIVATION AND/OR MAKE SOMETHING EASIER AT THE SAME TIME.

It's important to note that the Fogg Behavior Model and Nudge Theory are two distinct models and can operate independently. However, you can use one model to help flesh out how you apply the other. At its core, nudging is all about making the thing that you want someone to do the easiest or most obvious choice. That's why grocery stores have big displays of their promotional items next to the checkout aisle.

When you think about it, a nudge at the right time is a prompt that can both increase motivation and/or make something easier at the same time. In that way, a well-designed nudge can become a *power prompt*.

For instance, if your target behavior is to properly dispose of paper documents, then you might create a nudge by placing the shredding bins right next to the trash bins.

And then you further your behavior design by putting a sign about secure shredding near each printer and above the trash and shred bins.

By doing this, you are placing the prompt at the point of behavior. And you are nudging them as they decide how to dispose of the document. You can further the nudge and the motivation by adding a picture of peers disposing of paper the right way (to create social pressure), and so on.

At no time are you forcing the issue. You are merely reinforcing the behavior that you want by prompting at the right time, doing what you can to increase motivation, and

YOUR HOMEWORK

1. Consider contacting your own organization's marketing department. Ask them about campaigns they've run that have been effective and discuss what qualities made them effective.
2. Spend a few minutes conducting basic web searches around the concept of Nudge Theory. Specifically look for pictures of some of the examples. Write down at least five ideas about how you might consider nudging your employees in the right direction (or away from undesirable behaviors).
3. List the top behaviors that, if adopted, would have the most security benefit for your organization. Be specific. Is what you are listing a single behavior or an umbrella term for a group of behaviors? If it is a group, then list out each individual behavior.
4. For each behavior, be gut-level honest about if your organization will have the appetite to focus on changing that behavior.
5. Model the behaviors you want using the Fogg Behavior Model or simply by listing the promoting and inhibiting pressures.
6. Draft a proposed security awareness campaign that incorporates Acme SVP of marketing Luke's advice.

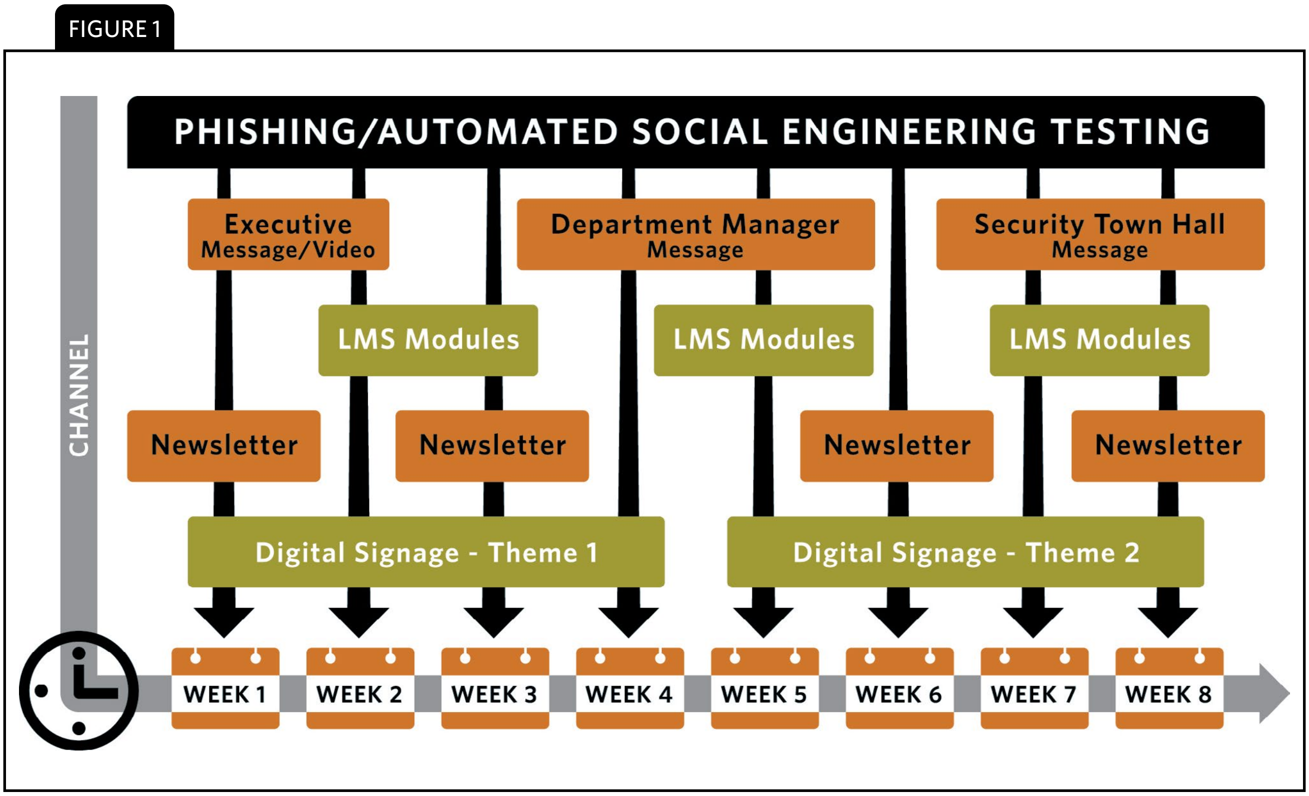
COMING UP: "IT TAKES A VILLAGE"

Our team realizes that the social aspect of behavior can't be ignored and works to find methods to move entire cultures and cliques within the organization. ■

—*P. Carpenter*

RETURN TO CONTENTS

FIGURE 1



making the desired behavior as easy—or easier—than the undesirable behavior.

Luke also helped with another big problem related to attention. He explained that a product's marketing strategy would not be successful if there were only one event per year. That's why we see advertisers hit us again and again with messages, images and stories about their product and how it fits into our lives.

"Think about your favorite fast food restaurant. You hear radio ads, see advertisements in videos and on TV," Luke said. "You see billboards on the side of the road, and you may even get hit with promotional notifications and coupons on your smartphone. These companies know that you need to constantly be reminded that they exist so that—at the right time—you'll act. If you really want to be effective, you'll find ways to do the same types of things in your security awareness program."

Luke then approached a nearby whiteboard and began drawing a chart to help communicate his thoughts. The vertical axis of the chart accounted for multiple channels of communication like executive videos, learning management system modules, newsletters, posters and more. The horizontal axis represented time. Luke was showing how a single campaign theme would launch these different communication strategies at different times to keep the message top-of-mind and increase the chance of catching their audiences' attention and increasing overall retention.

Lastly, after chatting a bit more, Krish and Katie added vertical arrows going down the chart at regularly spaced intervals. These arrows represented frequent simulated phishing training so that they could help employees build motor memory and strength through constant training *(see Figure 1, above)*.

Now that they knew what needed to be done, their next challenge was to make sure the training worked as intended. In the next episode, we'll take a look at the often-overlooked secret of how to make your program go viral and how to make it sustainable. We'll get into organizational dynamics and the fundamentals of how to measure and move the security culture of your organization. ■

PERRY CARPENTER *is the chief evangelist and strategy officer at KnowBe4, Inc. and author of* Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors *(Wiley Publishing, 2019), upon which this series is based.*

HAVE A QUESTION FOR PERRY?

You can reach him on LinkedIn at /in/PerryCarpenter, Twitter: @perrycarpenter, or email: perryc@knowbe4.com. He's also inviting our readers to join his *Transformational Security Awareness* group on LinkedIn (https://www.linkedin.com/groups/12207804/) or by simply typing "Transformational Security Awareness" into the LinkedIn search.

Teaching Cyber Safety Post-COVID-19

by Pat Craven

I AM SURE, just like me, you are still trying to get your bearings and figure out what in the heck has been going on these past few months. COVID-19 has forced all of us to reexamine how we live, work and play. The changes may be short- or long-term. Right now, we just don't know if or when life will go back to "normal."

One thing we do know is that this global crisis has created a much-needed increase in the desire for more information on how to stay safe online. Your Center for Cyber Safety and Education has seen unprecedented spikes in requests for tips and information from individuals, businesses and the media. We've seen a 132% increase in web traffic and more than a 300% increase in media coverage compared to last year.

The closing of schools and businesses around the world took away our key method for delivering both our Garfield and Safe and Secure Online trainings. But with the demand on the rise, we couldn't let that stop our efforts to make it a safer cyber world for everyone.

In addition to the increase in frequency and timeliness of our blog posts, website updates and social media postings, in June we launched a new digital eLearning program for children called Garfield at Home (see the July/August issue of *InfoSecurity Professional* magazine for details). Now, younger children can learn the basics of internet safety from home with the help of Garfield and Friends.

Like the Garfield's Cyber Safety Adventures Educator Kit, the Safe and Secure Online series for children, parents and senior citizens was also designed as a group presentation. Volunteers and professionals like yourself would typically deliver the PowerPoint presentation at a local school, library, community center or other similar venue. Well, the pandemic hasn't changed that; it's just impacted where those assemblies are taking place. Now, more of these educational trainings are being conducted online using platforms like Zoom, Webex, Microsoft Teams, Facebook Live and others.

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

Individual (ISC)² members, volunteers and chapters around the world have moved their community outreach efforts online, with great success. I have received notes recently from the chapters and volunteers around the world, expressing their enthusiasm with both the materials and their ability to continue their community outreach during the pandemic.

Photograph: Getty Images

> *The SSO material provided by (ISC)² and the Center for Cyber Safety and Education is exceptional and delivers all the right messages to the audience. I truly loved presenting to children as well as parents. The thought that my efforts made the internet a bit safer to all those kids gives me immense satisfaction and pride as a mom and as an IT security professional.*
>
> *—Hyma Pandyaram, CISSP, (ISC)² Alberta Chapter*

> *It is an honor to share cybersecurity tips and hints with senior citizens from all around the world. They are a target of cybercriminals and it is our responsibility to help them stay safe and enjoy the benefits of being online.*
>
> *—Juan Araya, Volunteer, Spain*

The Safe and Secure Online trainings are available in 20 languages, and you can download them for free from our website www.IAmCyberSafe.org. No special training, applications or background checks required. All you need is the knowledge and desire to help make the cyber world a safer place for everyone. Feel free to share with us your stories and photos at center@isc2.org.

Advice on Blacklisting IP Addresses, Prep for the CISSP Exam, Effective Endpoint Protection

QUESTION:

I see high levels of failed login attempts to our Microsoft 365 environments and could spend my life blacklisting these IP addresses. A similar issue applies to the volume of malicious emails that we receive, mostly blocked but sometimes getting through the net. We have other layers of controls in place but would like to address the issue at the source. I'd be happy to hear your thoughts on the most effective measures to deal with these malicious computers.

—Posted by RichT

SELECTED REPLIES:

How about subscribing IP reputation-based filters? I believe it should have some automation in place to list and delist bad and good IPs.

—Posted by Vasan

You can always create a null route on your border router and add the list of blacklisted IP addresses on that if you are not an ISP. Another way is creating a network object group on your firewall for upstream and downstream.

—Posted by harvinderdhami

I am frequently relying on Check Point's suspicious activity rules that are being dynamically created to block originating IPs for predefined periods of time after x failed logon attempts, network or port scans. This not only deals with botnet-infested sources, but limits the activity of Shodan and like services from spilling the data about your network.

—Posted by vt100

Find this complete thread here.

QUESTION:

In preparing for the CISSP exam, I have used online class training, the Sybex official study guide and Sybex practice tests. Some of my friends have advised me to take the Boson practice exam to really judge if I am ready to take the real exam. Is it a "definite must" for anyone preparing for the CISSP exam?

—Posted by Gerald-victor

SELECTED REPLIES:

I used Boson to prepare. For me, the value was in the detailed explanations they provide for both the correct and incorrect answers. The actual exam will test your ability to apply knowledge in sometimes not-so-straightforward ways.

—Posted by chogan

I just used the practice questions in the (ISC)² textbook and All-in-One. The usefulness of the questions is in working out if you understand the domain. Don't fall into the trap of thinking you will do well on the exam simply by taking practice tests; try to learn the material by transforming into your own understanding, i.e., what works for you in understanding and recalling it.

—Posted by Steve-Wilme

Find this complete thread here.

QUESTION:

We are looking for an alternative for our current EPP (endpoint protection platform), which is more than AV (antivirus) alone. I had a short presentation by a vendor that seems to have developed its solution from scratch. They are officially an EDR (endpoint detection and response) vendor; however, they told me that other customers have replaced their AV solutions with this vendor's product. Do you think there is really a (sharp) distinction between EDR, AV and EPP at all?

—Posted by the_admin

SELECTED REPLIES:

I think you are getting caught up in the name game! Forget what they are calling things and look just at what they can and cannot do. If you drop or hide all the names and look just at functionality, what do things look like? Every vendor will claim its product is the best and can do it all, until you want to see it done!

—Posted by JKWiniger

EDR or even MDR (managed detection and response) is the new AV these days, watching user behavior and other characteristics from the cloud. They do this by using all the many customers' intelligence, building up use cases and collaborating with many others to provide a universal picture of what is going on in the real world. Especially during the world situation at the moment, this is vitally important.

—Posted by Caute_cautim

Find this complete thread here.

(ISC)² Community Is Updated! Take A Fresh Look and Connect with Your Colleagues

The (ISC)² Community has a new look and feel, an updated user experience and new groups added to enhance your career development as you collaborate with colleagues and share information on topics within cybersecurity. The Community is a tool to discuss new technologies and regulations, best practices, professional development, the challenges and opportunities facing the cybersecurity workforce, ways to make the most of your (ISC)² certification, membership and much more. Log in to see the updates or create your (ISC)² Community account today!

(ISC)²

Earn CPEs

While Building Cybersecurity Skills

Seeking more ways to keep cybersecurity skills sharp and knowledge fresh? (ISC)² Professional Development Institute (PDI) has you covered with the flexibility of online, self-paced courses. Dive into our portfolio of over 35 online courses – **FREE for (ISC)² members** and available for purchase by non-members. Build skills and earn 100+ CPEs, no travel required.

Stay on top of your craft with…

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

Start FREE Courses

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