

WHERE PEOPLE (NOT TECHNOLOGIES) ARE THE DIFFERENTIATORS

InfoSecurity PROFESSIONAL

SEPTEMBER/OCTOBER 2022

Practical Advice. Actionable Insights.

DOXXING

IT'S WAY MORE THAN PUBLIC DISCLOSURES

IS THERE AN UPSIDE
TO DEEPPAKES?

BREAKING DOWN SOCIAL
MEDIA'S RISKS

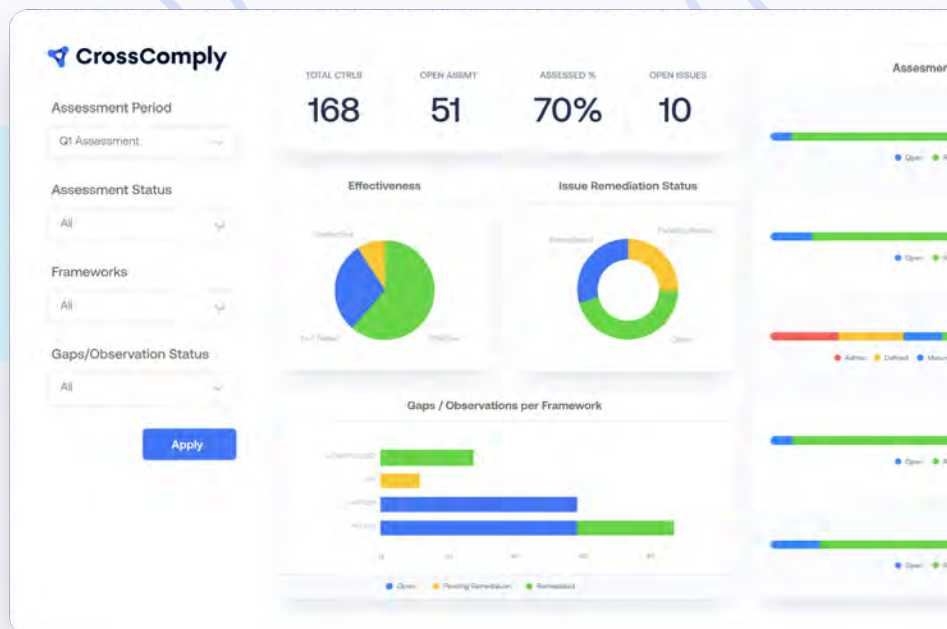


(ISC)²

Security Compliance, Accelerated.

Simplify and scale your compliance program with a platform that unifies SOC 2, ISO 2700x, NIST, CMMC, PCI DSS, and more across your organization.

- ▶ Assess Once, Comply With Many
- ▶ Automate Evidence Collection
- ▶ Get Real-Time Insights



- **Scale Quickly**

Automatically map new frameworks to your controls with a Unified Compliance Framework® common control set.

- **Reduce Duplicative Work**

Leverage the common controls crosswalk to visualize the overlap across frameworks and avoid audit fatigue.

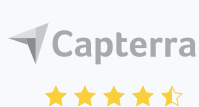
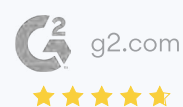
- **Eliminate Manual Evidence Collection**

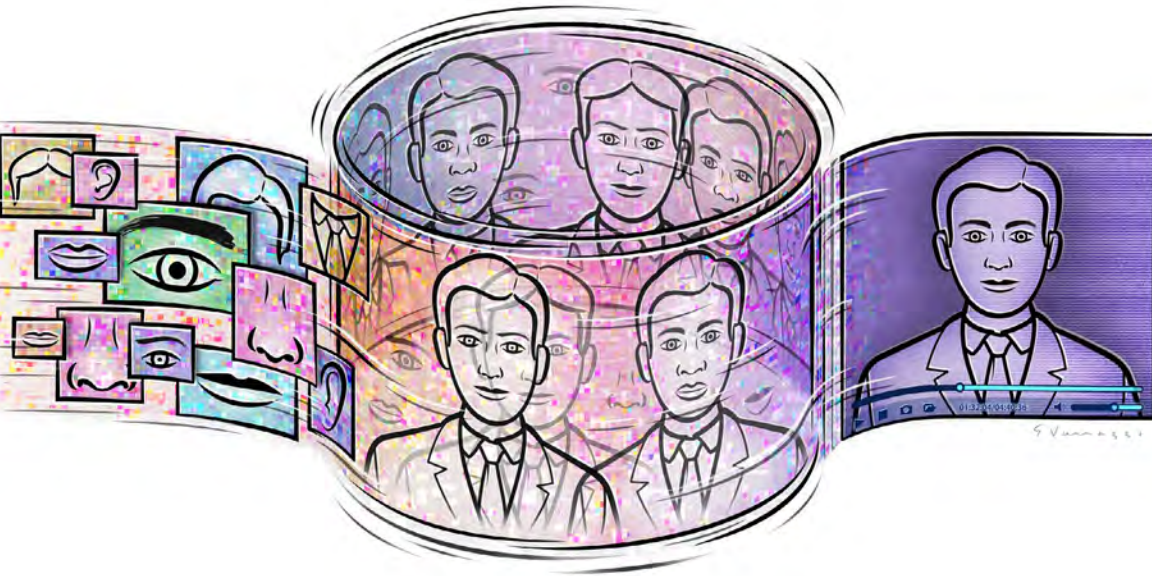
Connect directly with your source systems to obtain the needed information and consolidate requests.

- **Track Issues in Real Time**

Get visibility into identified issues, gaps, vulnerabilities, and action plans with dashboards and powerful reporting tools.

Top-Rated by Customers





Limiting the negative impact of deepfakes.

PAGE 33

FEATURES

27 Doxxing

BY MICK BRADY

It's way more than public disclosures.

33 Seeing is Disbelieving

BY PAT RARUS

The impact of deepfakes on today's cybersecurity.

39 Strategies to Handle Risky and High-Stress Situations

BY VINCENT T. COVELLO, PH.D.

An excerpt from *Communicating in Risk, Crisis, and High Stress Situations: Evidence-Based Strategies and Practice*

DEPARTMENTS

5 Editor's Note

On the internet, everyone does know you're a dog.

BY ANNE SAITA

9 Executive Letter

Let's have a chat, shall we?

BY JOHN GIDDINGS, VP, GLOBAL CUSTOMER EXPERIENCE, (ISC)²

11 Field Notes

(ISC)² Security Congress preview; free certification education and exams announced; (ISC)² chapters reach 10-year milestone; magazine recognized for excellence; (ISC)² Global Achievement Award recipients for 2022; and more.

22 Member's Corner

What accounts for the West's most serious cyber risk?

BY MICHAEL WIGLEY, CISSP

25 Help Wanted

Background checks are key to avoiding risky business.

BY DEBORAH JOHNSON

45 Office Hours

How to earn respect and influence others.

BY MICHAEL HANNA, CISSP

7 ADVERTISER INDEX

Cover illustration by
John Jay Cabuay

Illustration (above) by
Enrico Varrasso

Page 39 illustration (right)
by Zhenia Vasiliev





RISK,

PRIORITIZED



- FIND RISKS AND ELIMINATE BLIND SPOTS
- FOCUS ON WHAT MATTERS
- FIX ISSUES AT THE SOURCE

LEARN MORE



Cloud Security
from Source to Run



3 CVE-2022-17752



EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

On the Internet, Everyone Does Know You're a Dog

OUR BELOVED FAMILY DOGS DIED within two weeks of each other—one from old age and one from cancer. As all pet lovers understand, these were huge losses for us. Bereavement is commensurate with the depth of our relationships with the departed, and in that regard some of us (maybe most) grieve passionately and persistently when a pet passes. That's partially because of the unique social contract we have with these animals. In exchange for keeping them fed, groomed, exercised and sheltered, we humans receive unconditional support when we need it (and sometimes when we don't). They keep our secrets and ease our stress. They force us outdoors and to interact with neighbors and strangers we'd otherwise ignore.

Most of the time, we present articles in *InfoSecurity Professional* to help you professionally. This time, we focus on online dangers such as doxxing and deepfakes. We offer pointers for regaining ground when attacked on social media. It's a scary world out there, but I don't need to tell you that.

The same month we said good-bye to Pip and Axel, my two granddoggies celebrated a social media milestone—their Instagram account surpassed the 1,000-follower mark. It's still climbing as I write this. Their manager, my son-in-law, explained that Ford and Brewer figured out quickly that playing nice and showing kindness garner lasting attention, slowly but surely. The pair behave as if they aren't popular and put up with paparazzi on outings. No deepfakes needed with those two photogenic Labrador retrievers. Nor would they ever consider causing harm through online harassment.

Years ago, when the online world was more mysterious than malevolent, *The New Yorker* published a now-famous illustration in which a dog sitting in front of a desktop turns to his canine companion and says, "On the internet, nobody knows you're a dog." It was a warning to users that they may not really know who they are engaging with online.

That's still true, as this issue illustrates. But I never really knew if the illustrator meant dog as in animal, or dog as in someone unpleasant, even wretched. Either way still works. Even in a world where humans now are behind the online accounts of actual dogs. •



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

Photograph by Louise Roup

We offer pointers for regaining ground when attacked on social media. It's a scary world out there, but I don't need to tell you that.

CONTRIBUTORS



Mick Brady, who wrote our cover story, once drove more than 700 miles in winter weather to

appear in a community theater production, arriving 10 minutes before the show started. "I had a very good reason for being away, and no one would have faulted me for not making it back on time, but I was one of four actors in a cast that had no understudies, and I didn't want to let everyone down," she says. It's an example of how she'll literally go the extra mile to get a job done.

Pat Rarus, a seasoned writer with roots in medical tech, found the subject of her article on deepfakes to be fascinating... and troublesome. Pat previously contributed to our bimonthly newsletter, *Insights*.



Dr. Vincent T. Covello penned the excerpt from his latest book *Communicating in Risk,*

Crisis, and High Stress Situations: Evidence-Based Strategies and Practice (IEEE/Wiley, 2021). He is the director of the Center for Risk Communication and author of more than 100 articles in scientific journals.

London-based illustrator **Zhenia Vasiliev** honed his skills as an information designer. Beyond applying his talents on one of our feature articles, Zhenia's focus is on creative content such as iconography, spot illustrations and animation assets. His clients include *The Guardian*, *The New York Times*, Adobe, United Nations, NBC Universal and many more.

As a creative, Ontario-based **Enrico Varrasso** does it all—from his highly conceptual editorial illustrations (like interpreting GAN technology), to his mixed media fine art incorporating everything from wood, metal, paint and more. When not creating, Enrico enjoys traveling.

A “Shadow Data in the Cloud” Primer for Information Security Professionals



Amit Shaked
CEO and Co-founder,
Laminar Security

What is Shadow Data in the Cloud?

As a quick definition, Shadow Data is your company’s data that is likely copied, backed up or housed in a data asset that is not governed, under the same security structure, nor kept up-to-date. Shadow Data assets are spawned by your daily, weekly, monthly, and even yearly operations. So, without controls, Shadow Data assets don’t go away, ever, and their numbers increase over time.

Why is this important?

Shadow Data assets often contain sensitive data and company Intellectual Property yet are typically underprotected if not totally unprotected. As such, malicious hackers target these assets. A couple of recent examples:

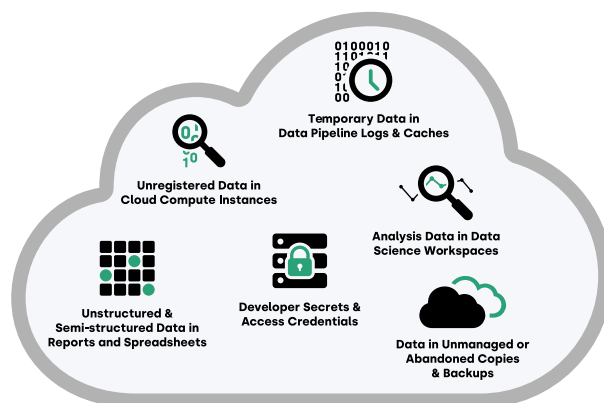
- SEGA Europe data breach (Jan 2022): The massive gaming company inadvertently left users’ personal information publicly accessible on an Amazon Web Services S3 bucket. The mishap enabled hackers and cybercriminals to dig into many of SEGA Europe’s cloud services, MailChimp, and Steam.
- Sephora (Mar 2022): Almost half a million customers’ sensitive data including PCI, PII, and more were leaked. Shadow Data was exported from their production database and stored in an unsecured, publicly accessible Amazon S3 bucket.

Where does Shadow Data live?

Most companies have Shadow Data in the following locations:

- Test Environment: Most organizations have partial copies of their production data in test environments.
- Backups: In addition to primary Shadow Data, often the backups become Shadow.
- Leftover Data from Cloud Migration: Frequently, the original data is not deleted “just in case” it’s needed.
- Toxic Data Logs: Developers and log frameworks log sensitive data, which creates sensitive files that are not classified as sensitive and are unprotected.
- Analytics Pipeline: Company analytics pipelines typically contain sensitive data.

Shadow Data Examples from Customers



Where can you learn more?

Find us at (ISC)² Security Congress | Booth #219
Read our blog: <https://laminarsecurity.com/blog/>

READ. QUIZ. EARN.

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

In order to earn the two CPE credits, you must pass the issue quiz. Please provide your name and (ISC)² member number so that we can award the two CPE credits to your account. This typically takes up to 30 business days to be added to your account.

The quiz and CPE credit opportunity for this issue will be available for 12 months from the date of publication.

<https://www.isc2.org/InfoSecurity-Professional>

Learn about more opportunities to earn CPE credits at <https://www.isc2.org/Membership/CPE-Opportunities>

ADVERTISER INDEX

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

Auditboard.....	2	(ISC) ² SECURE Summits.....	21
Sysdig.....	4	Synopsys.....	23
Laminar Security	6	(ISC) ² Build Your Best Team, Entry-level Up...24	
(ISC) ² Security Congress.....	8	(ISC) ² Volunteer Program.....	26
(ISC) ² Essential Skills eBook.....	10	Google-Chronicle, LLC.....	31
SEM.....	14	(ISC) ² Certified in Cybersecurity:	
SimSpace.....	15	Throw Down the Ladder.....	32
Menlo.....	17	Imperva.....	37
Wallix.....	18	(ISC) ² Commit: CCSP-#1 in Cloud Security ..	38
(ISC) ² 2022 SECURE Webinars.....	19	(ISC) ² CISSP/CCSP: Power Duo	44
		(ISC) ² CCSP Evolved - New Training	46

InfoSecurity Professional is produced by Twirling Tiger® Media. 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. ©2022 (ISC)² Incorporated. All rights reserved.

(ISC)² MANAGEMENT TEAM

EXECUTIVE PUBLISHER
Chris Green
+44-203-960-7812
cgreen@isc2.org

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

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

SR. CORPORATE COMMUNICATIONS SPECIALIST
Andrea Moore
727-270-9613
amoores@isc2.org

EDITORIAL ADVISORY BOARD

Anita Bateman, U.S.
Felipe Castro, Latin America
Brandon Dunlap, U.S.
Rob Lee, EMEA
Jarred LeFebvre, (ISC)²

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

TWIRLING TIGER MEDIA MAGAZINE TEAM

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

ART & PRODUCTION DIRECTOR
Maureen Joyce
mjoyce@isc2.org

Twirling Tiger Media is an award-winning women-owned content marketing company. This partnership reflects (ISC)²'s commitment to supplier diversity.



12th Annual

(ISC)² | SECURITY CONGRESS

EMPOWER YOUR FUTURE

Join thousands of leading experts from around the world at our industry's must-attend event of the year. Get a jolt of inspiration at this one-of-a-kind meeting of the minds, driven to advance innovation, leadership and growth in cybersecurity.

Impactful Keynotes



Ian Bremmer



Carey Lohrenz



Ciaran Martin



Robert Mazur

New for You:

- 100+ Sessions — explore the hottest topics in infosec, risk management, incident response, forensics and much more
- Nightly Networking Events — reconnect with your colleagues and make new professional connections in person and virtually
- Career Center Resources — get ahead with one-on-one consultations, resume reviews and more
- Exhibit Hall, In-Person and Virtual — learn about the latest products and technologies and chat with the vendors
- Pre-Conference Training — take a deep dive into CISSP®, CCSP and the new Certified in CybersecuritySM entry-level certification

(ISC)² members, this is your biggest CPE credit opportunity of the year!

[Register Now](#)

October 10 - 12, 2022 • Caesars Palace, Las Vegas
In-Person + Virtual

Let's Have a Chat, Shall We?

BY JOHN GIDDINGS, (ISC)² VICE PRESIDENT OF GLOBAL CUSTOMER EXPERIENCE

At (ISC)², we aspire to be a world-class and award-winning operation, where people (not technologies) are the differentiators. When consumers talk about a great customer experience, they often talk about the people impact. We want to have that impact on our members too, which is why we're planning changes to ensure members receive excellent customer service when and where they wish.

One way to provide prompt communications is through live chats—with humans, not bots. Live chat fulfills customers' main asks: to engage immediately with polite, friendly employees who can resolve an issue or answer a question quickly—without the back-and-forth of emails and voice messages at odd hours. Similarly, members should have the option to instant-message us and receive timely, requested information regardless of their location in the world.

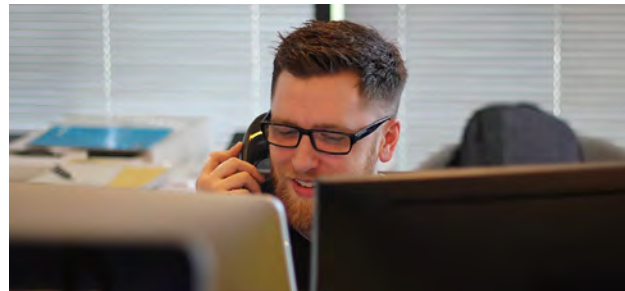
Such an omnichannel approach is coming to (ISC)². As the (relatively) new vice president of global customer experience for the organization, I will be overseeing an expansion of digital communications tools, so members can talk to us through their channel[s] of choice.

This is part of a broader strategic vision and global customer experience in which we remove siloed regional offices and unite the Americas, EMEA and APAC regions under one global roof, so to speak. This drives up economies of scale and allows a member to gather information from anyone and anywhere in the world—at any time.

Such initiatives are backed by findings in the most recent U.S. Contact Center Decision-Makers' Guide for how brands can improve their customer experience through management, technology and strategic changes. With more than 200 participating contact centers, the annual study is among the largest of its kind.



John Giddings is (ISC)² vice president of global customer experience. He can be reached at jjiddings@isc2.org.



The latest report shows most importantly that a customer contacting an organization, either by phone or digitally, wants:

- Issues or questions resolved on the first attempt
- A short wait time for a response
- Polite and friendly employees

Thirty percent of both customers and businesses also want choices in communications channels. With more options, our members can talk with someone as and when needed and receive prompt responses and resolutions to any issues or questions they have.

A smooth customer journey leaves a lasting impression that benefits both the member and the organization it serves. I've seen this happen with other established brands where I've worked, including IKEA and Virgin, and the International Association of Certified Public Accountants.

This is the vision I carried into the organization when I joined back in January, working out of the United Kingdom. Elevating day-to-day global customer satisfaction with a consistent and positive end-user experience, whether an existing or prospective (ISC)² member, is not just aspirational; it's achievable.

I look forward to introducing a more modern way for everyone at (ISC)² to assist you on your journey to building a bigger and better cybersecurity career. •

ESSENTIAL SKILLS

Make the Difference

Building your strongest cybersecurity team requires more than technical knowledge. Successful candidates need essential skills like problem-solving, analytical thinking and creativity to make an impact and move your organization forward.

When recruiting for your cybersecurity team, seek out critical thinkers, team players and individuals passionate about solving problems and finding a role that fits their skills. Learn more in the eBook, *6 Essential Skills to Hire for in Cybersecurity*.

Inside the eBook:

- Communication and Collaboration Skills to Look for in Cybersecurity Candidates
- Where Technical Training Comes In
- Preparing Your Team for Success

[Get the eBook](#)



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

All Bets are Good at This Year's (ISC)² Security Congress

THERE'S STILL TIME to register (and at early bird pricing!) for the 12th annual (ISC)² Security Congress being held October 10–12, in-person at Caesars Palace in Las Vegas and live online. The first hybrid Security Congress will provide plenty of opportunities for cybersecurity professionals to learn and network both online and on site.

(ISC)² members earn significant CPE credits, including 20 or more for live, in-person attendees and 17 or more for live, virtual attendees. Participants can earn up to 100 CPE credits by accessing the recorded sessions through December 31, 2022.

Other conference highlights:

- Pre-conference training courses on our most popular certifications including CISSP, CCSP and our newest entry-level Certified in Cybersecurity certification are available both in-person or virtual.
- Virtual attendees can access sessions live and for replay after 24 hours. There also will be a virtual exhibit hall, online access to the (ISC)² Career Center, virtual bookstore, and opportunities to interact live with other attendees.



- In-person conference-goers will have almost three full days of presentations, including five keynotes and more than 100 interactive breakout sessions, evening networking events, access to the (ISC)² Career Center, bookstore and exhibit hall with more than 50 vendors.

Don't leave anything to chance. Visit congress.isc2.org to learn more, including early bird price deadlines, to advance in your cybersecurity career. •

Photograph by Stephen Leonardi on Unsplash

LOOK WHO'S TALKING

Keynote speakers for (ISC)² Security Congress include experts in fields outside of cybersecurity to help attendees better manage risks, threats, users, workforces and careers.

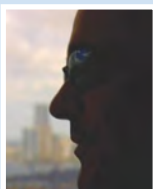
**Ciaran Martin, Founding CEO,
UK National Cyber Security Centre**

Tuesday, October 11, 2022
Cybersecurity Insights



**Robert Mazur, President
of KYC Solutions, Inc.**

Tuesday, October 11, 2022
Why \$2 Trillion is Laundered
Every Year



**Ian Bremmer, President and
Founder of Eurasia Group
and GZERO Media**

Wednesday, October 12, 2022
Managing Risk in an Unstable World



**Carey Lohrenz, First Female U.S.
Navy F-14 Tomcat Fighter Pilot**

Wednesday, October 12, 2022
Help Your Team Triumph in a
High-Risk, Time-Crunched World



(ISC)² Pledges to Expand and Diversify the Cybersecurity Workforce with Free Certification Education and Exams for One Million

REGISTRATION OPENS IN SEPTEMBER for the new (ISC)² One Million Certified in CybersecuritySM program, which will put one million people through its foundational Certified in Cybersecurity entry-level certification exam and education program—for free. The program builds upon the success of the (ISC)² 100K in the U.K. initiative, which pledged 100,000 free exams and course enrollments for U.K. residents earlier this year.

Announced during the Cyber Workforce and Education Summit at the U.S. White House in July, the program builds upon (ISC)² leadership in delivering solutions to our global cybersecurity workforce challenges. Research suggests organizations that focus on recruiting and developing entry-level cybersecurity staff—including those with little or no technical experience—accelerate the invaluable hands-on training the next generation of professionals needs to start a successful cybersecurity career.

“Our 100K in the U.K. program garnered more than 10,000 applicants in its first two months. It is a resounding call to action for organizations serious about expanding the cybersecurity workforce to make the necessary investments now to break down barriers and clear obstacles for anyone interested in a cybersecurity career.”

—Clar Rosso, CEO, (ISC)²



Those who earn the (ISC)² Certified in Cybersecurity certification, which was globally piloted earlier this year, can demonstrate to employers that they have the foundational knowledge, skills and abilities necessary for an entry-level cybersecurity role.

“Our 100K in the U.K. program garnered more than 10,000 applicants in its first two months. It is a resounding call to action for organizations serious about expand-

ing the cybersecurity workforce to make the necessary investments now to break down barriers and clear obstacles for anyone interested in a cybersecurity career,” said Clar Rosso, CEO of (ISC)², in a prepared statement.

How the program will work

Qualified individuals will receive a free exam, as well as access to the (ISC)² Certified in Cybersecurity online self-paced education course. The course provides a review of the subject matter published in the Certified in Cybersecurity exam outline, which shares the security concepts on which certification candidates will be evaluated, including:

- Security principles
- Business continuity (BC), disaster recovery (DR) and incident response concepts
- Access controls concepts
- Network security
- Security operations

University students, recent graduates, career changers and other professionals wishing to expand their skills and opportunities are encouraged to participate, especially individuals employed or seeking employment within small and mid-sized businesses.

(ISC)² will work closely with new and existing partner organizations to reach historically under-represented populations and encourage greater diversity within the cybersecurity community. (ISC)² has pledged that half of the expanded commitment—500,000 course enrollments and exams—will be directed toward students of historically black colleges and universities (HBCUs), minority-serving institutions, tribal organizations, women’s organizations and those with disabilities across the globe.

After successfully completing the exam, candidates will become (ISC)² members with access to a wide array of professional development resources to help them throughout their careers. The (ISC)² entry-level cybersecurity certification is the first step on a career-long journey that will help cybersecurity professionals gain experience and work toward advanced qualifications such as the (ISC)² CISSP and (ISC)² CCSP.

For more information on the (ISC)² Certified in Cybersecurity, please visit www.isc2.org/certified-in-cybersecurity. ●



Fifty (ISC)² Chapters Celebrate a 10-Year Milestone



THIS MONTH MARKS a major milestone for 50 (ISC)² chapters celebrating their 10th anniversary as an official chapter.

The (ISC)² Chapter Program was launched in September 2011 at the first (ISC)² Security Congress, with several chapters being established in the first year. Since then, (ISC)² chapters have made a significant impact worldwide by establishing meaningful connections, providing education on latest trends and technologies, inspiring the next generation in their career path, and securing communities by generating cybersecurity awareness and empowering others to be safe online.

Congratulations to the following chapters on this impressive achievement:

- Alamo Chapter
- Alberta Chapter
- Argentina Chapter
- Atlanta Chapter
- Auckland Chapter
- Austria Chapter
- Baltimore Chapter
- Central Florida Chapter
- Central Ohio Chapter
- Charleston Chapter
- Chennai Chapter
- Chicago Chapter
- Chile Chapter
- Cleveland Chapter
- Colombo, Sri Lanka Chapter
- Cyprus Chapter
- Eastern Massachusetts Chapter
- Ethiopia Chapter
- Gauteng Chapter
- Germany e.V. Chapter
- Ghana Chapter
- Greater Detroit Chapter
- Hong Kong Chapter
- Hungary Chapter
- Italy Chapter
- Kenya Chapter
- Korea Chapter
- Kuwait Chapter
- Maine Chapter
- National Capital Region Chapter
- New Jersey Chapter
- New York Metro Chapter
- Omaha-Lincoln Chapter
- Ottawa Chapter
- Philadelphia Chapter
- Phoenix Chapter
- Pikes Peak Region Chapter
- Pittsburgh Chapter
- Romania Chapter
- San Francisco Chapter
- Silicon Valley Chapter
- Singapore Chapter
- St. Louis Region/Scott AFB Chapter
- Switzerland Chapter
- Tampa Bay Chapter
- Toronto Chapter
- Twin Cities Area Chapter
- Utah Chapter
- Virginia Peninsula Chapter
- West Michigan Chapter

If you are interested in joining an (ISC)² chapter or starting one, visit www.isc2.org/chapters.

Magazine Earns International Recognition (Again!)

FOR THE SEVENTH CONSECUTIVE YEAR, *InfoSecurity Professional* has earned top honors in two journalism and design contest for business and trade publications.

The March/April cover story on 5G cybersecurity risks took home the national Silver Award in the Technical Feature category at the 2022 American Society of Business Publication Editors' Awards of Excellence program. The article also won the Bronze Award in the Technical Article category at the 2022 Trade, Association and Business Publications International (TABPI) program. The same article, as well as the art and design for an article on quantum cryptography, took the gold award in the regional competition.

The magazine's editorial and creative teams also have earned past excellence awards from AM&P Network EXCEL Awards from the Software & Information Industry Association (SIIA).



End-of-Life HDDs: Degauss and Destroy

For magnetic hard disk drives (HDDs), the only way to ensure complete data sanitization is to follow the NSA's mandate to degauss and destroy.

SEM's best-selling NSA listed degauss and destroy package includes the EMP1000-HS degausser and 0101 hard drive crusher for a secure, economical solution for classified and sensitive HDD sanitization.

Trusted by the U.S. Government, Intelligence Community, and the world's top cloud service providers.



Global Leader in High Security Information
End-of-Life Solutions for Over 50 Years



- ▲ EMP1000-HS degausser
- ▲ 0101 HDD crusher



800.225.9293 | www.semshred.com

October is International Cybersecurity Awareness Month

NEED A REASON TO REINFORCE cybersecurity best practices? Both the European Union and United States will celebrate Cybersecurity Awareness Month in October with special programs, announcements and security awareness activities to promote better cyber hygiene worldwide.

Major themes surrounding the 10th annual European Cybersecurity Month are phishing and ransomware. In the U.S., the Department of Homeland Security plans to provide multimedia tips to #BeCyberSmart during National Cyber Security Awareness Month.

Looking for ways to celebrate #CyberSecMonth at your organization? Visit <https://cybersecuritymonth.eu> for a list of upcoming activities in EU countries and other helpful resources. Find more resources at <https://www.isc2.org/cybersecurity-awareness-month>.



Photograph by AbsolutVision on Unsplash



Creating Cyber Confidence.

SIMSPACE CYBER RANGE

ATTACK SIMULATIONS

ACTIONABLE INSIGHTS

[SimSpace.com](https://simspace.com)
info@simspace.com
simspace.com



2022 © SimSpace Corporation. All rights reserved.



Announcing This Year's (ISC)² Global Achievement Award Recipients

Congratulations to the following security professionals recognized for their outstanding contributions to the cybersecurity industry. The annual (ISC)² awards honor exceptional practitioners for their commitment to a safer cyber world for one and all. Each will be honored at next month's (ISC)² Security Congress in Las Vegas.

(ISC)² Senior Professional Award

Recognizing individuals who have significantly contributed to the enhancement of the information security workforce by demonstrating a leadership role in an information security workforce improvement initiative, program or project. The 2022 honorees:

Americas:

Shawn Harris, CCSP, CISSP, CISSP-ISSAP, Senior Director of Information Security and Compliance, Chipotle Mexican Grill



For his involvement in the development and implementation of the Cloud Controls Matrix (CCM), a cybersecurity control framework for cloud computing aligned to the Cloud Security Alliance best practices, considered the de facto standard for cloud security and privacy.

APAC:

Chou Yen Ju, CCSP, CISSP, Chief Information Security Officer, OneDegree Hong Kong Limited



For his role in developing the Digital Asset Risk Assessment, a methodology to help the insurance industry better manage escalating cyber risks.

The methodology contributed by this project has been reviewed and approved by the Hong Kong Insurance Authority. An insurer/reinsurer can provide insurance coverage to the industry based on this methodology.

OneDegree is the first insurer in APAC and the second insurer in the world that provides digital asset exchanges, custodians, and wallet solution providers the insurance coverage. The project helps the industry with the best practice to manage the escalating cyber risk. Chou Yen Ju led a task force to contribute the Digital Asset Risk Assessment methodology to the underwriting, which realizes Chou Yen Ju's vision of reducing the knowledge gap between the underwriters and cyber professions. The methodology can evaluate the digital asset's risk and provide the clients the best practice to manage the risk with the insurance coverage.

EMEA:

Ali Isikli, CCSP, CISSP, Systems Security Engineering Manager, ASELSAN Inc.



For founding the ASELSAN Cyber Security Team to oversee customer, internal development and management efforts to assess, identify and evaluate the cybersecurity maturation of systems. The initiative is said to have impacted more than 10,000 people tied to Turkey's defense industry.

(ISC)² Mid-Career Professional Award

Recognizing individuals at their mid-career stage who have demonstrated commitment and achievement in managing or implementing a vital component of a cyber, information, software or infrastructure program/project. The 2022 honorees:

Americas:

Benjamin T. Koshy, CISSP, Chief Information Security Officer, Indian Health Service



For expanding the utility of Indian Health Service's security information and event management (SIEM) system, which was previously only used to gather a small subset of security logs from information systems for use in incident response. This enabled Indian Health Service to not only satisfy the cybersecurity logging requirements but also provide the service analytics to enhance the IHS mission objective.

APAC:

Shakthi Priya Kathirvelu, CISSP, VP and Head of Information Security and IT, Funding Societies | Modalku Group



For her efforts to build out and lead a dedicated information security team developing a digital financing and debt investment platform for Southeast Asian small and mid-sized enterprises. She's also recognized for expanding into a leading neobank to provide a secure customer experience, while ensuring regulatory compliance in the countries the business operates in.

In addition to contributing to fundraising for the organization, her efforts have also helped secure corporate resources during a period of significant growth for the organization.

EMEA:

Lucy Prudence Shenton, CISSP, Expert Associate Partner, McKinsey & Company



For her role in building a cybersecurity roadmap for a large, global financial institution. Lucy led the strategic vision and secured a multi-million-dollar, board-level commitment to drive maximum impact—and data security—for all internal and external customers.

The program continued with a deep dive architectural design into improving user experience and strengthening the security of the organization's identity and access management (IAM) capabilities as well as implementing a proof-of-concept of its Zero Trust identity architecture. In the end, this program not only helped to secure and

protect enterprise-wide data, it also resulted in a differentiator for the organization by envisioning a streamlined identity and access management process for its millions of external customers and internal users.

(ISC)² Government Professional Award

Recognizing government information security leaders whose commitment to excellence has helped to improve government information security and to advance an in-demand workforce. The 2022 honorees:

Americas:

Jermone Andre Leach, CAP, CISSP, Defensive Cyber Operations Lead, United States Coast Guard



For his efforts in ensuring industry standard awareness and threat remediation. This includes a focus on International Defensive Cyber's Hunt Forward Operations.

MENLO
SECURITY

Make it
never
happen

**Stop
zero-day
attacks in
like zero
seconds.**

makeitneverhappen.com

EMEA:

**H.E. Dr. Mohamed Hamad Al-Kuwaiti,
Head of Cybersecurity, UAE Government**



For being instrumental in elevating the UAE's position as a global leader in the cybersecurity field, improving the national cybersecurity capabilities and collaborating with other nations to improve the national cyber defense and response mechanisms. He led the UAE National Cyber Capacity Building initiative, which is a multipronged program addressing several crucial aspects to improve the UAE's national cyber resilience and strengthen the cyber security posture of the UAE.

(ISC)² Rising Star Professional Award

Recognizing the accomplishments and contributions of an up-and-coming professional who has made a significant impact in the information security industry early in their career. The 2022 honoree:

Americas:

**Rajvardhan Oak, Applied Scientist,
Microsoft**



For his involvement in the Network Protection team for Microsoft ads, developing novel algorithms to detect poor quality traffic originating from specific questionable sources using clustering and other machine learning techniques. One of the key breakthroughs that provided significant improvement in time-to-detect and time-to-mitigate was the correlation of data in a coherent manner across various disparate datasets to construct ground truth.

(ISC)² BOARD AWARDS

Recognizing outstanding contributions and achievements in the field of cybersecurity throughout a career. The following award recipients for 2022 were selected by the (ISC)² Board of Directors.

REGAIN CONTROL OF YOUR ACCESS WITH WALLIX PAM4ALL

**LEADER IN THE
2022 GARTNER®
MAGIC QUADRANT™
FOR PRIVILEGED
ACCESS MANAGEMENT**

WWW.WALLIX.COM



(ISC)² Diversity Award

The (ISC)² Diversity Award honors an individual who represents the core values of (ISC)² through significant contributions to driving a more diverse workforce in the cybersecurity community. The 2022 recipient:

Sarah B. Lee, Ph.D., Director, School of Computing Sciences and Computer Engineering, The University of Southern Mississippi



In 2019, Sarah co-founded The Last Mile Education Fund to provide financial support to college students in computing majors when they find themselves faced with challenges beyond their control. Since then, the nonprofit organization has provided funding for 1,200 women who were facing financial obstacles to degree completion. Recently, the organization was awarded a \$6 million grant by Microsoft.

The Mississippi Alliance for Women in Computing (MAWC) project that Sarah started in 2016 identified

and capitalizes on factors that influence and motivate female students and female African American students in Mississippi to enroll and persist in an undergraduate computing or cybersecurity major. Using discriminate analysis methods, the project analyzed which pre-collegiate experiences influenced them to enroll; determined which stakeholders influenced these girls in their decision-making process; and what programs are effective in impacting their persistence in the major. From there, a team created activities designed to engage girls and young women with computing and cybersecurity, emphasizing computational thinking and cybersecurity knowledge and awareness, as well as illuminate a pathway forward through Alliance partnerships.

MSAWC continues to generate interest and participation of women in computing and cybersecurity, improve recruitment and retention rates of women in undergraduate computing and cybersecurity majors, and help post-secondary women make a transition to the computing and cybersecurity workforce.

(ISC)² SECURE SUMMITS

(ISC)² SECURE Webinars bring you together with leading cybersecurity experts to explore solutions that answer the most critical challenges facing your region. Take back actionable ideas and strategies that help strengthen the security of your organization's cyber operations, assets and critical data. Cybersecurity professionals in every stage of their career are encouraged to attend.

Features:

- Earn 1.5 CPE credits for each webinar
- 60-Minute Presentation
- 30-Minute Live Q&A
- Live Chat with attendees
- Immediate access to CPE transcripts
- Download materials and resources

PRICING

Single webinar:
(ISC)² Member **\$99**
Non-Member **\$129**

Save up to **40%** by purchasing multiple webinars at once.

Asia-Pacific

September 26, 2022
December 5, 2022

North America

September 12, 2022
October 31, 2022

U.K. & Europe

September 19, 2022
November 14, 2022



(ISC)² CEO Award

The (ISC)² CEO Award is presented annually to (ISC)² members who have made a significant impact on the cybersecurity profession through dedicated and exceptional volunteer efforts. This award is a top honor among the annual (ISC)² Global Achievement Awards. The 2022 recipient:

Andrew Smeaton, CISSP, Chief Information Security Officer, DataRobot, Inc.



Andrew is being recognized for his heroic action in conducting a risky rescue mission for a colleague and his family who were in distress amidst the Ukraine crisis. His dedication to his team far exceeded any expectations, traveling 4,500 miles from his home in Boston, MA, U.S. to bring a co-worker’s family to safety. (ISC)² celebrates members like Andrew whose character, moral instincts and passion for people continue to inspire a safe and secure cyber world.

(ISC)² Chapter Recognition Awards

The (ISC)² Chapter Recognition Awards are presented to official chapters of (ISC)² within each region that best promote the vision of (ISC)² by inspiring a safe and secure cyber world. Each chapter has demonstrated a well-rounded offering of activities and services designed to benefit its members and affiliates while making a significant contribution to the profession and its local community through the core focus areas of the (ISC)² Chapter Program of Connect, Educate, Inspire and Secure. The 2022 recipients in each region are as follows:

**Americas:
New Jersey Chapter**



The chapter took a creative approach to overcome the challenge of the pandemic and quickly adapted to virtual connection with members with meetings every month as well as larger joint conferences with other organizations; they also held outdoor picnics. The chapter supported members and cybersecurity professionals by holding resume and personal branding/development workshops, certification bootcamps, mentorship programs, and partnering with multiple levels of schools including high school, college and graduate. The efforts across the different chapter focus areas of Connect, Educate, Inspire and Secure have had a global reach and impact.

**LATAM:
Mexico City Chapter**



One of the newest chapters that launched at the beginning of the pandemic and overcame adversity at every turn. The chapter held multiple virtual educational member meetings, partnered with universities to help prepare students for a career in cybersecurity, and developed a partnership with schools, the National Guard and police departments to raise cybersecurity awareness for parents and kids.

**APAC:
Colombo, Sri Lanka Chapter**



The chapter hosted a series of panel discussions and conferences with multiple organizations to connect with the community to foster education, raise awareness, and support diversity and inclusion. The chapter was a partner for the 14th Annual National Conference on Cyber Security, attended by 1,046 participants, where the president moderated the panel discussion on “COVID 19 Triggered Shift to Digital.” The chapter also offers mentorship programs and workshops for students that encourage them to pursue a career in cybersecurity, hosting multiple workshops with over 50 students in attendance at various sessions.

**EMEA:
Hellenic Chapter**



The chapter held multiple member meetings in addition to participating in industry events with other organizations. The chapter focused on connection by launching a newsletter and utilized social media to cultivate its membership. They implemented several creative ways to earn or win CPEs to reward chapter members and increase engagement. They held CISSP trainings, Safe and Secure Online presentations, and created cybersecurity awareness videos for parents and kids in collaboration with other organizations that are available to the public. The chapter received the Bronze award for “Public Cybersecurity Awareness” at Greek Cybersecurity Awards 2022. ●



SECURE SUMMITS

Make plans now to attend this exciting new event series in 2022.

Register today and join your peers for a collaborative deep dive into the latest cybersecurity issues impacting organizations in your local and regional markets. You'll come back inspired with new ideas and solutions from a diversity of perspectives.

Each SECURE Summit features:

- Expert Presentations
- Exclusive Networking
- 7 CPE Credits Available
- Exhibit Hall

IN-PERSON SUMMITS:

- [SECURE Washington, D.C.](#)
Friday, December 9
Renaissance Washington,
DC Downtown Hotel

LIVE VIRTUAL SUMMITS:

- [SECURE Asia-Pacific](#)
Thursday, November 10
- [SECURE UK & Europe](#)
Wednesday, November 16



LEARN MORE
AND REGISTER AT
www.isc2.org/events



INTERESTED IN SPONSORING? [EMAIL US](#) FOR MORE INFORMATION.

The West's Most Serious Cyber Risk

BY MICHAEL WIGLEY, CISSP

U.S. Air Force and Space Force Chief Software

Officer Nicolas Chaillan didn't mince words last September when he [posted his farewell in a lengthy LinkedIn post](#).

He wrote: "Please stop putting a Major or Lt. Col. (despite their devotion, exceptional attitude and culture) in charge of identity, credential and access management (ICAM), Zero Trust or cloud for one to four million users when they have no previous experience in that field—we are setting up critical infrastructure to fail. We would not put a pilot in the cockpit without extensive flight training; why would we expect someone with no IT experience to be close to successful?"

He was specifically referring to the U.S. Department of Defense, but the same could be said of many other government departments. It is certainly true within the U.K.'s Ministry of Defence.

Simply put: When it comes to certain countries' military, the role of IT security practitioners is not always well understood. People seem to understand the level of skills, training and certifications required to be an accountant, attorney, medical doctor or engineer. But for active duty members assigned to IT roles, their resumes do not necessarily match the role required.

The wrong people assigned to important IT tasks

In the [2021 \(ISC\)² Cybersecurity Workforce Study](#), participants admitted they experienced misconfigured systems, improper risk assessments and management, unpatched critical systems and rushed deployments as a result of staff being stretched thin. The same occurs when suitably qualified and experienced personnel are underutilized. We've probably all seen the person with limited knowledge auto-

matically clicking the "Next" button repeatedly during installation of complex enterprise software. Or the IT manager making a bad decision due to lack of technical experience.

In defense environments, we have additional frustrations stemming from:

- Poorly defined IT roles, including requisite qualification and experience requirements.
- Lower pay rates than in the private sector.
- Lack of career progressions available "in post" (requiring someone to move to an unrelated, often non-IT post to gain promotion).
- Unqualified recruiters that do not recognize who is most suitable for an IT role.
- Fixations on shiny new tools and ideas without considering the talent required to implement them.

This isn't to say that groups of well-motivated, innovative, experienced and trained IT professionals don't exist within the armed forces. It's just that there currently aren't enough of them, and those brought in—whether active duty or civilian—to fill the IT positions aren't necessarily up to the tasks. This poses a serious risk to national defense.

No better time to make changes

Something needs to change—now—as nations are already involved in "soft conflicts" that lack traditional weaponry and open warfare. We need our military organizations to develop:

- A professional IT/cyber career path within military organizations that allows for promotions.
- A flat management hierarchy so that

those higher up the management chain have a better understanding of what is happening and can respond accurately to threats.

- Assignment to the IT management hierarchy from within the same general IT discipline.
- Pay packages that reflect industry rates for civilians.
- A mechanism of tertiary education that delivers an appropriate supply of junior IT professionals.

The current ad hoc approach is also wasteful. Expensive training and experience is regularly lost to the organization when staff leave IT posts due to the lack of professional progression. This includes when someone moves to a non-IT post internally to gain promotion or resigns and goes into the private sector to remain within their chosen IT field.

All this may seem obvious to cybersecurity professionals who know the difficulties and dangers an ill-equipped cyber workforce poses. Yet assigning complex IT security

tasks to underqualified staff persists. When a complex knee surgery is needed, we don't allow unqualified and inexperienced physicians to perform the operation, but we tend to do the equivalent when it comes to critical infrastructure and national defense IT.

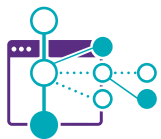
Yes, there's a global cybersecurity workforce shortage. And, yes, that includes a talent shortage within our armed forces. But placing the unskilled into complex IT security situations is not the answer. Change is needed, and now. ●



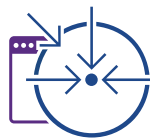
Michael Wigley, CISSP, is an experienced application software and platform solution architect. He started 40 years ago, after a mathematics and computing degree, as a programmer in the London Stock Exchange and moved into systems analysis and architecture through a wide variety of business areas, including health, aviation and telecoms. He is currently contracted to the U.K. Ministry of Defence and is a British Computer Society assessor (for Chartered status). Additionally, he is a cybersecurity/IA architect—senior practitioner under the U.K. National Cyber Security Center.

SYNOPSYS[®]

Build Trust in Your Software



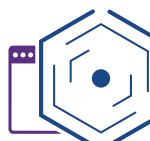
Black Duck[®]
Software Composition Analysis (SCA)
Secure and manage open source risks in applications and containers



Defensics[®]
Protocol Fuzzing
Identify defects and zero-day vulnerabilities in services and protocols



Coverity[®]
Static Application Security Testing (SAST)
Address security and quality defects in code as it's being developed



WhiteHat[™]
Dynamic Application Security Testing (DAST)
Verify the security of web applications in development and production



Seeker[®]
Interactive Application Security Testing (IAST)
Automate web security testing within DevOps pipelines



Code Dx[®]
Application Vulnerability Correlation
Correlate and prioritize test findings to provide insight into business risks

Learn more at

<https://www.synopsys.com/software-integrity.html>



Certified in
Cybersecurity

An (ISC)² Certification



Build Your Best Cybersecurity Team from Entry-Level Up

To help answer the critical need for new talent, (ISC)² launched the **Certified in CybersecuritySM (CC)** entry-level certification. With no experience required, it opens opportunities in the field to a much broader range of candidates to help organizations like yours build their strongest lines of defense.

Lower your hiring risk. When your employees are Certified in Cybersecurity, you're assured they've acquired the foundational knowledge of key cybersecurity concepts, determined by expert professionals in the field. As they gain experience, they'll be positioned to move into leadership roles within your organization.

Ready to identify potential cybersecurity candidates for your team?

[Build Your Team](#)

Background Checks are Key to Avoiding Risky Business

BY DEBORAH JOHNSON

In the rush to hire a promising candidate in this extremely competitive market, it is still vital to do a proper background check. A [survey](#) of 2,500 hiring managers by CareerBuilder revealed that 75% of the respondents have caught a lie on a candidate's resume. Skipping that background check is risky business, Jim Emanuel, Society for Human Resource Management Knowledge Advisor and Senior Certified Professional (SHRM-SCP), said in a phone interview: "The major reason to conduct a background and reference check is to avoid harm, even legal liability tied to the employer or to others."

Checking that a candidate is who they say they are involves more than a couple of reference checks, Emanuel added. "Background investigations would generally involve determining whether an applicant is not qualified for a position due to criminal conviction, motor vehicle violation, credit history or misrepresentation regarding education or work history because, these days, negligent hiring is really a compelling reason."

To do a complete background check, it might be wise to go with an outside agency, advised Patrick Proctor, SHRM-SCP, HR vice president at children's brand Hanna Andersson. "It's a disproportionate amount of busy work with making sure all the bases are covered." Specialists, he told me, "have a system to ensure that the details are captured and have a process that ensures that if they need to go to multiple states, for example, they can easily do that."

One more item to add to the checklist: social media. In a recent [survey](#) of 1,000 hiring "decision-makers" by the Harris Poll for Express Employment Professionals, 71% reported that "checking social media is an effective way to screen candidates."

Proctor said that hiring managers can learn a lot about a candidate from their online persona. "Unofficially, it's an indicator of how they might conduct themselves in managing the company's brand."

Jim Emanuel agreed: "Individuals choose to put their lives out there." He suggested going beyond a general background check because how an employee uses social media can inflict damage to the company brand, the culture and even employees.

While background checks can be tailored to specific positions, they must be done across the board, warned Emanuel. "You can't pick and choose who gets checked and who doesn't. You should apply it evenly with all new hires once you establish the criteria [and that] can change by position, by level of responsibility."

Finding a "glitch" in a background check does not necessarily mean the candidate should be immediately disqualified. "It's very important to [maintain] dialogue with the candidate," urged Proctor, to find out what exactly happened. It's also mandated in many states. "If you deny employment based on a finding on a background check, some states have legal language that [requires] letting the candidate know what you came across."

The bottom line, HR experts agreed, is that doing a healthy background check on prospective employees is crucial. "You owe it to the employees [as] their culture, their reputation, their brand can be really adversely affected. Do you wait until something happens before you take this seriously?" said Emanuel. "You don't want that news headline that finds out that this company didn't do a background check that could have negated whatever occurred." •



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



Serving as an (ISC)² volunteer is a rewarding experience that provides the opportunity to:

- Share ideas and expertise
- Work with colleagues outside your usual work environment
- Interact with industry experts
- Make an impact in the local and cybersecurity communities

The larger the pool of volunteers, the greater the variety of perspectives and ideas that benefit the organization. Our volunteer base is diverse, which brings a broad perspective, a wealth of ideas and a depth of understanding of member interests to the table.

(ISC)² offers a variety of ways for members to get involved, from short-term volunteer projects to committee, council and board services. With every new volunteer, (ISC)² grows more energized, diverse, inclusive and ready to reach our common goals.

**Give back and connect with your peers.
Be a part of the (ISC)² Volunteer Program!**

[Learn More](#)



DOXXING

IT'S WAY MORE THAN PUBLIC DISCLOSURES

BY MICK BRADY

DOXXING, A THREAT ACTOR TERM FOR “DROPPING DOCUMENTS,” or releasing private information, has become an insidious way to shame people around the world. Sometimes it is misguided retribution for behaviors others don’t appreciate, such as racism or bullying, or expressing controversial political views. Often it is an act of hatred or revenge, and the doxxing itself is fueled by racist, sexist or other malicious intent.

Doxxing is a slippery concept that defies efforts to pin it down with a precise definition. One perspective is that doxxing refers to the act of publicizing private information with the specific goal of causing physical harm.

ILLUSTRATION BY JOHN JAY CABUAY

A broader take is that doxxing refers to publicizing private information with the intent of creating emotional harm—bullying, harassing or intimidating, causing reputational damage or other negative consequences, with or without the component of a physical threat. However, a much more fluid description is gaining a foothold: Doxxing is the act of making public information more public. The common thread in these definitions is that doxxing is carried out with nefarious intent.

How can cybersecurity professionals guard against it without clarity on what constitutes the threat?

FOR THE PUBLIC GOOD

Establishing intent to harm is tricky, particularly in cases that involve the public interest. Investigative journalists regularly expose information that might otherwise be protected as private. “In the ’70s, if people were prevented from using private information, nothing about Watergate would have come to light,” noted Ed Moyle, systems and software security director for [Drake Software](#). “Intent has to be considered. The journalist’s goal is not to harass, although they’re putting out info someone might be very uncomfortable with.”

There is also the matter of accountability. Doxxing tends to apply to the actions of rogue operators who are trying to stay anonymous, observed Trip Hillman, director of cybersecurity services at [Weaver](#). With a journalistic endeavor, “there’s somebody who’s taking accountability for those resources and sources of information, vetting them based upon some agreed-upon methods before moving forward.” In many cases, a journalist’s disclosures would fall into the realm of “public interest.” The information is not necessarily in the public domain, but public interest in its disclosure outweighs the individual’s interest in nondisclosure.

Even if their intent is to serve the common good, journalists must exercise caution in deciding how much information is relevant to the public discourse. “For instance, pointing out a politician lives outside of the area they are required to live would be pertinent,” said Rob Enderle, principal analyst at the [Enderle Group](#). However, “giving their exact street address isn’t necessary for that story.”

The line between relevant information and too much detail is often blurry. Like United States Supreme Court Justice Potter Stewart’s famous [declaration](#) about pornography—“I know it when I see it”—identifying doxxing can be highly subjective. Yet there are high-profile cases that indisputably qualify.

FROM TOXIC TO LETHAL

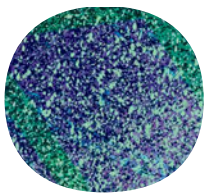
Following the deadly Boston Marathon bombing in 2013, an attempt at crowd intelligence-gathering went very wrong, as Penn Pantumsinchai recounted in an in-depth journal article examining the mob justice phenomenon. The subreddit “r/findbostonbombers was soon created,” she wrote, “partly fueled by the FBI’s call for information, photos and videos from the public. Whether or not it meant to, r/findbostonbombers became part of a vigilante witch-hunt to find the bombers. As Redditors combed through photos and videos, innocent people were named, shamed and harassed.”

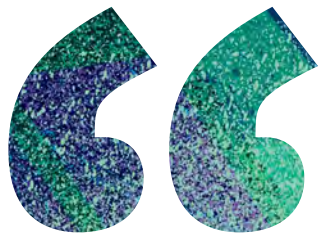
The Redditors eventually fixated on an innocent individual whose name was tweeted and retweeted by high-profile influencers with millions of followers. After authorities apprehended the actual bombers, the Redditors acknowledged their mistake. However, shortly after the debacle, the wrongfully targeted man committed suicide.

Doxxing is a way to carry out an agenda from a distance—almost like sticking pins in a voodoo doll. But instead of magic, the doxxer is relying on a stirred-up crowd to harass, intimidate or otherwise harm the target. When a big game hunter killed Cecil, a lion beloved in his native country, outrage was swift and harsh. The man’s business name, address and phone number were widely publicized, resulting in his business website going down and a flood of negative



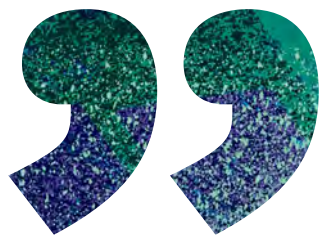
How can cybersecurity professionals guard against it without clarity on what constitutes the threat?





If sensitive information is public by one's own consent... can consent be withdrawn if the information is subsequently appropriated by another actor for the purposes of inflicting reputational damage or emotional/psychological distress? Legally, that's doubtful.

—Jonathan Terrasi, freelance technology and culture journalist



reviews on Yelp. The hunter's home address and phone number reportedly also [circulated on social media](#), along with calls for retribution and outright death threats. He closed his business and [went into hiding](#), according to reports.

While there are many well-known cases of doxxing, there are countless incidents that do not go viral but nevertheless severely impact their targets. "Nearly two decades ago, I took a controversial position against Linux and open source," recalled Enderle. "I was doxxed and people sent me death threats, drove by my house in a threatening manner, and stole and likely killed one of my cats, among other things. Few of those people were coders or even understood the issue. They just became angry and acted."

NEW LAWS, CREATIVE INTERPRETATIONS

Although doxxing may precipitate acts that are clearly illegal, the legality of doxxing itself is muddy.

"If sensitive information is public by one's own consent ... can consent be withdrawn if the information is subsequently appropriated by another actor for the purposes of inflicting reputational damage or emotional/psychological distress? Legally, that's doubtful," observed [Jonathan Terrasi](#), a freelance technology and culture journalist.

The Interstate Doxxing Prevention Act, [introduced](#) in the U.S. House of Representatives in 2016, didn't make it out of subcommittee. However, at least 11 U.S. states have [adopted anti-doxxing laws](#) or modified their existing cyberstalking laws to include doxxing, and several more states are considering new anti-doxxing laws. Existing laws against harassment, identity theft and incitement to violence also might apply.

Unauthorized access of private information could be prosecuted under the Computer Fraud and Abuse Act, said Terrasi. "We've already seen it interpreted creatively ... such as in [United States v. Drew](#) in which it was invoked to prosecute a woman who allegedly engaged in cyberbullying against a teenage girl who subsequently committed suicide."

If doxxing is meant to include "more widely circulating information that is already public, addressing that is a tall order," Terrasi said. "[Smith v. Maryland](#) has been used to establish that social media owns the content you post on it, for example. So, if you try to limit circulation of open information based on ownership, you're going to bump into legal reasoning like that."

PUTTING A LID ON DATA

Public information is low-hanging fruit for doxxers. "The details of someone's mortgage, bankruptcy history, criminal arrest records—all seem pretty sensitive and personal," said Moyle, "and if someone pulls information of that type together in one place and ties it to a person's online presence it can be really intimidating and threatening."

Securing the type of semi-private information people often share on social media sites or online forums is less daunting, he suggested, because users typically can change privacy settings to control who sees what. To make sure truly private information stays private, "it's always good practice to use multifactor authentication and to make sure that you practice good identity protection measures, such as strong passwords that are unique per service," Moyle added.

Hillman drew on the [NIST Cybersecurity Framework](#) as a useful model to apply to the problem, whether at the enterprise or personal level. NIST lays out "processes and cybersecurity practices to identify, protect, detect, respond and recover from any type of cyber event," he noted.

Securing sensitive personal information is not unlike Coca-Cola protecting its formula for making Coke, Hillman continued. "We can take lessons from that. What is the information that could be impactful to me as an individual if it were to become publicly available? Or is

there information that I'm putting out there—open-source public information—that I need to be aware of so that I can detect and respond to it?"

Sometimes there isn't a path to protecting data, but in such cases, a potentially effective approach would be to shift to vendor risk management mode, Hillman suggested. "And then taking that down to a personal level—who are the people that I'm partnering with and giving my information to? Is it to a utility? A government entity, a state agency? Is it going to a charitable organization? Is it going to a nonprofit?" Having a catalog of where sensitive information resides is a proactive first step to controlling access to it.

CYBERSECURITY APPROACHES

Until internet users absorb the necessity of living privately, cybersecurity professionals can apply some of their professional knowledge, skills and tools to the problem. Hillman recommended attack surface monitoring as one useful approach.

"If I was already employed, I could maybe reach out to my current HR to see the background check information that's been most recently returned on me so that I can understand what is my baseline," said Hillman. "If I was unemployed, I would potentially consider running a background check on myself through a service to see what potential employers are going to see about me." The idea is to adapt the same methods used at the enterprise level to personal circumstances, he said.


"Search for your own identity with the same tools an attacker would," suggested Terrasi. "This is the same principle behind the idea of red teaming and penetration testing: Attack the asset exactly as the attacker would, catalog the results and address the shortcomings." He offered the following steps as a general guideline for shoring up personal privacy:

1. **Log out** of all your accounts, clear your browser and enable private browsing.
2. **Look up** your name on major search engines and in the search fields for major social media platforms.
3. **Conduct** background checks on yourself.
4. **Request** government or business records, such as licenses.
5. **Examine** resources, records and pages associated with your current and previous jobs.
6. **Learn** how to use open-source intelligence (OSINT) tools.
7. **Go to** places where you found data on yourself and see if configuration changes or takedown requests can get the information removed.
8. **Take advantage** of "right to be forgotten" features and regulations, if available to you.

NO REST FOR THE DOXXER

For all of the harm doxxing causes to those who are targeted, it can also have severe repercussions for persons accused of carrying it out—especially if they are completely innocent. "This is a case where your best defense is to be able to show your receipts," said Terrasi. "The nature of the internet is such that metadata gets created and logged all the time. ... A skilled digital forensics technician may be able to extract logging data from your mobile device indicating what network connections were open [and] when."

As for those who are guilty of doxxing, Enderle pointed to the consequences that might befall the perpetrator. "When you dox someone, it makes it personal, and the response of the person attacked can be extreme. ... Doxxing is like launching a bomb with poor guidance and high potential for collateral damage into a population center. It is extremely irresponsible and could lead to long-term damage to both the doxxed person and their family, and the person who did the doxxing."



General
guideline for
shoring up
personal
privacy



Although benefits are not quickly realized, education can be a powerful tool.

OWNING THE CYBERSLEUTH DISPOSITION

Although benefits are not quickly realized, education can be a powerful tool. “Very often, people don’t consider how information they put online can be misused against them,” said Moyle. “Cybersecurity practitioners can help point these things out. Likewise, cybersecurity practitioners can help evangelize concepts like strong passwords and multifactor authentication.”

Cybersecurity professionals also might play a role in bringing issues like online harassment, doxxing and bullying to the attention of school administrators, noted Terrasi. “What would happen if digital literacy curricula became a high school graduation requirement, like state civics tests?”

Individuals who are drawn to cybersecurity careers may have certain traits that make them better suited to protect themselves—and their families, friends and organizations—than people outside the profession.

“There’s a certain amount of sleuthing, right?” said Hillman. “You have to be able to think as an attacker would. If you can impersonate those malicious behaviors and simulate them to a certain degree, that will give you the best opportunity to intercept an attack and prevent or mitigate a negative impact. So maybe you have a little bit of savviness that naturally comes from being in this profession.” •

Mick Brady is a freelance writer based in Ventura, Calif.



Detect, investigate and hunt at Google speed

Chronicle, now part of Google Cloud, is a security analytics platform that works at planet-scale. Redefine your SIEM with zero-management security analytics from Chronicle and let us ensure perfect fidelity, no matter how much data you generate.



Modernize your enterprise security with [Chronicle](#).

<https://chronicle.security>





Certified Information
Systems Security Professional

An (ISC)² Certification



Throw Down the **LADDER**

to Tomorrow's Cybersecurity Leaders

There's never been a greater urgency for cybersecurity professionals — yet the dangerous gap in available talent puts us all at risk. The world needs close to 3 million more professionals to meet demand. We need your help.

You've experienced the rewards of a career in cybersecurity. As one of the fastest-growing and most lucrative fields, it opens limitless opportunities for professionals around the globe.

Now it's your time to inspire tomorrow's cybersecurity leaders to get **Certified in CybersecuritySM**. The entry-level certification with no experience requirement starts candidates on their path to advanced certifications and long-term success. Pay it forward.



Certified in
Cybersecurity

An (ISC)² Certification

Share this special limited-time offer:

FREE! Online Self-Paced Course

With the purchase of a Certified in Cybersecurity exam voucher (US \$199). Includes two opportunities to pass the exam.

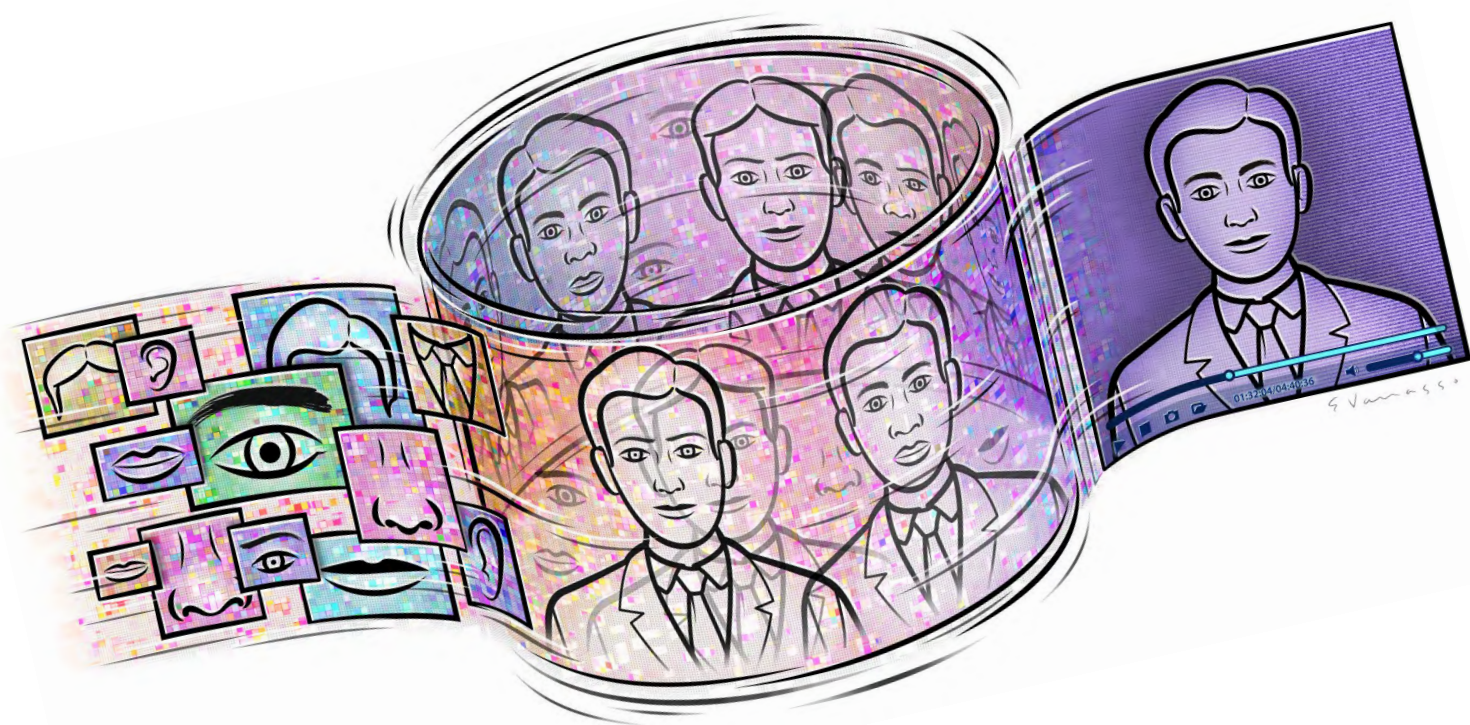
**Spread the word and help close the
cybersecurity workforce gap.**

Download and Share

certifiedincybersecurity.org

SEEING IS **DISBELIEVING**

THE IMPACT OF DEEPPAKES ON TODAY'S CYBERSECURITY BY PAT RARUS



WHEN INTERNATIONAL MOVIE STAR TOM CRUISE appeared in a TikTok video in early 2021, viewers were amused at first, then outraged when they learned that instead of the popular actor, they were watching an AI-crafted imitation known as a deepfake.

While that video was created for parody and removed by Belgian visual effects artist Chris Ume—who insisted that he meant no malice—other deepfake incidents have proven far more troubling, as well as financially devastating.

Scammers stole U.S. \$35 million after using forged email messages and deepfake audio to persuade an employee of a United Arab Emirates company that a senior executive needed the money to fund an acquisition of another business, according to an October 2021 Forbes report via the site [Gizmodo](#).

ILLUSTRATION BY ENRICO VARRASSO

“When you run this simple mechanism with millions and millions of iterations, it will eventually create an image that the discriminator will look at and say, ‘Yep, I can’t tell that this is not a person,’ and now you have it [the deepfake].”

—Hany Farid,
deepfakes expert,
University of
California, Berkeley

“Dubai investigators have revealed that the crooks used deep voice technology to simulate the voice of the director,” the site reported. “Authorities believe that the scheme involved as many as 17 different people and that the stolen cash was funneled to a number of bank accounts scattered throughout the globe.”

In addition to business hoaxes, deepfake technology is increasingly used in romance fraud, where vulnerable singles, usually women, are targeted by scammers. These masters of disguise often steal real people’s identities from the web. In 2019, a California widow was scammed out of nearly U.S. \$300,000 by an unidentified overseas con man who courted her online using a deepfake video to pose as the superintendent of the U.S. Naval Academy, according to federal prosecutors.

Some 96% of deepfake videos involve pornography, often with celebrities’ faces digitally pasted onto the bodies of porn stars, according to *The Guardian*. Deepfakes are also used to impersonate political leaders, including Ukrainian President Volodymyr Zelensky, urging his citizens to surrender to Russia, in late March 2022, according to credible news reports. The following week, another deepfake video depicted Russian President Vladimir Putin supposedly declaring peace in the Ukraine war.

HOW DEEPFAKES ARE MADE

Deepfakes are developed by a generative adversarial network (GAN), a machine-learning model in which two neural networks challenge each other to become more precise in their predictions. The two neural networks that comprise a GAN are called the generator and the discriminator. The generator is a convolutional neural network, and the discriminator is a deconvolution neural network. The objective of the generator is to artificially manufacture outputs that could easily be mistaken for real data. The objective of the discriminator is to identify outputs it receives as artificially created.

When developing a deepfake image, the creator starts at the top of a random image and drops in a bunch of pixels. That image goes into a generator that creates the fake image and then is digitally placed into the discriminator, which has access to real people’s images, including politicians and celebrities. The discriminator determines if it can distinguish the image provided by the generator from the images of real people. If yes, the discriminator goes back to the generator and checks again. The generator makes additional modifications to the pixels, and this process goes back and forth, millions of times in a very tight loop.

“When you run this simple mechanism with millions and millions of iterations, it will eventually create an image that the discriminator will look at and say, ‘Yep, I can’t tell that this is not a person,’ and now you have it [the deepfake],” explained Hany Farid, a deepfakes expert at the University of California, Berkeley, in a keynote at the Spark + AI Summit 2020.

HOW EXPERTS SPOT DEEPFAKES

“We learn the mannerisms and facial tics people have [especially well-known politicians such as former U.S. Presidents Obama and Trump] by looking at hours of video,” said Professor Farid. “We then take all of that information, and we extract 190 measurements and project them onto a two-dimensional space, using basic hide-and-face tracking.” He added that while this technique works very well with high-profile politicians and celebrities whose images dominate the media, it is not so effective for detecting fakes of average people.

To do that, Farid and his UC Berkeley team use a technique of mapping sounds people make—phonemes—and the shape of people’s mouths when they speak—visemes. For example, when words with the consonants “f” and “v” are spoken, such as in the words “favor” or “victor,” the lower lip curves in ever so slightly and the top teeth come down.

“When we create things like lip-sync deepfakes, those mechanisms ... the GAN doesn’t know anything about phonemes or visemes,” Farid said. “All it knows about are pixels and these

classifiers, and so we can leverage that ignorance to determine whether the mouth is making the proper shape to say a particular phoneme.”

HOW CORPORATIONS AND GOVERNMENTS ARE FIGHTING DEEPPAKES

In addition to UC Berkeley’s detection efforts, tech giants are creating their own systems to fight deepfake content. Microsoft, Google, Meta (formerly Facebook), Amazon Web Services and others work with academia and government agencies such as DARPA (the U.S. Defense Advanced Research Projects Agency) to find altered photos and videos. They even create competitions, such as the Deepfake Detection Challenge (DFDC)—spearheaded by Meta in late 2019—offering U.S. \$500,000 in prize money to find new ways of exposing deepfake videos. “[The DFDC has enabled experts from around the world to come together, benchmark their deepfake detection models, try new approaches and learn from each other’s work,](#)” stated a June 2020 posting on Meta AI.

Microsoft uses a multi-modal, multi-stakeholder approach in dealing with deepfakes, according to Ashish Jaiman, the company’s director of product management on the Bing multimedia team.

“We focus on education and awareness, ethics, global policy work and cross-industry collaboration,” he said in a telephone interview. “We are working with RealityDefender.ai [a provider of an enterprise-grade deepfake detection platform] to optimize their solutions to authenticate if the content is real or fake. GANs-based deepfakes can improve themselves and fail detection, which is challenging. We are a founding member of C2PA, or the Coalition for Content Provenance and Authenticity, to find a long-term solution to deepfakes and disinformation.”

“GANs-based deepfakes can improve themselves and fail detection, which is challenging.

—Ashish Jaiman,
director of product
management on the
Bing multimedia team,
Microsoft

WHAT IS THE WORLD DOING ABOUT DEEPPAKES?

In July 2021, the U.S. Senate introduced Bill S2559 to establish the National Deepfake and Digital Provenance Task Force, requiring the Department of Homeland Security to work with the White House Office of Science and Technology Policy to legislate the use of deepfakes. As of this writing, the bill was still in the Senate Homeland Security and Governmental Affairs Committee.

A House of Representatives version of deepfakes legislation—USHR3230—dead-ended in committee in December 2020. Since then, Representative Adam Schiff (D-California), who chairs the House’s Permanent Select Committee on Intelligence, has been actively working on ways to introduce new laws against deepfakes. “[We can and are trying to fund the technology to detect them and detect them quickly, so that when something is put out by, say, an adversary power to influence our elections, we can get good intel on it,](#)” he told a CBS News interviewer in 2021.

However, as *60 Minutes* reporter Bill Whitaker pointed out in that October 10 episode, in general “[deepfakes are considered free speech, and attempts at legislation are all over the map.](#)” For instance, in New York State, commercial use without consent is banned for 40 years after death. California and Texas prohibit deceptive political deepfakes leading up to an election.

The European Parliament and EU member states agreed to pass the Digital Services Act in April. The milestone law mandates that Big Tech companies swiftly clear their platforms of illegal content, including deepfakes, and noncompliance could result in fines of as much as 6% of the companies’ annual global revenue. In the case of Meta, such a fine could reach €6.74 billion based on 2021 sales figures. The law still needs official approval by EU institutions; provided that happens, the new law is expected to go into effect by 2024, [according to an April 2022 CNBC news report.](#)

The APAC region is also deeply concerned about the impact of deepfakes.

In April, Taiwan’s Cabinet approved draft amendments to four vital laws to curtail their use.

POSITIVE ASPECTS OF DEEPPFAKES

DESPITE MOUNTING ANXIETY, fear, frustration and shame about the political, financial and privacy issues involved with deepfakes, positive aspects abound for this ever-evolving, AI-based technology. Applications range from the fun and frivolous with celebrity imitations to vital new approaches in education and healthcare.

Entertainment

For example, after the mafia-based hit movie *The Irishman* aired on Netflix in 2019, a fan-made deepfake video modifying the CGI-generated special effects of veteran actors Robert DeNiro and Al Pacino was called “better than the real thing,” according to a [December 2020 post on the British entertainment website The Independent](#).

Education

To rectify the adverse impact of pandemic-related absences from classrooms around the globe, teachers could use abundant doses of creativity to recapture their students’ interest and attention. To that end, deepfakes can provide educators with interesting subject matter, advancing far beyond conventional visual and media offerings.

“Artificial intelligence-generated synthetic media can bring historical figures to life in the classroom, thus making lessons more engaging and interactive,” [stated a blog post](#) by KnowledgeNile. “With the scale and low cost, the use of synthetic voice and video can also improve success and learning outcomes.”

Healthcare

In healthcare, deepfake technology can be used to blend realistic data to assist researchers in developing new ways of treating diseases without relying on real patient data. In fact, in September 2018, researchers from Nvidia, the Mayo Clinic and the Mass General Brigham Center for Clinical Data Science presented an academic paper on their collaborative efforts of using GANs to create synthetic brain MRI images.

The team trained their GAN on data from two datasets of brain MRIs—one containing approximately 200 brain MRIs showing tumors, the other containing thousands of brain MRIs with Alzheimer’s disease. [According to the researchers, algorithms trained with a combination of “fake” medical images and 10% real images became just as proficient at discovering tumors as algorithms trained only with real images](#), stated an April 2022 blog post by futurist Richard van Hooijdonk.

Because the images are synthetically created, neither patient privacy nor patient data are compromised. In addition, the generated information can easily be shared among medical institutions, allowing for a wide variety of combinations that can be employed to improve and advance their work.

“The team hopes that the model will help scientists generate new data that can be used to detect abnormalities quicker and more accurately,” Hooijdonk noted. •

—P. Rarus

Specifically, the production and proliferation of fake or altered images and videos for financial gain now is a crime punishable by up to seven years’ imprisonment.

The draft legislation was introduced after a Taiwanese social media user was arrested for allegedly developing and profiting from embarrassing deepfake videos involving more than 100 public figures. [“Taiwan is dedicated to making its digital transformation as smooth as possible for its citizens,” stated an April 2022 post on OpenGovAsia](#). “To that end, it’s moving mountains to get rid of possible abuses.”

In Australia, deepfake pornography became a crime in 2019 and is punishable by up to three years’ imprisonment and/or substantial fines. An independent government agency, the eSafety Commissioner, protects Australians from online abuses, including deepfakes. Despite

“There should be government regulation on the use of AI technology for that purpose. ... There continues to be misinformation during the Russian-Ukrainian war. Is that free speech? Not in my opinion.”

—Steven Adegbenle, CCSP

continuing efforts, the challenge remains formidable. According to a January 2022 posting on the agency’s website: “A holistic approach is needed to counter the negative impacts of deepfakes. eSafety leads this approach in Australia, working with industry and users to address the issue.”

VIGILANCE WITH EVERY CLICK

With deepfake AI technology still in its infancy, government, businesses, academia and consumers need to be ever more vigilant and, yes, skeptical of what they view online. Perhaps San Marcos, Calif.-based CCSP Steven Adegbenle said it best in a telephone interview: “I find the rise of deepfake technology very alarming. There should be government regulation on the use of AI technology for that purpose. ... There continues to be misinformation during the Russian-Ukrainian war. Is that free speech? Not in my opinion.”

Futurist Richard van Hooijdonk agrees about the need for vigilance.

“Going forward, in order to minimize deception and curb the undermining of trust, technical experts, journalists and policymakers will play a critical role in speaking out and educating the public about the capabilities and dangers of synthetic media,” he wrote in an [April 2022 blog post](#).

“With increased public awareness, we could learn to limit the negative impact of deepfakes, find ways to co-exist with them and even benefit from them in the future.” •

Pat Rarus is a freelance writer based in Oceanside, Calif.

The advertisement features the Imperva logo and the text "Comprehensive Digital Security". It lists three key capabilities: "Unified cloud-native protection from Edge through Applications to Data", "Automated threat detection and classification across Security, Compliance and Governance", and "Simplified risk management and analytics for IT, Security and DevOps". On the right, a circular diagram shows four layers of security: Network Security, Application Security, Data Security, and Security Automation, all surrounding a central "im" logo.

imperva Comprehensive Digital Security

Unified cloud-native protection
from Edge through Applications to Data

Automated threat detection and classification
across Security, Compliance and Governance

Simplified risk management and analytics
for IT, Security and DevOps

www.imperva.com

Network Security
Application Security
Data Security
Security Automation

im



Certified Cloud
Security Professional
An (ISC)[®] Certification

Answer the Demand for **CLOUD CYBERSECURITY EXPERTS**

Validate your expertise and answer the demand for cloud security experts.

CCSP certification sets you up for success with the knowledge and skills you need to stay on top of emerging trends and technologies in cloud security.

Now is the time to map your strategy and achieve your goals. Download your (ISC)² Exam Action Plan and get started today.

[Get Your Action Plan](#)



CCSP:
*The Top Security Certification
Experts Plan to Earn in 2022*
- Certification Magazine

Commit. Plan. Succeed.



SOCIAL MEDIA CHALLENGES

FOR RISK, HIGH CONCERN, AND CRISIS COMMUNICATION

An excerpt from *Communicating in Risk, Crisis, and High Stress Situations: Evidence-Based Strategies and Practice* (Wiley-IEEE Press, 2021)

BY VINCENT T. COVELLO, PH.D.

Along with its many benefits, the social media revolution also poses unique challenges for risk, high concern, and crisis communicators. The following describe landmines everyone must negotiate, whether they engage through social media or not.

It is hard to refute or recover from a negative story or misinformation posted on a social media site, and even harder to delete the information.

Rising Expectations

Organizations must keep pace with stakeholders' expectations regarding the use of social media. People increasingly demand immediate information. These rising expectations have resulted in an "expectation gap" between organizations and their audiences. It is forcing many organizations to invest internal resources to create an active social media presence.

Repostings/Redistribution

Social media messages are often reposted and redistributed by users in many forms, such as from Twitter and Facebook to YouTube, Instagram, Reddit, TikTok, WhatsApp, and Snapchat. This is a benefit for wide reach but also requires that in the world of digital communication, messages must be crafted with expectations of their reuse.

Every social media message can be repurposed and recontextualized multiple times; the shorter and clearer a message is, with embedded sourcing and time stamping, the less it will deteriorate in meaning through reuse. Critical information posted on a social media platform needs to be time stamped. If a social media post is not time stamped, someone may see that post hours later and share it. This makes the post seem "current" despite the information being hours old and possibly revised. One strategy used by social media professionals to address this issue is to take pictures or screenshots of a media release or a blog post and attach it as an image with a time stamp embedded in the post.

Permanent Storage

Information posted on social media platforms may be stored for as long as there is access to the site on which it was first displayed. It is hard to refute or recover from a negative story or misinformation posted on a social media site, and even harder to delete the information. As a result, risk, high concern, and crisis communicators need to exercise great care before posting content, including vetting by others and testing. Even if a post is deleted, it is likely that screen captures still exist.

Hacking/Security

Social media sites are highly vulnerable to hacking and security breaches, including breaches that insert false or doctored information. Hacking is nearly at epidemic levels. For example, disinformation is widely spread through multiple routes, including false or misleading news stories, *trolls* (people who deliberately post lies on social media platforms), *trick search algorithms* (invisible links to target sites), *cyberbullies* that target specific individuals or groups, and social media *bots* (automated fake users). Message content needs to be protected with state-of-the-art security practices, just as protection is employed for confidential information.

Rise and Fall of Social Media Platforms

Social media platforms rise and fall rapidly. Continual effort is needed to track the growing number of social media platforms and near-constant changes in their popularity and numbers of followers. As a result, risk, high concern, and crisis communicators need to continually evaluate and prioritize social media platforms, calculate resources and time available for social media engagement, and prioritize attention and resources on social media sites used by target audiences.

Resources

Monitoring social media content can be a full-time activity. Substantial resources are needed to share content with stakeholders, let alone interact with them. *Organizations need to prioritize and budget resources carefully.*

Privacy and Confidentiality

Information shared through social media sites often violates privacy standards and expectations of confidentiality. Social media privacy and confidentiality mean the ability to control

Unfortunately, people often believe and share news that confirms their personal beliefs and ignore or discount news that is contrary to their personal beliefs.

(1) interactions with others, and (2) who gathers and disseminates information about oneself or one's group and under what circumstances. Individuals and organizations use multiple techniques to enhance privacy and confidentiality.

In a crisis, it is critical that employees be reminded of the organization's social media policies; that what employees post on their social media platforms becomes part of the public and legal record; that journalists may scan social media sites of employees for information about the crisis; that persons with negative intentions, such as terrorists, may scan the social media postings of employees for insider information; and that prosecutors have used risk-related postings of employees on social media platforms in civil and criminal filings.

Cognitive Overload

Search engines and social media platforms, such as YouTube, provide users [direct access to an unprecedented amount of content about risks and threats](#). However, the proliferation of information from social media sites, and easy access to such information, can also create a [cognitive overload](#).

Cognitive overload occurs when a person's working memory receives more information than it can handle comfortably. As information about risks proliferates through social media, [the brain's processing abilities can create bottlenecks](#), favoring the use of mental shortcuts, information that is the most easily accessed, or information that is consistent with, or conforms to, existing beliefs about susceptibility (i.e. vulnerability to the risk), severity, benefits of protective measures, and barriers to the adoption of protective measures. As a result, information about a risk or threat shared through social media channels is typically more effective when it is presented in tiers, with each tier increasing in content and complexity.

Players on the Field

One of the greatest challenges raised by social media for risk, high concern, and crisis communicators is the much broader range of players that can now share and exchange information about risks, threats, high concern, and emotionally charged issues. This exponential widening of the playing field creates immense opportunities but also immense dangers, including concerns about censorship, monopolies, privacy, biases, disinformation, rumors, and campaigns aimed at defaming, dividing, discrediting, and distracting. Awareness of the complexity of this environment and strategies to monitor the social media environment are important as social media communication plans are developed.

Misinformation, Disinformation, and Rumors

Social media platforms are a breeding ground for *misinformation*—false information spread unintentionally, *disinformation*—false information spread with the intent to do harm, and *rumors*—unverified information that can be true or false. The spread of misinformation, disinformation, and rumors through social media platforms typically becomes greater when there are controversy, confusion, and mistrust.

Fake news—[news that is untrue and disseminated under the guise of news reporting](#)—is a particular problem for both social media and mainstream media outlets. According to the Pew Research Center, approximately two-thirds of all adult [Americans say fake news causes them a great deal of confusion](#). Approximately one-quarter of all adult Americans report they have shared a made-up news story—either knowingly or not. Unfortunately, people often believe and share news that confirms their personal beliefs and ignore or discount news that is contrary to their personal beliefs.

False information can quickly go viral through the internet and social media outlets. Two of the most [egregious examples of false information](#) spread widely initially by Facebook and other social media platforms was the claim that Pope Francis had endorsed the candidacy of Donald Trump in the 2016 U.S. presidential election and the bizarre “pizzagate” story that became viral and led a North Carolina man to bring a gun into a popular Washington, D.C. pizza restaurant

Detecting Fake or Misleading Social Media Content

1. Authenticate the domain site, logo, contact information, and office location.
2. Check the accuracy, date, and source of quotes.
3. Check the publishing date.
4. Check links and references for accuracy.
5. Check the authenticity of photos.
6. Check for the presence of ads for commercial products.
7. Check for headlines that do not reflect facts in the story.
8. Investigate the reputation of the author or posting organization.
9. Check for criticism from reputable sources.

—V. T. Covello

False information was 70% more likely to be retweeted on Twitter than accurate information.

under the impression that the restaurant was hiding a child prostitution ring. As a result of a tsunami of disinformation spread through social media platforms, important sites need to be continually monitored for misinformation, disinformation, and rumors. If found, they need to be addressed immediately.

Content on the organization's website and social media platforms also needs to be regularly updated to prevent speculation. To efficiently respond to social media misinformation and disinformation, managers and communicators need to decide which social media platforms are most important, which platforms exert the most influence on key stakeholders, and which resources (e.g. staff and time) can be devoted to the problem.

Of the challenges described, the spread of false information by social media platforms is perhaps the most serious. *Recommended Best Practices (above)* contains examples of tactics for detecting fake and misleading news.

There is increasing global concern about the proliferation of false or misleading information about risks and high concern issues. To understand better [how quickly false information spreads](#), researchers examined over 126,000 rumors spread by approximately three million people on Twitter from 2006 to 2017. False information reached more people than the truth; lies spread exponentially faster than truth; false information found many more followers than accurate facts. False information was 70% more likely to be retweeted on Twitter than accurate information. False information occurred in virtually all domains, from terrorism and natural disasters to financial information and science.

Public and private sector organizations have mounted efforts to combat the spread of false

What is a Risk, High Concern and Crisis Communicator?

WHEN TASKED WITH conveying information in risky, concerning or full-blown crisis situations, the objectives are to build trust, promote knowledge, and encourage appropriate behaviors and supportive relationships.

As mentioned in *Communicating in Risk, Crisis, and High Stress Situations: Evidence-Based Strategies and Practice*, those tasked with responding to a broad range of situations are referred to as risk, high concern and crisis communicators.

Risk Communications

The functions of risk communication are multi-fold. First it must communicate the probabilities and consequences of known risks to stakeholders. Second, it must communicate to stakeholders the proposals and policies for preventing, avoiding, mitigating, reducing and managing the risk. Third, it should seek consensus among stakeholders regarding a specific course of response and mitigation.

High Concern Communications

A high concern issue is a problem of great interest. It becomes more intense when it has a high consequence (stakes), occurs repeatedly (frequency), has lasted for a significant amount of time (duration), affects many people (scope or range), disrupts personal or community life (disruptive), deprives people of their perceived legal or moral rights (equity) and has negative effects perceived to be serious enough to require attention (severity).

Crisis Communications

Crisis communication can be defined as the exchange of risk information about an abrupt, uncertain, nonroutine and disruptive event that poses immediate and significant consequences. It's important to plan ahead and implement that plan effectively to avoid contradictory messages, refusals to follow recommendations, counterproductive behaviors, loss of trust and social disruption. •

—V. T. Covello

information. Solutions include removing false information from a social media site; labeling false information in much the same way as food is labeled; elevating the search engine ranking of authoritative sites; redirecting advertising money away from social media platforms that spread false information; identifying fake accounts; developing a rumor management/rumor control site to correct misinformation; and suspending or banning social media accounts of people who post false information—recognizing there may be concerns about the trustworthiness of the policing sites.

Effective solutions may have to wait for better evidence-based understanding on issues such as how false information spreads and why people spread false information. •

Vincent T. Covello, Ph.D., is a global leading expert and practitioner on risk, crisis, and high stress communications. Dr. Covello's work has been applied to a wide range of topics including cybersecurity, terrorism, environmental incidents, natural hazards, disease outbreaks, industrial accidents, operational disruptions, organizational changes and much more.



THE
POWER
DUO

CISSP® CCSP®

of Cybersecurity Certifications

CISSP:

The Most Required Security Credential
by Hiring Managers on LinkedIn

CCSP:

The Top Security Certification Experts Plan to Earn
in 2022, Certification Magazine

To learn more, download our Ultimate Guides:

Get the Guide

Get the Guide

(ISC)²

How to Earn Respect and Influence Others

BY MICHAEL HANNA, CISSP

When I think about deepfakes, doxxing and disinformation, one word stands out: influence. Yes, there's also manipulation, coercion or deception. But foundationally, bad actors use these tactics to influence. This made me reflect on how we, as cybersecurity professionals, can influence and manage stakeholders from the board of directors and executives to managers and employees. We can even use influence to dissuade malicious activity.

At the highest level, cybersecurity programs are a concerted effort of policy, process, people and technology. To receive the funding, buy-in and support, there is a "political" environment that security leaders must navigate to promote and achieve their initiatives. Stakeholder management can help, as it is an analysis of the power and interest of a stakeholder. (See Figure 1.) As security leaders, it is important to constantly assess stakeholders by their interest in your project and their power within the organization.

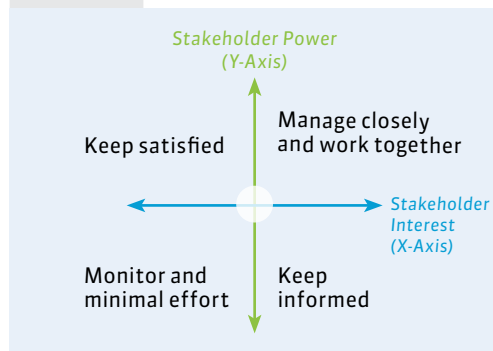
Someone once said, "Leadership is the ability to influence." Our personal ability to influence is critical to any organization and security initiatives. Here are a few ways you may be able to increase your influence:

Make yourself more likable. Being liked does not necessarily make you more influential, but it changes how other people perceive you, listen to you and connect with you. There is a right way and a wrong way to criticize and argue. Certain words, tone and nonverbal cues may create a psychological block when used ineffectively, and your message may fall flat.



Dr. Michael Hanna is a leader and a university professor within the field of information technology and cybersecurity. He specializes in developing high-performing teams, artificial intelligence and cybersecurity. You can reach him on LinkedIn at [Michael Hanna](#). The views expressed here are solely those of the author, and do not necessarily reflect those of the Department of the Navy, Department of Defense or the United States government.

FIGURE 1



Place all stakeholders in the most appropriate quadrant to determine which must be actively managed to promote organizational success.

Put yourself in the other person's frame of mind. People want to feel important and valued. Others care about things *they* treasure most. You must find out what motivates someone and align your value proposition to fulfill that desire. (Think to the last time someone tried to sell you something that you found no value in. What did you do? Probably smiled and nodded without really giving the pitch much thought.)

Continue your personal development. In my last column, I emphasized the importance of coaching and development. I'd like to continue underscoring that message. Improving your influence and use of stakeholder management requires a deliberate personal decision to improve. Keep your skills up to date, continue learning from experts and maybe find the right executive coach.

Take personal stock of your ability to influence. Or better yet, ask a trusted colleague. The next time you start a project, map out your stakeholders and make use of stakeholder management. Then watch as everyone helps *you* achieve project, program and organizational success. ●

CCSP®

Certified Cloud
Security Professional

An (ISC)® Certification

Cloud Security is Evolving—and so is the CCSP

On August 1, 2022, the CCSP domains were refreshed to accurately reflect the most pertinent issues faced by cloud security professionals today. At (ISC)², the rigorous exam update process is fundamental to maintaining the relevancy and integrity of our certifications.

Get the Latest Courseware and Save 20%

Industry-leading education from (ISC)² ensures you're learning the most relevant courseware that aligns to the refreshed version of the exam. For a limited time, save on online training when bundled with an exam voucher.

Training Types



Self-Paced

Online learning at
your own pace



Online

Instructor-Led

Virtual learning with
live instructor

Save 20% Today

