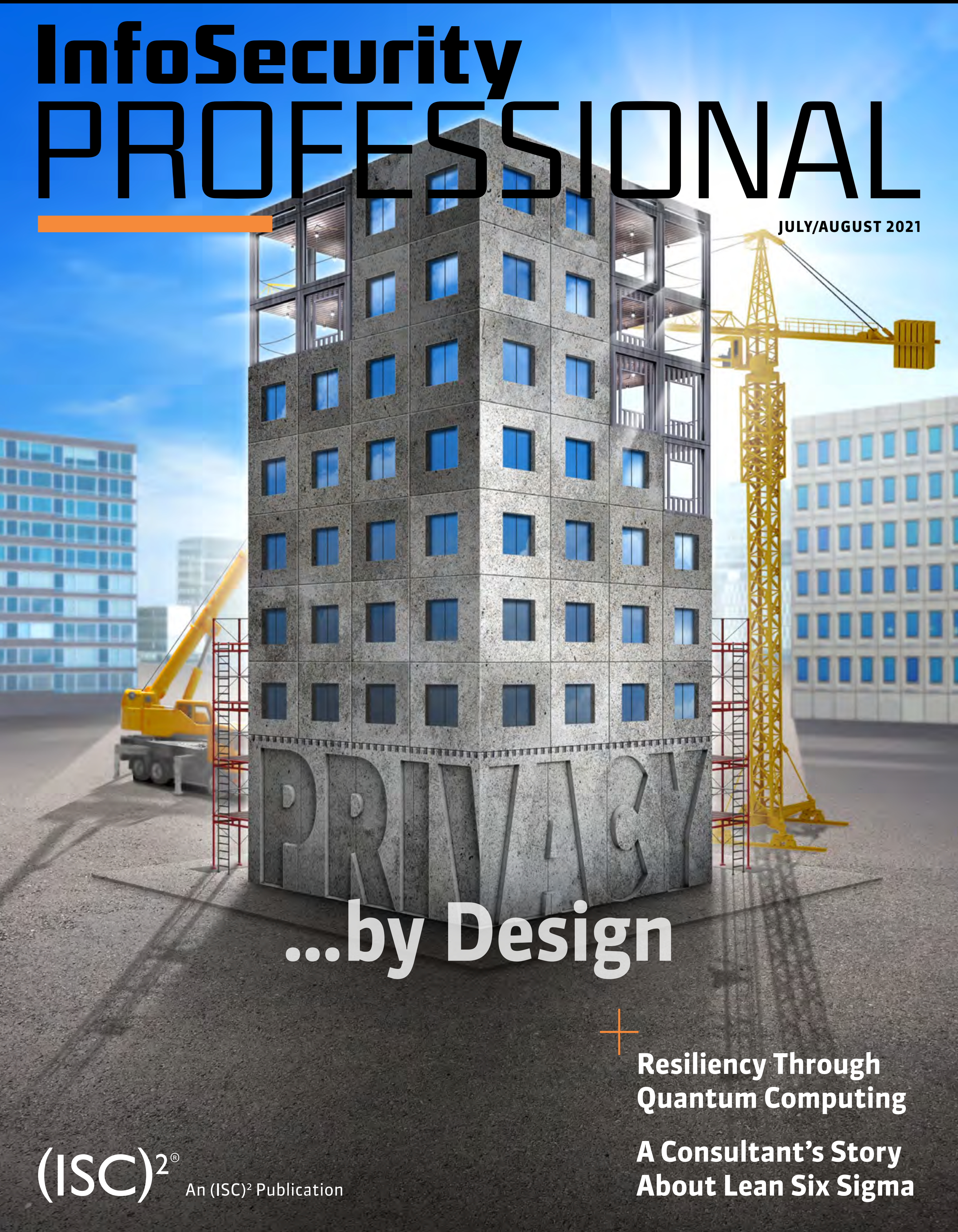
7 WAYS TO STRENGTHEN YOUR BUSINESS REPUTATION

InfoSecurity PROFESSIONAL

JULY/AUGUST 2021



...by Design

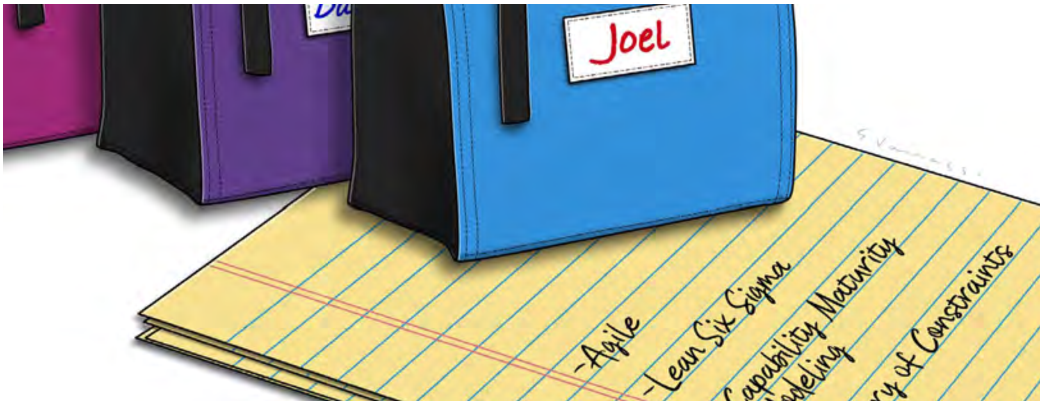
Resiliency Through Quantum Computing

A Consultant's Story About Lean Six Sigma

(ISC)² An (ISC)² Publication

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

CONTENTS ▪ JULY/AUGUST 2021 ▪ VOLUME 14 - ISSUE 4



A cybersecurity consultant breaks down basics for popular business frameworks.

PAGE 31

FEATURES

Cover illustration by Jeff Mangiat

Illustration (above) by Enrico Varrasso

Photo illustration (right) by John Kuczala

DEPARTMENTS

LEARN HOW TO EARN FREE CPE CREDITS

EDITOR'S NOTE

ANNE SAITA EDITOR-IN-CHIEF

Privacy in the Age of COVID

IF YOU'RE SOMEONE WHO thoroughly guards your personal information, chances are you've had to make some sacrifices. For too long, participation on social networks and mobile apps required blanket acceptance that your clicks would be tracked by default and your personal data shared in return for free use.

The EU's General Data Protection Regulation, now into its third year of enforcement, meant to flip the switch and let consumers, not companies, dictate what was—and wasn't—shared. My home state of California did something similar with its own groundbreaking consumer privacy laws to curb Big Tech data practices. Then the pandemic hit, and everything related to consumer privacy was in flux. Sure, you could continue to decline having your cookies tracked or remove apps no longer working as well with more limited data sharing. But now we had a public health crisis in need of data altruists—people willing to share both identifiable and de-identifiable personal health information in order to track COVID-19's spread. We still need accurate data as we respond to global surges and work toward vaccinating enough of Earth's 7.9 billion people to truly turn the tide.

Like all of our features, we keep technical topics accessible so you can share the article within and outside IT circles.

This is a huge task—and topic. (ISC)² member Anita Bateman, CISSP, knew she couldn't include everything related to privacy in her cover story. Instead, she decided to focus on aspects of pandemic life—such as workplace safety and in-person classrooms—through the filter of Privacy by Design. It's a novel approach I think everyone should consider.

It's been several years since we've written about quantum anything, and who better to discuss the cybersecurity pros and cons of quantum computing than Duncan Jones and Mark Jackson, two experts with Cambridge Quantum Computing. Like all of our features, we keep technical topics accessible so you can share the article within and outside IT circles. Finally, it's summer and this issue needs a good tale. In this case, Lloyd Diernisse, CISSP, CCSP, CAP, recalls how he introduced Lean Six Sigma to employees who find such frameworks fleeting. Yes, the concepts are more closely aligned with business operations. But guess what—so is your job now. ●

Photograph by Louise Roup

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

CONTRIBUTORS

Anita J. Bateman, CISSP, tackles our cover story on privacy during COVID-19. A past contributor to the magazine, Anita is an IT executive with experience in technology, utilities, oil & gas and automotive/manufacturing. She also has presented at (ISC)² Security Congress.

Duncan Jones and **Mark Jackson** are ideal for explaining quantum cybersecurity promises and threats. Duncan is head of quantum cybersecurity at Cambridge Quantum Computing. He has 13 years of experience developing security solutions for global companies, with projects ranging from internet-connected hair straighteners to national ID systems. Mark is a quantum evangelist at Cambridge Quantum Computing, with a B.S. in physics and mathematics from Duke University and doctorate in theoretical physics from Columbia University. He spent 10 years researching superstring theory and cosmology, co-authoring almost 40 technical articles, and founded the nonprofit Science Partnership Fund to promote the public understanding of science.

Lloyd Diernisse, CISSP, CCSP, CAP, has a number of titles (and additional credentials), including subject matter expert on strategic risk and cloud security at (ISC)². It's his experiences as a cybersecurity consultant in both public and private sectors that inspired his article on how popular business methodologies do actually work for cybersecurity professionals.

CONTENTS

InfoSecurity
PROFESSIONAL

An (ISC)² Publication

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

isc2.org community.isc2.org

READ. QUIZ. EARN.

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

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

https://www.isc2.org/InfoSecurity-Professional/Magazine-Archive/Quiz/July-August-2021

Learn about more opportunities to earn CPE credits.

ADVERTISER INDEX

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

(ISC)² Security Congress 2021	2
IBM Security	4
(ISC)² Professional Development Institute	6
(ISC)² CCSP: Secure Cloud Migration Starts Here	9
(ISC)² Community	13
San José State University	14
(ISC)² 2021 Cloud Security Report	18
(ISC)² 2021 Cyberthreat Defense Report	20
SEM	30
(ISC)² Commit to Certification – CCSP	37

(ISC)² MANAGEMENT TEAM

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

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

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

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

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

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

TWIRLING TIGER MEDIA MAGAZINE TEAM

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

ART DIRECTOR, PRODUCTION
Maureen Joyce
mjoyce@isc2.org

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

How Battling a Pandemic Mirrors the Challenges of Cybersecurity

BY CLAYTON JONES, MANAGING DIRECTOR, ASIA-PACIFIC, (ISC)²

Many professions have been working on solutions to navigate the COVID-19 pandemic, and there are some parallels to be drawn between the ones who have been able to make progress under incredibly difficult circumstances.

In the medical profession, years of training and commitment put professionals in a position to be able to help patients infected by the virus, including using medical science knowledge to diagnose symptoms and prescribe treatments. Dedicated nurses and doctors ascribe to a code of ethics (to do no harm) for patient welfare and healthcare privacy. They invest in continuous learning about new techniques and therapies because approaches change. In doing so, they were able to come up with creative solutions to change course once they understood how COVID-19 affected people. They have sacrificed much to contend with the virus, even as seemingly endless and continuous waves of infections poured through their hospital waiting rooms.

The same could be said of the scientific and pharmaceutical communities, which utilized established protocols to develop and quickly test vaccine candidates against a particularly novel and nebulous attacker, which spread easily and targeted the human vascular system in a sophisticated way. And yet, against all projections, several working vaccines were developed, tested and brought to market in record time.

Educators also were forced to quickly pivot, master the technical aspects of online learning and reinvent their teaching methods, almost overnight. No two schools anywhere in the world handled this in the exact same way, and many went back and forth between in-school, remote and hybrid learning environments depending on the changing health landscape. There was no lesson plan that could have prepared our teachers for this.

Similarly, in cybersecurity, our dedicated members were hit with an unprecedented challenge as businesses enacted remote work policies and moved their entire staffs off premises. In fact, our 2020 Cybersecurity Workforce Study found that 30% of cybersecurity professionals had one day or less to transition employees to remote work and secure their organizations' newly transformed IT environments. They also had to remain vigilant as new threat vectors emerged, targeting those remote users. Leaning on their knowledge and agility, the cybersecurity workforce pivoted quickly in managing new technologies in remote environments and ensuring businesses remained operational. Even in the most challenging of times, our membership ranks continued to grow, engagement with our professional development education was as high as ever and we saw record attendance at our annual Security Congress. This demonstrates the passion these individuals bring to their careers.

Across all of these professions, resilience has been the key to managing the ongoing crisis. The past 18 months have seen economies globally go through various periods of triumph and loss when dealing with COVID-19. The resilient have been able to fight off a creeping false sense of security, fatigue that would lead them to let their guards down, and varying levels of organizational preparedness around them.

And that's the hard truth. While the pandemic may abate someday soon, vigilance by cybersecurity professionals continues 24x7 because we all recognize that threat actors need to succeed only once, while we need to be successful every time. Continuously adapting, learning and monitoring is key. There is no letting up. ●

Clayton Jones is managing director, Asia-Pacific at (ISC)². He can be reached at cjones@isc2.org.

7 Ways to Enhance Your Business Reputation Through Security

YOUR BUSINESS REPUTATION is key to building communities, establishing partnerships and why others choose your solutions. That reputation, whether you operate as a "solopreneur" or employee, is an external evaluation based on such criteria as direct experience, communications, branding, and/or established thought leadership.

Information security professionals too often leave business reputations up to other departments or employees. However, they play no small role in how that organization's reputation is shaped and evolves.

Here are seven recommendations cybersecurity professionals can do to assist.

1. **Use social media strategically.** In modern social media environments, it is not always possible to control the message; so, be sure to check with your organization's CISO and corporate communications team before responding to a post as part of a corporate information security strategy.
2. **Seek and present third-party validations.** Remember, reputation is not evaluated entirely by communication, history, credentials or awards. It is also based on other parties vouching for your trustworthiness.
3. **Develop strong, consistent messaging.** Uncertainty in communications can introduce doubt and reputation risk, as well as create wariness among customers.
4. **Earn credentials that reflect expertise and high standards.** Associating with institutions and training providers, as well as demonstrating compliance with regional, national and international standards, allows potential partners to expect standard behavior rather than just trusting your goodwill.
5. **Do your own homework.** It is not possible to create trust just by having a third-party validation or time-tested control procedures. Fact- and background-check sources of information to prevent impersonation or unwarranted criticism.

iStock/Getty Images Plus

6. **Seek solid testimonials and referrals.** Recommendations from those with good reputations lend more authority and add weight to your opinion.
7. **Vet your supply chain and service lines.** Where your products rely on third-party providers, ensure that you have confidence in *their* reputation and ability to deliver. Research has shown that when delegating tasks, customers rely on the reputation of the primary partner, but confidence actually comes from the quality of the service.

Business advantages of being in good standing include being able to charge a premium or receive preferential treatment on goods or services, an increase in the number and quality of business contacts, and the prestige of becoming a sought-after reliable business partner.

Duncan Greaves, Ph.D, CISSP, is a U.K.-based cybersecurity researcher and writer with interests in systems architecture, human factors and digital trust. An expanded version of this article appears in the June *Insights* newsletter.

CONTENTS

Global Diversity, Equity and Inclusion Resource Center Opens

The online library of free assets supports DEI programs within teams and organizations

THE (ISC)² COMMUNITY now has a new online resource center to help them audit, build and maintain more diverse, equitable and inclusive teams. The multimedia DEI Resource Center hosts an expanding range of documents, webinars and research to help inform and guide anyone wanting to learn more about these important topics.

Initial assets available on the DEI Resource Center include:

- Glossary of 80 diversity and inclusion definitions you should know
- Guide titled *How to Develop a Strategic Diversity, Equity & Inclusion Plan*
- A toolkit for defining and shifting the DEI business case
- Scholarship opportunities that encourage diverse participation in the field of cybersecurity
- An (ISC)² International Women's Day webinar
- A blog post on tips from women who have built careers in cybersecurity
- "The Power of Side Hustles and Alliances: Finding Your Tribe" 2020 Congress presentation
- Links to relevant videos, podcasts and articles

"Diversity, equity and inclusion are not only moral imperatives for today's organizations to champion; they also help to inspire a safe and secure cyber world by increasing the size of the recruitable workforce that is focused on protecting us from cyber threats. Everyone wins when we expand the tent, welcome more talent in and afford all staff the same opportunities for career advancement," said (ISC)² CEO Clar Rosso.

For more information, please visit https://www.isc2.org/dei. ●

(ISC)² Achieves IAS Accreditation for All 9 Certifications

(ISC)² RECENTLY BECAME the first U.S.-based cybersecurity certification organization to meet the rigorous requirements for International Accreditation Service (IAS) accreditation. The honor increases global recognition and credibility for (ISC)² certification holders and organizations that hire them.

"This achievement brings additional value and recognition to current (ISC)² members who have earned our certifications. It also serves as reassurance for candidates and employers that certifications like the CISSP lead the market in accreditation of international standards and validation of professional excellence," said Dr. Casey Marks, (ISC)²'s chief product officer and vice president.

All nine certifications within the (ISC)² portfolio meet both IAS's AC474 and ISO/IEC Standard 18024:2012. (ISC)² received similar recognition previously from the American National Standards Institute (ANSI), the International Accreditation Forum (IAF), the American Council on Education (ACE), the Australian Computer Society (ACS) and others.

The (ISC)² accredited certifications that are now recognized by the IAS are:

- Certified Information Systems Security Professional – CISSP®
- Systems Security Certified Practitioner – SSCP®
- Certified Cloud Security Professional – CCSP®
- Certified Authorization Professional – CAP®
- Certified Secure Software Lifecycle Professional – CSSLP®
- HealthCare Information Security and Privacy Practitioner – HCISPP®
- Information Systems Security Architecture Professional – CISSP-ISSAP®
- Information Systems Security Engineering Professional – CISSP-ISSEP®
- Information Systems Security Management Professional – CISSP-ISSMP® ●

In late June, (ISC)² announced that it had extended access to its popular Professional Development Institute (PDI) course titled "Ransomware: Identify, Protect, Detect, Recover," to the public for free through July 31. The popular two-hour ransomware course is Quality Matters (QM) approved and covers the major distinctions between ransomware and malware, the key characteristics of ransomware attacks and the protection strategies and remediation plans for ransomware attacks that should be in place ahead of time. ●

CONTENTS

Q&A

HOW I GOT HERE

Getting a Seat at the Table for Women in Cybersecurity

INTERVIEWED BY DEBORAH JOHNSON

How would you characterize today's cybersecurity opportunities for women?

Change, on the scale we are facing with pandemic management, can present new opportunities. 'Work from home' can provide flexibility, space and time to be innovative; however, too much churn and physical isolation can limit effective collaboration, interactions and innovation. Excessive demands while working from home may lead personnel—women, in particular—to drop out of the sector.

What specific challenges do women face?

The gap between required and available talent may be alleviated by adapting and opening the sector to retain and attract a wider talent pool, aiming at those looking for longer-run career stability, higher overall salaries and lower personal risk tolerances. That is a challenge in today's startup environment, which is often less focused on long-run strategic planning and employee retention and satisfaction over time.

There are indications that women, such as in Canada, the U.K. and the U.S., are more vulnerable to being left behind or dismissed if they leave the cybersecurity workforce for any reason. Pandemic management is adding pressures on women, in particular. Combined with ageism, these factors could deter women from choosing the sector (already characterized by intense change, rapid obsolescence and intensive lifelong learning) and negatively affect the availability of female role models and mentors for future cohorts.

As the co-founder of the Security Partners' Forum and the founder of the Women in Security and Resilience Alliance, you clearly see the need for networking. What are some of the significant benefits, especially for women?

Maintaining connection and communication are critical for advancing and thriving in our careers. Seeing and being seen, having a voice and being heard—these will always be central to how we operate as humans. Online tools and platforms can supplement but not substitute fully for in-person human interactions. Having a seat at the table adds dimension and diversity of perspective and experience by identifying and highlighting real women, doing real work, in real careers. ●

BONNIE BUTLIN

Butlin received the 2020 Fellow of (ISC)^2 distinction for her outstanding contributions to the information security profession. With degrees in international affairs and political science as well as being published in cybersecurity journals, she speaks English, French, Spanish and German.

CONTENTS

RECOMMENDED READING

Suggested by **Dr. Richard N. Knepp**, CISSP

The Complete DoD NIST 800-171 Compliance Manual

BY MARK A. RUSSO *(Syber Risk, 2021)*

MARK A RUSSO
CISSP-ISSAP CEH
The Complete DOD NIST 800-171 Compliance Manual
Comprehensive Controlled Unclassified Information (CUI) Marking & Handling Section

The authors of Recommended Reading did not receive financial compensation from the book publishers, nor a free copy of these books. All opinions are the authors' alone.

ON SEPTEMBER 29, 2019, the Department of Defense (DoD) announced the development of the Cybersecurity Maturity Model Certification (CMMC) by amending the Defense Federal Acquisition Regulation Supplement https://www.acq.osd.mil/cmmc/faq.html.

The CMMC is based on the National Institute of Standards and Technology (NIST) 800-171. The DoD is migrating to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB) sector by implementing the appropriate cybersecurity practices and processes to protect federal contract information and controlled unclassified information within their unclassified networks.

The DoD, federal agencies and any contractors that support the DIB will have their 110 cybersecurity controls assessed (CMMC levels 1-3) for the maturity/institutionalization of cybersecurity practices and processes in their company. This book by Mark A. Russo, CISSP-ISSAP, is important to the cybersecurity professional in that it explains and covers these 110 controls, providing some minimum/more complete examples as well as a link to a 250-page cybersecurity policy spreadsheet template for those who purchase the book.

Even if you do not support the DoD, these templates are an excellent resource for any cybersecurity team. ●

RECOMMENDED READING

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

The Handbook of Next-Generation Emergency Services

BY BARBARA KEMP AND BART LOVETT *(Artech House, 2021)*

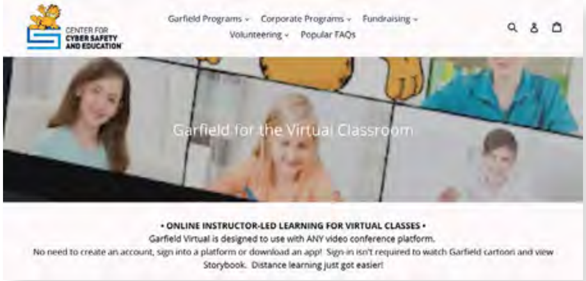
TRADITIONAL 911 EMERGENCY assistance could soon be moving from the telephone to the secure Internet Protocol system and is outlined in *The Handbook of Next-Generation Emergency Services*. The next generation is the use of NG911, which includes the use of a secure Internet Protocol system containing hardware, software, and supporting policies and procedures.

Authors Barbara Kemp and Bart Lovett review the historical and technological changes in emergency services and present the challenges to designing and implementing a next-generation emergency services system. There is insight into planning and funding, project management, infrastructure—the many elements needed in such a major change. The authors explain the legal and regulatory requirements that vary state by state, and the types of agreements that are required (e.g., Open Settlement Protocol [OSP] interconnection). And while there is reference to the security and privacy challenges ahead, hopefully there will be more on the subject in a subsequent volume.

The Handbook of Next-Generation Emergency Services is an excellent foundation for NG911 for security and privacy professionals to consider. ●

CHAPTER SPOTLIGHT

Hawaii Chapter Brings Garfield Lessons to 1,300 Schoolchildren



• ONLINE INSTRUCTOR-LED LEARNING FOR VIRTUAL CLASSES •
Garfield Virtual is designed to use with ANY video conference platform.
No need to create an account, sign into a platform or download an app! Sign-in isn't required to watch Garfield cartoon and view Storybook. Distance learning just got easier!

THANKS TO A GIFT from the (ISC)² Hawaii Chapter, 1,300 elementary school children at the Leilehua Complex received *Garfield's Cyber Safety Adventures* lessons. The online instructor-led program promotes digital citizenship through interactive storybooks, online class discussions and engaging Garfield cartoons.

The lessons are in line with Hawaii's push for computer science instruction and, more locally, with the Leilehua Complex's goal of integrating digital citizenship into academic programs so students and their families stay safe online.

"Having Garfield, an established cartoon character, cross the threshold from simply a lasagna-loving feline to advocate for cybersecurity, helped draw interest from teachers and students while helping demystify cybersecurity as something only 'techie people' can teach," said Chapter President Lito Alvarez.

He said the lessons were timed to be held prior to the school district's spring break, so students had the tools to safely navigate online while on vacation. This made timing among the Chapter's biggest challenges in presenting specific lessons within the three-volume series.

"We were given a limited window for access to Volume 2. During that window, we had to schedule a teacher training, allow teachers to familiarize themselves with the materials and timeline after their training, then leave a window of time for the teachers to do the lesson with their students," Alvarez explained. "Perhaps this school year is the anomaly with scheduling, but the teachers struggled with finding a good time to implement."

That said, both Chapter participants and the Center for Cyber Safety and Education behind *Garfield's Cyber Safety Adventures* were delighted that so many children and their families received cyber safety training.

"This resource also helps us entice teachers to learn more about cybersecurity (and computer science) as it makes the content user-friendly. With today's heavy reliance on technology and online navigation, digital citizenship is a top priority," said Jenny Yamamoto, Leilehua High School librarian, and Grant Toyooka, resource manager, at the Leilehua Complex. ●

(ISC)²'s Global Chapters Connect Members at the Local Level

140+ Chapters

50+ Countries

32,000+ Members

(ISC)² chapters support their members by building a local network of peers who share knowledge, exchange resources and collaborate on projects.

The (ISC)² Chapter Program opens the door for you to participate in local events and activities that connect like-minded individuals with networking and career opportunities, educate members on the latest trends, new technologies and preparing for (ISC)² certification, inspire the next generation of cybersecurity professionals, and secure the community by generating awareness about cybersecurity and empowering individuals to protect themselves online. Locate, join or start a chapter near you. ●

CONTENTS

(ISC)² Career Study: Look Beyond 'All Stars' When Hiring

(ISC)² | The Cybersecurity Career Pursuers Study
BUILD
RESILIENT
CYBERSECURITY TEAMS
Stop Chasing 'All Stars' for Short-Term Gain and Develop Your Team for Years of Success

NEXT TIME THERE'S a job opening on your cybersecurity team, don't automatically overlook internal or entry-level candidates with less experience in pursuit of someone with impeccable credentials and technical chops. There are far fewer "all stars" to go around, and all the time you spend searching for these standouts could be better spent building out a deep security bench for long-term success.

That's among the key takeaways of unique research (ISC)² recently conducted with 2,034 established cybersecurity professionals and cybersecurity jobseekers in the United States and Canada.

Among the key findings:

- Just 51% of current cybersecurity professionals have degrees in computer and information services. Less than half (42%) of professional respondents believed a dedicated security education is critical to working in the field.
- By a wide margin, fewer professionals who are relatively new to the field (less than three years) consider IT experience to be critical (46%) than do their more senior colleagues (69%).
- Military veterans and those with law enforcement experience made up 31% of the cybersecurity professional respondents.
- Cloud security was rated by both professionals and career pursuers as the most important technical skill new entrants to the field should learn, while problem solving was the top-rated "soft skill" they should have.

"Many organizations still default to job descriptions that rely on cybersecurity 'all stars' who can do it all. The reality is that there are not enough of those individuals to go around, and the smart bet is to hire and invest in people with an ability to learn … who can be a catalyst for robust, resilient teams for years to come," said Clar Rosso, CEO of (ISC)², in a prepared statement.

Download a copy of the report here. ●

(ISC)² Earns Industry Kudos for Certs, Magazine

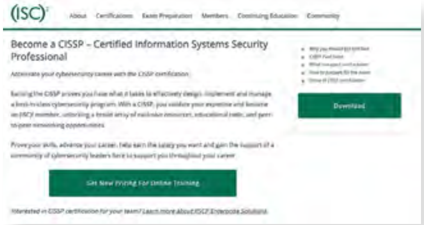
BOTH (ISC)² and its membership magazine recently received top honors in various competitive programs.

The CISSP certification won the Excellence Award for Best Professional Certification Program at the 2021 SC Awards announced online in May. "Any recognition of the CISSP is really a credit to our members who uphold its values and credibility through the great work they do every day to inspire a safe and secure cyber world," said Zachary Tudor, chairperson, (ISC)² Board of Directors, in a prepared statement.

Winners in the Excellence Award category were selected by a panel of IT security experts from both the private and public sectors. During the judging process, each finalist went through a rigorous evaluation that included in-depth analysis, analyst reports and/or product reviews.

InfoSecurity Professional also received national recognition in two separate industry awards programs. The 2020 series on security awareness training featuring a fictitious company earned a National Silver Award from the American Society of Business Publication Editors. It previously earned a Silver Award in the Feature Series category at the ASBPE's regional contest.

The November/December 2020 issue earned a Bronze EXCEL Award for Cover - Manipulated Media from the AM&P Network Associations Council. ●



(ISC)²

About Certifications Exam Preparation Members Continuing Education Community

Become a CISSP – Certified Information Systems Security Professional

Accelerate your cybersecurity career with the CISSP certification.

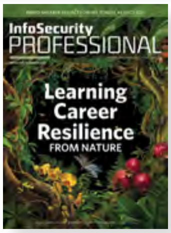
Earning the CISSP proves you have what it takes to effectively design, implement and manage a best-in-class cybersecurity program. With a CISSP, you validate your expertise and become an (ISC)² member, unlocking a broad array of exclusive resources, educational tools, and peer-to-peer networking opportunities.

Prove your skills, advance your career, help earn the salary you want and gain the support of a community of cybersecurity leaders here to support you throughout your career.

Get New Pricing For Online Training

Interested in CISSP certification for your team? Learn more about (ISC)² Enterprise Solutions.

- Why you should get certified
- CISSP Fact Sheet
- What to expect on the exam
- How to prepare for the exam
- [illegible]



MEMBER'S CORNER

WHY WE'RE STILL SEARCHING FOR 'THE FINISH LINE'

BY BARRY DOWELL, CISSP, AND MELISSA BISCHOPING

TOO OFTEN STAKEHOLDERS in and outside of IT fail to understand that when it comes to cybersecurity, they cannot apply old thinking to new solutions. Take the find-fix-finish approach that reinforces a misconception that IT security has a finish line. Most experienced industry professionals would counter that rather than a finish line, we at best reach temporary lulls between major threats.

One of the best comments made during a recent peer-to-peer discussion on this topic was: "Security isn't a noun, it's a verb." All the best tools in the world are not capable of "set it and forget it," and no tool fixes bad policy or stakeholder ambivalence to emerging threats.

Security is about layers; it's about always striving to be just a little better than the day before. It's about implementing needed changes that keep the business operational and continuing to increase protections around company data. As the business introduces new processes or technology, the existing security controls and methods need to adapt. By the very nature that business does not stay static (if it does, it likely doesn't last that long), security cannot be static either.

Similarly, let's remember compliance does not equal security. You can be compliant with all applicable regulations and standards yet still not be secure. Far too often, companies spend time and money on compliance, while neglecting the essential aspects of security fundamentals: accurate IT hygiene and asset management; proactive vulnerability remediation and patching; and attack surface reduction.

Unfortunately, many stakeholders tend to focus on compliance because the steep fines and lost business for noncompliance impact the bottom line. The true holes in security are not seen as having a financial impetus … until a breach occurs, and then the business demands to know how this happened when the auditors had checked all of the boxes on the forms last quarter. Mistaking true security for compliance today is borrowing against a financial and reputation cost that will one day come due.

Cybersecurity and the methods to secure an IT environment are moving targets. Stand still for too long and you'll actually move backward, losing whatever precious gains you'd previously made.

Mistaking true security for compliance today is borrowing against a financial and reputation cost that will one day come due.

Vendors want us to believe that if we purchase their "magic beans" all cybersecurity issues will be resolved. That is never really the case. Implementing the latest security product of the day may not be that useful. You can, hopefully, be more secure than others who may fall victim to data breaches more easily, but it doesn't mean you can do it once and forget about being active in the future.

During that earlier talk among colleagues, some recommended resources such as the CIS controls list. They also suggested that in order to get proper attention from management, you need to start with a discussion of what the company has of value: its reputation, data, and anything else negatively impacted by an IT security incident.

Given the financial impact of breaches that have been in the news over the last few years, this should hit home, though budget-constrained IT support departments may still find themselves losing the budget battle. ●

Barry Dowell is a CISSP, and **Melissa Bischoping** is pursuing an M.S. in Information Security Engineering through SANS Technology Institute. They work together in the IT security industry for the same company.

When's the Right Time to Turn to a Recruiter?

BY DEBORAH JOHNSON

You've searched the job boards, put the word out on social media, reached out to friends, colleagues, mentors. But you still haven't found the right person for a key role on your staff. Is it time to turn to a recruiter?

"You have to look at your capabilities to find talent from a cost versus time point of view," advises Jared Wagner, senior talent acquisition manager at Kansas-based DEG Digital. "If it's going to take too much time to find a certain specialized individual, it might behoove you [and] save you money in the long run to have a relationship with a recruitment firm."

Know that that relationship comes at a cost. According to Recruiters Lineup, an online platform of 10,000 recruiters and agencies, as well as a review of other recruiter websites, the average fee for a successful recruitment is 25% of the employee's annual salary. There are other, less expensive options to consider, such as resume-scanning services. But, again, weigh the investment.

Know the recruiter

Before you sign with a recruiter, make sure they understand your company. Be specific about what skills you need.

"If you are building your database and you are building excitement around a certain pool of candidates, let's say Microsoft Dynamics, you want to find a recruiter or recruitment firm that is only doing Microsoft Dynamics or maybe one or two proficiencies," Wagner advises.

The recruiter should take a deep dive into your company and learn everything they can, advises veteran recruiter Andrew Stoe in a blog post for First Round Review. "You want them to be as invested in the company as possible, because when they message that out to people that enthusiasm will come through."

It is also critical that the recruiter understands your company's culture. In a 2017 survey of 2,100 managers and staff by Hays, a global recruiting firm, 21.8% of IT respondents said a positive company culture is important, second only to salary.

Knowing as much as possible about the recruiter's methods and track record, combined with their deep understanding of your organization and its needs, will help you land candidates you want.

"If you have clarity" on your organization's core values, says Glenn Gutek, founder and CEO of Florida-based Awake Consulting, "then an important conversation you want revolves around 'Do the values of this consulting firm resonate with the core values of our business?'"

Caveat emptor

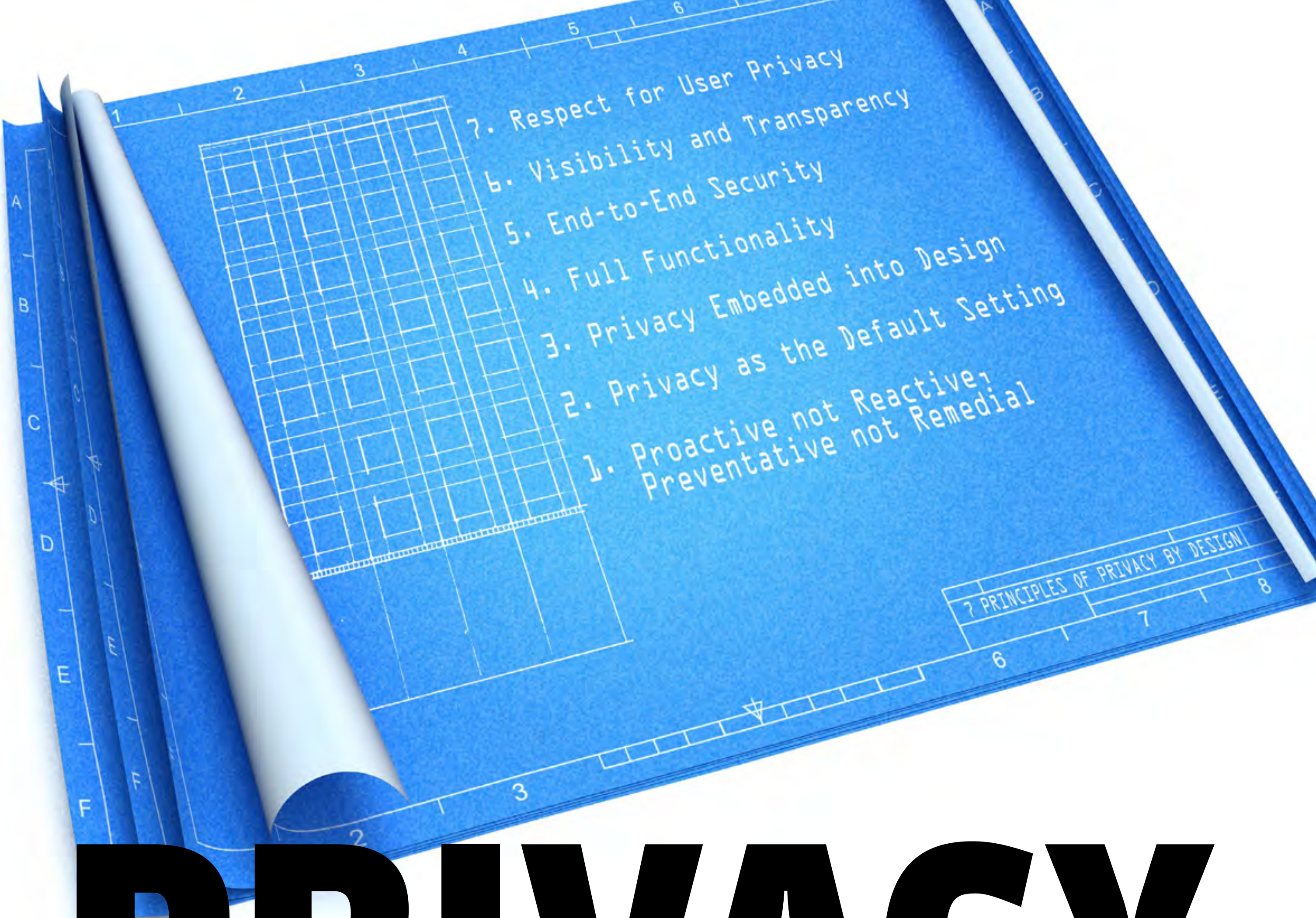
Knowing as much as possible about the recruiter's methods and track record, combined with their deep understanding of your organization and its needs, will help you land candidates you want.

But beware of the glib recruiter, warns DEG's Wagner. "There's a sales pitch that happens in the recruitment world. 'Yup, we can find that person. We know exactly what we're doing. We've staffed for this before.' If you engage someone who does just generalized IT, you're going to start from the bottom at some level." ●

Photograph by Louise Roup

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

CONTENTS


7. Respect for User Privacy
6. Visibility and Transparency
5. End-to-End Security
4. Full Functionality
3. Privacy Embedded into Design
2. Privacy as the Default Setting
1. Proactive not Reactive; Preventative not Remedial
7 PRINCIPLES OF PRIVACY BY DESIGN

PRIVACY *by design*

The Canadian-born concept provides a plan for negotiating a post-pandemic world

BY ANITA J. BATEMAN, CISSP

ILLUSTRATION BY JEFF MANGIAT

DATA PRIVACY is always a hot topic, but the pandemic turned that heat up tenfold.

How do we protect cloud-based personal health data on mobile apps critical to public health initiatives? Are vaccination passports the new frontier for fraudsters and identity thieves? Are remote employees maintaining safeguards for secure home networks now that hybrid workforces are emerging? And what about supply chains, biometrics, data privacy regulations and surveillance drones?

With so many privacy issues and players to track in an ever-changing threat landscape, where do we focus our efforts and attention? How do we maintain the calm minds and singular focus required of us as cybersecurity professionals, both now and when COVID-19 eventually loses its global grip?

I have a recommendation: Follow the principles of Privacy by Design.

7 PRINCIPLES OF PRIVACY BY DESIGN

1. Proactive not Reactive, Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality
5. End-to-End Security
6. Visibility and Transparency
7. Respect for User Privacy

Initially pioneered by Dr. Ann Cavoukian, Privacy by Design gives us a solid footing to meet pandemic challenges and provide cyber-secure and privacy-protected solutions. As a reminder, Privacy by Design was formalized in 1995 and published in 2009. It's included in the EU General Data Protection Regulation, better known as GDPR. And, while not explicitly included in the California Consumer Privacy Act (CCPA), Privacy by Design is integrated into newer legislation Californians passed in November 2020 to close CCPA loopholes.

The main tenet of Dr. Cavoukian's approach is: "Privacy must be incorporated into networked data systems and technologies by default."

She broke down her concept into seven principles that should be familiar to every (ISC)² member. They also should be followed, as they apply to fundamentals we've all learned from both education and experience. These Privacy by Design principles can help you to think through this and validate where your focus is needed. *(See p. 25 for a detailed version of "7 Principles of Privacy by Design.")*

We can start by reviewing our pandemic privacy point of view, both personally and professionally, and define our organization's point of view. Let's take a closer look at six scenarios and how the Privacy by Design principles can be applied.

SCENARIO 1: Identifying infected individuals during a pandemic

Key Principles Applied: Being Proactive, Not Reactive and Embedding Privacy in Design

Dr. Alexys Carlton wrote in March 2020 on towardsdatascience.com about privacy risks in tools where sick individuals are identifiable, looking back at the 2013-2016 Ebola epidemic and our new realities with COVID-19. Considering how these tools could cause physical harm, financial harm, emotional harm and unwanted solicitations, Dr. Carlton presents a clear list of suggestions for COVID-19 tool designers to consider that align with most of the Privacy by Design principles, especially being proactive, not reactive and embedding privacy in design. Her suggestions include:

- Use anonymous data
- Limit access rights
- Include a privacy notice
- Validate the data
- Follow legal requirements
- Get advice

SCENARIO 2: COVID-19 contact tracing mobile apps

Key Principles Applied: Privacy as the Default Setting and Visibility and Transparency

Data privacy presents a major challenge with newly developed COVID-19 mobile applications, most of which are focused on contact tracing to contain the spread of the virus. A July 2020 *Harvard Business Review* report indicates contact tracing apps require a minimum 60% adoption rate to work as intended, and privacy concerns often limit effectiveness and prevent user adoption.

Numerous private and government contact tracing app initiatives have run into these challenges. The debate about whether contact tracing should be decentralized vs. centralized continues—raising issues of risk, ethics, effectiveness and privacy. We need to consider how we can maintain privacy as the default setting and achieve greater visibility and transparency to gain public trust and adoption.

CONTENTS

SCENARIO 3: Remote learning with always-on video cameras

Key Principle Applied: Keeping Design User-centric

Remote learning with video technology continues to be a reality for many schoolchildren. Even where on-campus classes resume, many families elect to continue with online courses due to fear of coronavirus infections or work schedules.

A *Wall Street Journal* article in February 2021 discussed the privacy challenges and emotional hurdles with requiring students to keep their video cameras turned on. "Districts were hesitant to make cameras a requirement in the fall, out of respect for family privacy," the article explains. "Besides increasing anxiety for some kids, the live look into students' living quarters—not only by teachers, but also by fellow students—might pose equity issues."

Some school districts held focus groups to understand camera usage concerns, which ranged from self-consciousness to internet bandwidth consumption in the home. By implementing a waiver process with a mandated camera use policy, a Boston school district achieved higher video usage rates and had more positive feedback overall from students, parents and teachers.

By engaging their students and families, they were able to respect user privacy in program design.

SCENARIO 4: Privacy and pandemic impacts for employers

Key Principles Applied: Privacy embedded into design, Full Functionality and Full Lifecycle Protection

Employers continue to work toward safe in-person work. Challenges include collecting new employee health data (e.g., daily health checks, temperature monitoring, etc.); scheduling employee COVID-19 testing when an exposure occurs; navigating isolation/quarantine scenarios; and supporting their employees in the case of a death. According to a 2021 privacy study by Cisco Systems, "Privacy budgets doubled in 2020 to an average of U.S. $2.4 million."

An October 2020 report from Ernst & Young provides five strategies to tailor Privacy by Design principles to corporate situations and drive organization-wide embrace of Privacy by Design thinking. "The reaffirmation of privacy's value even during the pandemic positions it as a priority for years to come," its authors wrote. "Privacy is no longer an afterthought; it is core to how we work and interact with each other. The Age of Privacy has arrived."

Among the report's recommendations: Be as transparent as possible and give users more control over data sharing than they've had historically.

By implementing a waiver process with a mandated camera use policy, a Boston school district achieved higher video usage rates and had more positive feedback overall from students, parents and teachers.

SCENARIO 5: Taking a swipe at digital wallets

Key Principle Applied: Requiring no action by the individual to protect their privacy

The pandemic increased the use of digital wallets (due to contactless payment preferences), but further adoption may be hindered by a lack of consumer confidence, regional vendor support or mobile app usability.

"Some 46% of people surveyed by S&P Global's 451 Research said the pandemic prompted them to use mobile wallets and other contactless payments more often or for the first time in-store," according to the *Wall Street Journal*.

However, usage is expected to taper, according to another *Wall Street Journal* piece. "A recent study by Visa Inc. found that 24% of U.S. consumers said they would resume their old payment methods after a vaccine is widely available."

Some vendors are paying more attention to the Privacy by Design principles. For example, Google Pay is designed with these principles in mind—specifically, integrations with Gmail and photos are off by default. That's a start; however, unless vendors earn broader consumer trust and adopt other Privacy by Design principles, digital wallet technology will maintain a niche user base rather than reach mass appeal.

SCENARIO 6: Vaccine passports … data privacy is central to getting this right

Key Principle Applied: Embed privacy into product design

The debate on privacy and vaccine passports seems to involve everyone: private citizens, corporate giants and government leaders. By the time of publication, I expect this debate to still be very active. There are some interesting efforts in this area aligned with Privacy by Design thinking.

The Good Health Pass Collaborative is a global consortium of cross-industry and government organizations to "develop a blueprint of privacy-protecting, user-controlled, globally interoperable, and universally accepted digital health pass systems." Privacy by Design is central to this initiative.

Four major challenges exist, including creating the standards, protecting sensitive health data in a way that meets the highest data privacy requirements in the world, proving authenticity (e.g., matching the person to the credential), and creating a universal user experience to drive broad acceptance. This translates to implementing Privacy by Design by default from the beginning.

While global vaccine passports could be helpful to open up travel, other uses and abuses are already in play, including a new cybercrime threat vector of fake vaccination cards.

New Zealand's Office of the Privacy Commissioner weighed in on this in an April 2021 article highlighting the dangers of long-term solutions and misuse of the data, and advocating for Privacy by Design principles, limited necessity/proportionality, and data retention/safe deletion guidelines. Embedding privacy into design is key to these initiatives. IATA's (International Air Transport Association) Travel Pass, CLEAR's Health Pass, Israel's "green passport" and the EU proposal for a "digital green passport" are just a few of the other efforts underway in this space.

In early 2021, the Ada Lovelace Institute concluded, "Vaccine or immunity passports may well play a major role in the world's economic recovery. We need to ensure that as we develop these systems, privacy is not sacrificed at the altar of expediency."

7 PRINCIPLES OF PRIVACY BY DESIGN

Privacy by Design was introduced in the mid-1990s by Dr. Ann Cavoukian, who around that time was named Information and Privacy Commissioner of Ontario, Canada. It took more than a decade, and assistance from a Canadian-Dutch team, for the systems-oriented concept to catch on. Since 2017, Cavoukian has been the Distinguished Expert-in-Residence at the Ryerson Privacy by Design Centre of Excellence.

Here are the seven, broad foundational requirements for Privacy by Design to work as intended:

1. **Proactive not Reactive, Preventative not Remedial.** Privacy by Design comes before the fact, not after.
2. **Privacy as the Default Setting (or "Privacy by Default").** No action is required on the part of the individual to protect their privacy—it is built into the system, by default.
3. **Privacy Embedded into Design.** Privacy is integral and not bolted on.
4. **Full Functionality**. Positive-Sum, not Zero-Sum. Not Privacy vs. Security, but Privacy and Security is possible.
5. **End-to-End Security – Full Lifecycle Protection.** Secure lifecycle management of information from cradle to grave.
6. **Visibility and Transparency – Keep it Open.** Trust, but verify.
7. **Respect for User Privacy.** Keep it user-centric.

COMING UP WITH BEST PRACTICES

There are more privacy/pandemic topics to consider than we have time or space for here. Many states and some countries have passed or are introducing new data privacy legislation, following in the footsteps of GDPR and CCPA. With so many concerns, it's no wonder many of us feel overwhelmed right now. How do we wrap our heads around this space that is changing so rapidly and is so important for our world and global citizens to get right?

Let's go back to our fundamentals and ensure we are building Privacy by Design principles into our initiatives. Within each of our organizations, we need to align with leadership, consult legal and human resources teams, and stay up-to-date on relevant legislation. If you are in healthcare or government, consider how you might participate in the new initiatives focused on privacy protection.

The most recent Cisco privacy study concluded with "Privacy is much more than just a compliance obligation, it's a fundamental human right and business imperative." If we agree with this, we can all look to do our part and leverage fundamental tools, like the Privacy by Design principles, as our compass to help guide our path and set a roadmap for a privacy protecting and secure future.

The great basketball player Michael Jordan once said, "Get the fundamentals down and the level of everything you do will rise." We could all learn from the sports legend when it comes to reinforcing the basics that Privacy by Design promotes, especially as uncertain times continue to unfold. We may be nearing, or already in, a less restrictive phase of COVID-19 in some parts of the world, but its impact on data privacy will be felt for years to come. ●

ANITA J. BATEMAN, CISSP, works in Ohio in the automotive manufacturing industry. Her last article for *InfoSecurity Professional* was on clearing out IT "junk" for the September/October 2020 issue.

ADDITIONAL RESOURCES

Here are some additional data privacy resources to help cybersecurity professionals incorporate Privacy by Design fundamentals into their workflows.

1. M. Hatamian, "Engineering Privacy in Smartphone Apps: A Technical Guideline Catalog for App Developers," in *IEEE Access*, vol. 8, pp. 35429-35445, 2020, doi: 10.1109/ACCESS.2020.2974911.

2. "Tackling Privacy by Design: Practical Advice Following Multiple Implementations," by Mark G. McCreary, *CPO Magazine*, May 21, 2020. https://www.cpomagazine.com/data-privacy/tackling-privacy-by-design-practical-advice-following-multiple-implementations/

3. C. Pandit, H. Kothari and C. Neuman, "Privacy in time of a pandemic," 2020 13th CMI Conference on Cybersecurity and Privacy (CMI) - Digital Transformation - Potentials and Challenges (51275), Copenhagen, Denmark, 2020, pp. 1-6, doi: 10.1109/CMI51275.2020.9322737.

4. "GPA [Global Privacy Assembly] Executive Committee joint statement on the use of health data for domestic or international travel purposes," March 31, 2021. https://globalprivacyassembly.org/gpa-executive-committee-joint-statement-on-the-use-of-health-data-for-domestic-or-international-travel-purposes/

5. "6 things to watch for in the US privacy law debate," by Kirk Nahra, CIPP/US, IAPP, April 1, 2021. https://iapp.org/news/a/six-things-you-should-be-watching-in-the-national-privacy-law-debate/

6. "International Cybersecurity and Data Privacy Outlook and Review 2021," prepared by Ahmed Baladi, Alexander Southwell, Alejandro Guerrero, Vera Lukic and Clémence Pugnet, February 1, 2021. https://www.gibsondunn.com/international-cybersecurity-and-data-privacy-outlook-and-review-2021/

7. "Seven privacy megatrends: A roadmap to 2030." https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/seven-privacy-megatrends.html

8. "Privacy, security, and public health in a pandemic year," by Daniel Mikkelsen, Henning Soller, and Malin Strandell-Jansson, June 15, 2020. https://www.mckinsey.com/business-functions/risk/our-insights/privacy-security-and-public-health-in-a-pandemic-year

9. "Data Privacy During Pandemics: A scorecard approach for evaluating the privacy implications of COVID-19 mobile phone surveillance programs," by Benjamin Boudreaux, Matthew A. DeNardo, Sarah W. Denton, Ricardo Sanchez, Katie Feistel, and Hardika Davalani, 2020 RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA365-1/RAND_RRA365-1.pdf

10. "Privacy in a Global Pandemic: Analysis of COVID-19 Guidance by Data Protection Authorities," by Romain Perray and Mark E. Schreiber, March 23, 2020, the *National Law Review*. https://www.natlawreview.com/article/privacy-global-pandemic-analysis-covid-19-guidance-data-protection-authorities

11. "Personal Health vs. Data Privacy During and After a Global Pandemic," by Axel Wirth, September 17, 2020, *Journal of AHIMA* [American Health Information Management Association]. https://journal.ahima.org/personal-health-vs-data-privacy-during-and-after-a-global-pandemic/

12. "Privacy During a Pandemic," by Muhammad Asif Qureshi, CISA, CIA, CISSP, CCISO, PMP, December 18, 2020, ISACA. https://www.isaca.org/resources/news-and-trends/industry-news/2020/privacy-during-a-pandemic

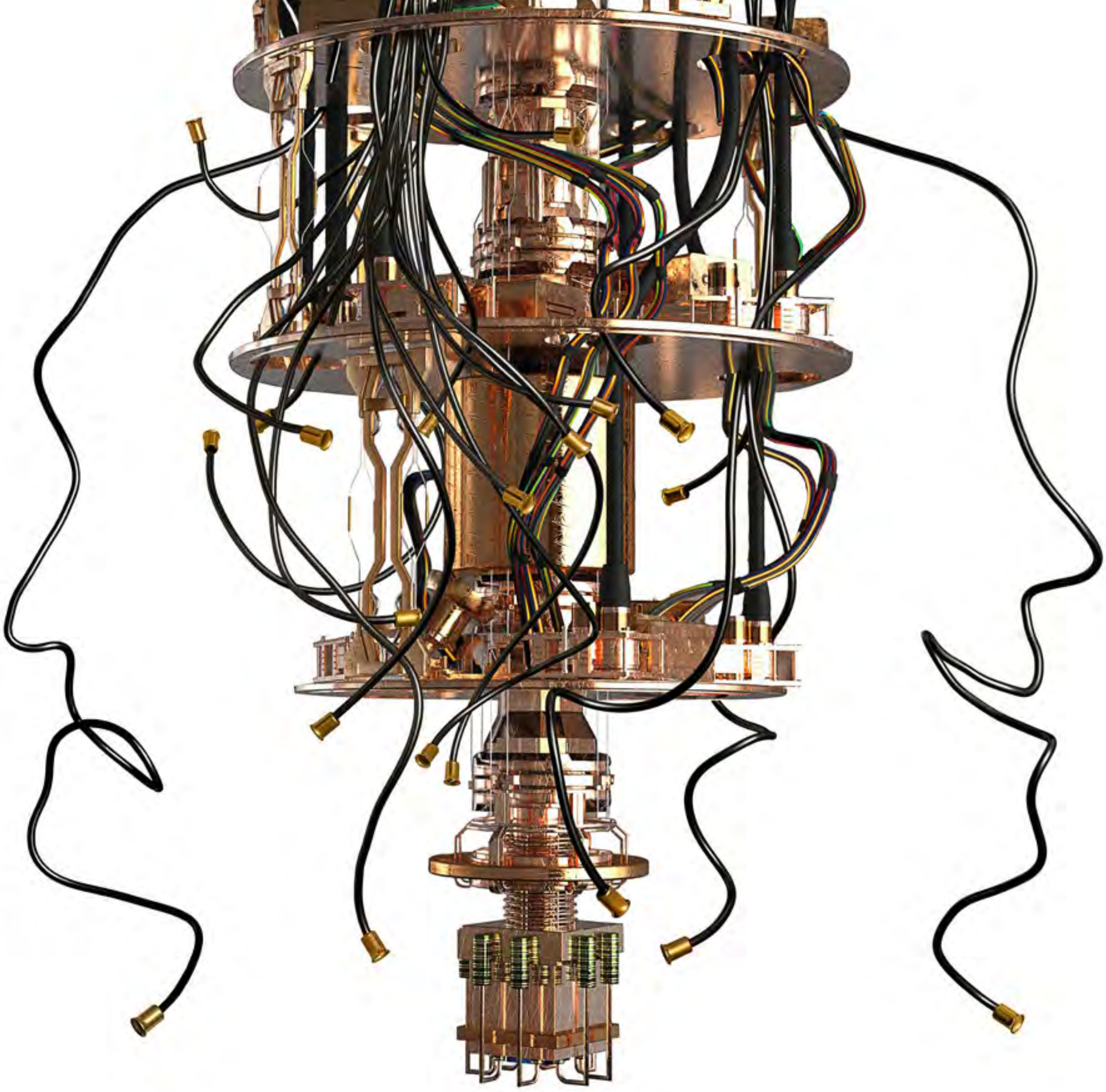
13. "NSF Convergence Accelerator – Privacy and Pandemics: Responsible Use of Data During Times of Crisis," by Jules Polonetsky, Dr. Sara Jordan, Christy Harris, John Verdi, December 16, 2020, Future of Privacy Forum. https://fpf.org/wp-content/uploads/2020/12/NSF-PP-FINAL-Paper-16-December-2020.pdf

14. "How the Global Pandemic is Impacting Data Privacy and Security," by Ameesh Divatia, May 6, 2020, *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2020/05/06/how-the-global-pandemic-is-impacting-data-privacy-and-security/?sh=430c71d95588

15. "The COVID-19 Pandemic: Where are we one year later? (Risk Management, Security and Privacy)," February 25, 2021, Forrester. https://go.forrester.com/press-newsroom/the-covid-19-pandemic-where-are-we-one-year-later-risk-management-and-security/

16. Toussaert, S. Upping uptake of COVID contact tracing apps. *Nature Human Behaviour* 5, 183-184 (2021). https://doi.org/10.1038/s41562-021-01048-1

17. Many other resources related to privacy and pandemic concerns are available at International Association of Privacy Professionals (IAPP): http://iapp.org



The Threat and Promise OF QUANTUM CYBERSECURITY

A look at all the ways these advanced technologies can both attack and protect us

BY DUNCAN JONES AND MARK JACKSON

EXPERTS BELIEVE THAT QUANTUM COMPUTERS will become powerful enough over the next few years to break current encryption methods, including the RSA public-key cryptosystem. It's believed that adversarial governments and other bad-faith actors are already pursuing a strategy of securing valuable digital assets, so they can be opened when quantum computers have achieved that ability.

Many cybersecurity professionals are aware of the looming threat that quantum computing presents to the long-term protection of their organizations' critical infrastructure and digital assets. However, what is not commonly known is the security resilience that quantum computers can also provide.

PHOTO ILLUSTRATION BY JOHN KUCZALA

CONTENTS

A 'QUANTUM ALGORITHM' IS BORN

The reason cybersecurity professionals need to completely rethink their data protection today is because back in 1994, Peter Shor's secret project had just hit paydirt.

Shor had been working furtively for about a year on a scheme he believed almost certain to fail. The applied mathematician at Bell Labs sought to develop a "quantum algorithm" to execute on a type of computer that didn't even exist yet. Such hypothetical devices would use the fundamental laws of quantum physics to perform certain types of calculations in parallel, eventually leading to an exponential acceleration in computations compared to standard, "classical" computers.

Shor's contribution was an algorithm that could efficiently factor a number into its constituent primes. For example, 15 can be factored into 5 times 3. Why would Shor focus his attention on such an apparently facile mathematical problem? The answer lay in the inability of classical computers to perform factoring of very large numbers, a fact that forms the bedrock of modern asymmetric algorithms, such as RSA. A new method to efficiently perform factoring would defeat modern encryption systems. And Shor had just provided the theoretical method for doing it.

Shor's Algorithm, as it became known, still required impressive quantum hardware. The number of quantum bits or qubits required is approximately twice the number of bits in the RSA key; an RSA key of 2,048 bits requires 4,098 qubits of perfect quality. For comparison, the computers of today have 50 to 100 qubits, and of an impressive, yet imperfect, quality.

A major milestone was achieved in October 2019 when Google demonstrated that quantum computers could perform a calculation in just a few minutes, which would have taken at least tens of thousands of years to complete on a classical computer.

A new method to efficiently perform factoring would defeat modern encryption systems. And Shor had just provided the theoretical method for doing it.

THE THREAT FROM QUANTUM COMPUTING

Despite such advances, there are varying opinions on when Shor's Algorithm may pose a serious threat to cybersecurity, with estimates ranging from five to 20 years. One factor suggesting a shorter timescale is the faster-than-Moore's Law trajectory of current quantum hardware. Honeywell, for instance, believes it can increase the power of quantum computers by a factor of 10 every year for the next five years, yielding an increase in power of 100,000x by 2025.

Does this mean you should wait until "Q Day" to become concerned? Absolutely not: The need to protect infrastructure systems is more immediate than that, for three reasons.

First, it takes time to upgrade security software, and massive infrastructure that corporations or governments utilize can require months or even years to make this transition.

Second, there are rumors that adversarial governments and other bad-faith actors are archiving data now in anticipation of future decryption capabilities, known as a "harvest-now, decrypt-later" attack. This means, for example, that the encrypted files of a future jet fighter could be stolen now and later decrypted.

Third, Shor's Algorithm is a proof that efficient decryption of RSA is realizable but is by no means the *most* efficient way to accomplish this; there have already been substantial improvements upon the original algorithm.

It is entirely possible that tomorrow a clever researcher could develop a vastly more efficient method of decryption, placing us that much closer to cybersecurity vulnerability. Thus, enterprises should consider making the transition as soon as possible.

Fortunately, intense effort is already underway to develop new cryptographic algorithms resistant to quantum hacking.

In 2016 the National Institute of Standards and Technology invited submissions for such "Post-Quantum Encryption (PQE)." Intense study followed as mathematicians, computer scientists and physicists did their utmost to defeat such submissions using quantum technology,

CONTENTS

both existing and theoretical. From the original 82 submissions, there are currently seven finalists. The winners are expected to be announced between 2022 and 2024. There will likely be a few algorithms selected, with a tradeoff between security and power consumption.

PROTECTION USING QUANTUM TECHNOLOGIES

While it has become well-understood that quantum technologies can be used to *attack* communications, what is lesser known is how they can be used to *protect* communications. In particular, their role in an often overlooked yet fundamental aspect of cybersecurity: randomness.

Randomness is most often associated with cryptographic keys or passwords. An obvious property of such keys is that their method of generation should be *non-deterministic*. Any mathematical formula or pattern in such supposedly random generation would render its usefulness null.

The other essential aspect is its *security*. After its generation, there should not be any means for an adversary to gain knowledge of what this key is. Both these number generation and security issues are directly relevant to quantum computing.

Let us first consider number generation. While we all have an intuitive sense of what randomness means, have you ever considered how to generate a truly non-deterministic random number? Your first instinct may be to toss a die. But consider that the die obeys the laws of physics, which are completely understood and completely predictable. If you measured the speed and direction of your toss, the air pressure, the weight of the die and so forth, and then performed careful calculations to compute the trajectory, you would predict the outcome with 100% certainty. The fact that such modeling is possible means that this outcome is not at all random.

If we generalize this concept, we realize that *any method using classical (non-quantum) physics is deterministic*. This includes asking a classical computer to generate random numbers. While they can certainly generate *pseudo* random numbers, the computer merely follows a formula based on internal, obscure data (such as the number of milliseconds to have elapsed since the last restart) to calculate numbers that only superficially appear random. All of this could be modeled by a quantum-powered attacker.

Quantum physics is based on superposition, the idea that a system can exist in multiple configurations simultaneously. Measuring the system then forces it to choose one of these configurations.

The answer to producing true randomness lies in quantum physics. Quantum physics is based on superposition, the idea that a system can exist in multiple configurations simultaneously. Measuring the system then forces it to choose one of these configurations.

To produce the quantum equivalent of a coin toss, prepare a quantum state in a 50% “1” state and 50% “0” state, and then measure it. This will result in a “1” or a “0” outcome with equal probability. Performing this operation several times results in a string of 1s and 0s corresponding to a random key.

There are a number of commercially available quantum random number generators (QRNGs) that attempt to measure quantum processes like this. While such QRNGs may be entirely viable ways of producing random keys, there is a shortcoming related to their security. If an adversary were to tamper with the quantum states, or at least eavesdrop, how would one know? The output is simply 1s and 0s, and so it would be impossible to determine if this were secure or not.

This is not merely a hypothetical: “Quantum Hacker” Vadim Makarov demonstrated that he was able to influence the output of quantum tunneling by shining a flashlight on the photodetectors. A similar issue would occur if the performance of the QRNG degraded over time—something that is quite feasible in a complex device that relies on mirrors and lasers.

Are we then cursed to have this theoretically random-but-insecure means of producing cryptographic keys? Fortunately, quantum mechanics comes to the rescue once again.

PLAYING DICE WITH THE UNIVERSE

Albert Einstein famously commented, "God does not play dice with the universe." Apparently, He (or She) does, and in 1964 Irish physicist John Bell proved it.

Bell developed a mathematical method to distinguish quantum processes from classical ones. This was based on *quantum entanglement*, the idea that the quantum state of one particle can be correlated with another, even if physically separated. Entanglement is a purely quantum property with no classical counterpart.

By focusing on entanglement, Bell provided a precise means of identifying quantum (and therefore random) processes from classical (and therefore deterministic) processes. And since any tampering or eavesdropping would require classical means, Bell also provided a proof of the outcome's security. There is no longer any trust in devices required, only fundamental physics.

New approaches to cryptographic key generation are being developed that build on this trustless entanglement technique. These approaches offer guarantees (and proof) that the keys are perfectly random in nature and haven't been influenced by any attacker, quantum or otherwise. As we move toward a quantum future, technology like this will be critical to maintaining the security we enjoy today. ●

Duncan Jones (https://www.linkedin.com/in/duncanjones/) is head of quantum cybersecurity and **Mark Jackson** (https://www.linkedin.com/in/drmarkgjackson/) is a quantum evangelist at Cambridge Quantum Computing.

LUNCH & LEARN

A cybersecurity consultant elevates breakroom banter into a teachable moment

BY LLOYD DIERNISSE, CISSP, CCSP, CAP, LSSBB, PMP, CSM, CMMI-A, ITIL-F V3

ILLUSTRATIONS BY ENRICO VARRASSO

A FEW YEARS AGO, a cybersecurity manager named Joel and I struck up a casual conversation in the company's breakroom about popular methodologies to optimize workflows and productivity.

"Lean, and all of those other ideas, are just fads, right?" Joel said with a smile. "Today, we should 'Think Lean,' or use Six Sigma; next month it'll be something else. Why waste time learning something that's just a buzzword from the C-suite and doesn't apply to our jobs?"

Over the years, I've heard similar comments in organizations that take up the latest magic elixir to cure internal problems and beat competitors. Lean Six Sigma. Capability Maturity Modeling. Agile. The Theory of Constraints. These and many others are viable concepts launched at considerable expense that too often end in frustration and broken promises.

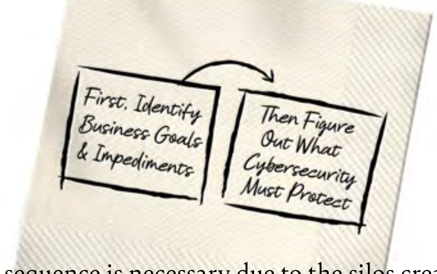
Yet some organizations successfully adopt them and realize their benefits.

Why do some succeed when others fail? A common thread among failures I've witnessed boils down to leaders essentially addressing a symptom, not the disease. To get results, you must start by asking the right questions. Not just of the C-suite, but of the cybersecurity professionals that support them.

ASKING THE RIGHT QUESTIONS

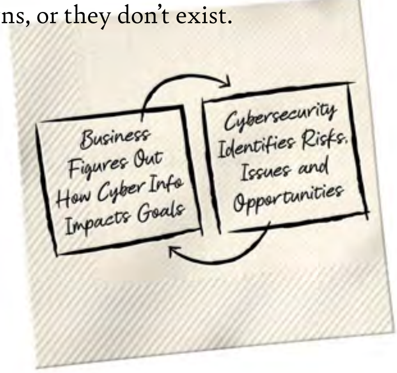
First, business leaders must ask themselves, "What do we want to achieve?" They need to ask employees, "What is—or could be—standing in our way?"

Second, cybersecurity professionals should ingest those answers and ask, "To support our business, what do we need to protect?" and "Protect it from what?"


First, Identify Business Goals & Impediments
Then Figure Out What Cybersecurity Must Protect

This sequence is necessary due to the silos created in traditional top-down hierarchal organizations that hold cybersecurity separate from other business activities. That's inefficient, costly and highly vulnerable, but still common.

The conversation isn't one-way, nor is it a "one and done." When cybersecurity folks perceive risks, issues or opportunities, they must inform the business by creating a feedback loop. Healthy organizations have several loops with traffic continuously flowing in and out of all silos. In unhealthy organizations, these loops suffer frequent breakdowns, or they don't exist.


Business Figures Out How Cyber Info Impacts Goals
Cybersecurity Identifies Risks, Issues and Opportunities

Cybersecurity
Business

Better communication is enabled when silos disappear, and the business sits upon a foundational culture of security—one it can draw support from while achieving goals. But you already know this, don't you?

Yet, if you don't have the authority to restructure the company, how do you get there?

Let's go back to our earlier chat with Joel. It inspired a "bring your own" lunch with the rest of the cybersecurity team, where I led a discussion about efficiency and quality, two aspects of cybersecurity that are often misunderstood or overlooked, even by the most diligent professionals. My goal was to help them see that Lean and Six Sigma were not fads but foundations to solid growth when understood and properly applied.

THE FIRST LUNCH

At that initial lunch, I asked who was familiar with the adage 'Complexity is the enemy of security.'

Everyone's hands went up.

"How many of you believe it?"

Not as many hands, though still a clear majority.

Barbara, the senior cybersecurity architect, spoke for the dissenters. "It's true in many cases, and my team strives to avoid unnecessary design complexity because it adds cost and increases the attack surface, thus exposing new vulnerabilities and attack vectors. However, sometimes we need more granularity to implement more refined security. Just like with microservices or containers, there are pros and cons in every design."

"Absolutely, Barbara," I replied. "We've all learned that security must be tailored. We do the business a disservice by insisting on a one-size-fits-all approach, particularly when solving technology-centric problems. However, what about process-centric problems?"

Crickets.

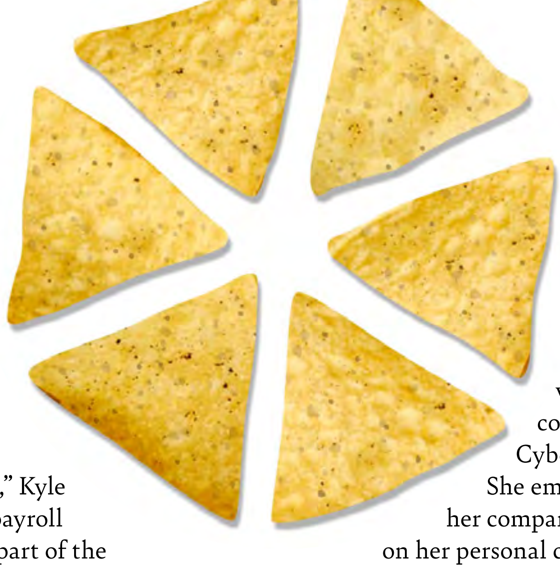
A cybersecurity engineer known as Kyle finally broke the silence. "That's in the business domain. That's up to them to figure out."

"Really?"

"Yes. We tell them how stuff needs to be protected, not how to do their jobs. They wouldn't want to hear that from us anyway," Kyle replied, with several others nodding in agreement.

"You're right," I responded. "They don't want to hear a message packaged like that. However, what if we offered to reduce levels of effort, save money *and* improve our security posture? Would they want to hear that?"

"How?" asked Kate, the director of change management.



"When the board of directors interviewed me, they mentioned a problem with the company payroll and releasing funds on time. Let's talk about what happened," I opened.

"I remember. We all do. We assumed that's why you were hired," Kyle interjected. "The person running payroll needed her personal computer for part of the process, and it failed. She was working from home during the pandemic and couldn't get a replacement computer in time."

"So," I began, "from a security standpoint, obviously several things are wrong, but as I understand it, she was simply doing her job within constraints imposed by people above her. These didn't just constrain security, they limited the business, delaying delivery of one of its most fundamental obligations on time. Their decisions created the situation; it was an accident waiting to happen.

"What we have is an illustration of how security problems are inseparable from business problems and poor decisions that create or complicate those problems," I continued.

That's when I steered the conversation to Lean Six Sigma as a way to bring up Joel's earlier comment about the process being another "fad from the C-suite."

A NOT-SO-DEEP DIVE

My goal was to show how Lean Six Sigma could support the culture the company wanted to build. I kept it high-concept, leaving the details for future lunches. And I kept the focus on a specific issue: the payroll analyst who couldn't complete her work.

"The payroll analyst encountered issues described by Taiichi Ohno, who is considered to be one of the founding fathers of process improvement in Japan. He described *muda* (wasteful or excess activities), *muri* (overburdening or unreasonableness) and *mura* (unevenness). He advocated 'thinking Lean,' to reduce activities that add cost without adding value. We become Lean by trimming away the excess or unnecessary components.

"Let's start with muda, or waste, if you prefer. Mr. Ohno identified seven types of waste, but nowadays, an eighth type is commonly added."

Then I broke it down on a whiteboard:

Excess motion: The analyst had to move back-and-forth, using two computers, although sitting side-by-side in her home office.

Excess transportation: Payroll information was transported through different systems. She used her company computer to calculate the payroll but couldn't download updated software from the bank. When she raised the issue, she was instructed to use her personal computer for bank connections until Cybersecurity approved the software. She emailed exported payroll data from her company computer to her personal email on her personal computer.

Excess inventory: Seen in the technology used above.

Waiting: Although wait times between steps were short, many were unnecessary. Wait times are cumulative—a few minutes per day quickly adds up to a few hours per pay period, then several hours, possibly days, per year. The adage 'Time is money' tells us that unnecessary waiting equals unnecessary (no value added) costs.

Over-processing and over-production: She "touched" the same information several times for one task and created several copies. Data, including sensitive personally identifiable information (PII), ended up in many places. The original export was in her company computer and in an email (stored in the Sent folder in her company account.) The Inbox of her personal email account held another copy and she saved yet another copy in her personal computer for convenience.

Correction: The cost of fixing mistakes, or defects, is a real possibility here because it involves extracting data from one system, transforming it into another format, and loading it into another system—an extract, transform and load process. If a mistake is corrected in one copy, but others aren't corrected or deleted, including email attachments, data gets out of sync.

Then I let everything sink in.

"See the overlaps? A single inefficiency created several types of waste. Business concerns created cybersecurity concerns, such as asset management, privacy, malware vectors and data exfiltration. Confidentiality, integrity and availability—the entire CIA Triad—was in jeopardy."

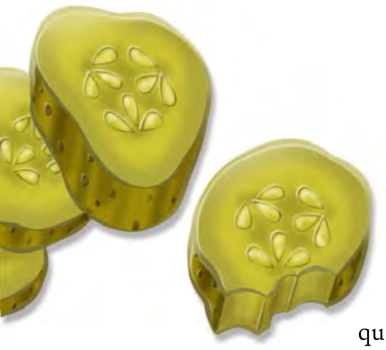
Kate asked, "What about the eighth type of waste?"

"It deals with *skills*, or the waste of human potential," I responded. "It's rampant here, as I'm sure you've seen by now, and it's on my radar, but it's another deep subject and unfortunately not one we'll address today."

THE SECOND LUNCH

During our second lunch, I explained how Six Sigma helps us manage the quality of our work. Until the 1980s, organizations typically tested for defects only *after they*

CONTENTS



produced something, but before it shipped. This is known as quality control (QC) because they were literally controlling how many defective products they ship.

Some organizations shifted the focus, integrating quality assurance (QA) activities into their creation processes, making it more difficult to *build* defective products. They sought out and measured variations in their processes, then performed QC tests to catch residual defects. If defects showed up anyhow, and some always did, they'd re-examine the process from the beginning to determine four things:

- Where did the defect occur (where did the process vary or deviate and by how much)?
- When did it occur (timing of events may be a factor)?
- Why did it happen (the root cause of the variation or deviation in the process)?
- How do we prevent a recurrence?

"Our QA is performed by testers," Joel said, "but not like that; they start after the developer has pushed their work from the development environment to the test environment. You're saying that's wrong?"

"The work isn't wrong, but the name is. That's actually QC," I responded. "It doesn't *assure* quality; it tries to *control* it in the test environment that sits between development and operations by running unit, functional or system tests. These are QC activities. That's critically important, but by itself, that's an inefficient and costly approach to defect management. In cybersecurity, we know hackers pounce on opportunities created by those inefficiencies. Testers uncover defects that require refactoring or new work, followed by more testing, and so on. Those costs don't add value because you already spent money creating a product, but it's defective, so now you must spend more to fix it. You're reactive, not proactive, and you're not ensuring better products going forward."

"I get it," Linda said. "Uncontrolled variations create Lean wastes, albeit in different forms. First, is overburdening, like testing and retesting, especially if it's manual. Waiting for something to move from development to testing and waiting for test results and rework. Then additional corrections and excess transportation and motion in the back-and-forth. Adding true QA to development with Lean Six Sigma improves our products *and* our security posture, by making it more difficult to build in defects or flaws, correct?"

"Exactly," I replied. "But there are no panaceas. Immature or unyielding organizations don't always acknowledge their problems and seek help. Mistakes happen, and problems occur in healthy organizations, too. That's a certainty, and there's plenty of valid debate about how much these programs help or hurt.

"Another certainty is that Six Sigma requires 'shifting left.' Thinking Lean and going back to the beginning of processes while looking for variations reduces both initial and recurring problems. That's the true meaning of quality assurance and why we integrate Lean with Six Sigma."

Joel asked: "I understand how Lean got its name, but what about Six Sigma?"

"Six Sigma is measuring the capabilities and variations in a process," I began. "In other words, how good is our process? Can it *consistently* produce the desired level of quality? If not, we investigate to understand where it's going awry (the variations) and root causes. A variation is expressed as the standard deviation (sigma) between a process's center, or ideal place, and boundaries (tolerances), called the upper limit and lower limit, which we get to specify and often display as a bell curve."

"Six Sigma, capitalized, is written as 6σ with the lowercase Greek symbol, differentiating it from the uppercase sigma used in other formulas," which I wrote on the board as ∑. In real numbers, this is only 3.4 defects per million. That's a high standard and it isn't always cost-effective to achieve it. By contrast, a standard of 5σ allows for 223 defects per million, and 4σ allows for 6,200 defects, so some companies use those values. People sometimes think of Lean Six Sigma only for manufacturing, because that's where it originated, but this is a way of controlling process variations—unwanted variations—in many industries, including IT.

"Six Sigma math can be a bit intense and it's a long road to certification. As a person demonstrates mastery of the techniques, they earn different colored belts. You may see Yellow, Green, and sometimes White Belts. It took me several years to earn certification as a Black Belt. Along the way, I learned that cybersecurity professionals can benefit from Lean Six Sigma as we seek to secure our organizations by improving quality and reducing inefficiencies that cost money without adding value."

With that, everyone in the room nodded as if taking in everything. I'd given them plenty of food for thought, but delivered it in smaller, digestible bites. Each now had a better idea of how methodologies long associated with other business units could be applied to their own. ●

LLOYD DIERNISSE, CISSP, CCSP, CAP, LSSBB, PMP, CSM, CMMI-A, ITIL-F v3, is a cloud, cybersecurity and Agile expert who helps organizations improve their processes, strategically manage their risks, and rationalize their portfolios. His latest course on Conducting Practical Risk Analysis for Security Professionals is available through the (ISC)² Professional Development Institute.

Garfield Heads Back to School

BY PAT CRAVEN

AS THE WORLD begins to slowly transition back to "normal," all signs are that children globally will be heading back to the classroom this coming school year. And that is great news for all of us.

When the pandemic began, schools quickly adopted virtual educational programs. Many were ill-equipped for the abrupt shift, with teachers required to provide meaningful lessons in formats for which they were not trained. Children were forced to spend more time online, with some students, parents and schools unprepared to offer adequate cyber safety educational training.

The Center for Cyber Safety and Education quickly converted our multi-award-winning, classroom based *Garfield's Cyber Safety Adventures* to a virtual format. We were able to create and offer live-video training on online safety for teachers to carry into their virtual classrooms.

Now, with a new school year on the way, we anticipate a surge in demand for our programs and have begun printing more copies. Educators and parents all realize that it was a mistake to put online safety training on hold and that it must now become a priority.

While our new Virtual Garfield and Garfield at Home programs will remain, students will be better served with the physical classroom Educator Kit that provides everything a teacher needs for 30 students in a single box, ready to go. If you are not familiar with our Educator Kit, check out this short video that unpacks six pounds of Garfield fun for children ages 6-11. (A Spanish language version is available.)

You and your company can now partner with us to help keep children in your community safe and secure online.

But the question I have for you is: Are your children and grandchildren going to be getting the program at their school this year? Well, that is up to you!

The small, hard-working team of four at the Center cannot possibly contact every school in the world. We need your help to reach children around the globe. Talk with your school leadership as well as your own employer about the importance of proper cyber safety training for children. You and your company can now partner with us to help keep children in your community safe and secure online. Here's where to order. If you have any questions please contact us at center@isc2.org.

Coming soon … Garfield lessons in Spanish. Sign up for our newsletter to keep in touch at www.IAmCyberSafe.org. ●

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

NEWSLETTERS WEBINARS PDI BLOG COMMUNITY MAGAZINE EVENTS CHAPTERS RESEARCH

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

"How do you know if you have a shadow IT problem? Don't go out and find every shadow IT connection—follow your users. They'll take you to the issue."

—Rob Bolton, Senior Director, Information Protection, Proofpoint, during (ISC)² Security Briefings Webinar "Cyberthreat Game Changer: A New Look at Insider Threats"

"Working from anywhere can be made secure if you have time to prepare and test. I was just brought into an agency in January 2020. The CIO was asking to purchase desktops. I asked: 'Shouldn't we be looking forward to having a mobile workforce and get laptops instead?' He replied, 'No. Desktops are the way to go.' Four weeks later we were sent home."

—CISOScott, Community Champion, on (ISC)²'s Community page discussing the post "Work From Home Being Blamed for Security Risks"

"When I first started in cybersecurity, I was a cybersecurity analyst, but I was specifically really enjoying incident response. Every opportunity I had, I would make sure to insert myself into anything that was related to incident response. And I proved myself and it clicked for them."

—Megan West, CISSP, X-Force Cybersecurity Incident Response Consultant, IBM, during (ISC)² Think Tank Webinar "Celebrating International Women's Day: Carving a Cybersecurity Career Path"

"If an organization hasn't committed to full patching and response, then they will serve as a pivot point to other services they are tied to."

—Anonymous respondent to (ISC)² Community SolarWinds breach survey

Source: (ISC)² blog post "Survey: Cybersecurity Community Increasingly Concerned About SolarWinds Breach"

"The first ransomware case I ever worked, the demand was for $700 worth of Bitcoin. I had to drive to a tavern in Crestwood, Alabama, and take $700 in cash. They had a Bitcoin ATM in their bar and I had to buy $700 worth … that's the first one I ever worked. The demands have just skyrocketed since then."

—Will Taylor, Senior Security Consultant, NXTsoft, during (ISC)² Security Briefings Webinar "Top 3 Trends in Today's Cyber Attack Landscape"

"Improper use of the default namespace—where system components run—was the most common mistake, which could give attackers access to the system components or secrets."

—Accurics research report on cloud misconfiguration remediation issues.

Source: May Cloud Security Insights