PUTTING YOUR BUSINESS CONTINUITY PLAN TO THE TEST

InfoSecurity PROFESSIONAL

JULY/AUGUST 2020

A Publication for the
(ISC)²® Membership

UNDER PRESSURE. UNDER CONTROL.

How to stay sane and manage stress during an exceptional time

+

Understanding Stress Models to Build a More Resilient Workforce

EPISODE 2 OF
PERRY CARPENTER'S SERIES

Trojan Horses for the Mind

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

contents

VOLUME 13 • ISSUE 4

I think I know how we can do that.
We just have to get them to care.
I'm listening, Katie.

PAGE 29

features

Cover illustration: ROBERT NEUBECKER Illustration above: TAYLOR CALLERY

departments

InfoSecurity Professional is produced by Twirling Tiger® Media, 7 Jeffrey Road, Franklin, MA 02038. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)²® on the issues discussed as of the date of publication. No part of this document print or digital may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of (ISC)². (ISC)², the (ISC)² digital logo and all other product, service or certification names are registered marks or trademarks of the International Information Systems Security Certification Consortium, Incorporated, in the United States and/or other countries. The names of actual products and companies mentioned herein may be the trademarks of their respective owners. For subscription information, please visit www.isc2.org. To obtain permission to reprint materials, please email infosecproeditor@isc2.org. To request advertising information, please email lpettograsso@isc2.org.

editor's note | *by Anne Saita*

A Sheltered Life

I KNEW EVENTUALLY I'D CRACK while hunkered down to avoid the quiet killer known as COVID-19. What I hadn't anticipated was the catalyst being a children's television program. Pre-pandemic, the show was an integral part of our early morning routine—a routine I quickly craved in the wake of the initial chaos and uncertainty. When the show came on a month into our self-quarantine, I instantly longed for my former life and then felt guilty, given so many others have lost so much more.

I know everyone reading this experienced something similar. We either desired alone time in a crowded home or actual face-to-face interaction in a near-empty one. At one point, half of the world's population was sheltering in place to help stop the spread of a novel coronavirus we could not see nor control. We reeled from the sudden loss of simple freedoms, the harsh economic fallout and the persistent supply shortages. We were (and maybe still are) consumed with grief. Too many of us now live without loved ones who never got a proper send-off. Too many of us still face financial insecurity. Too many of us show symptoms of post-traumatic stress disorder, especially essential workers who risked their lives in order to spare ours.

Even before this contagion upturned life as we know it, we wanted to provide (ISC)^2 members constructive tips on staying in control while under pressure—because cybersecurity is a demanding occupation regardless of where you work. We already planned to provide expert advice for how to psychologically handle an incident, never imagining an event on this scale. And, because security awareness training is at the heart of any organization's cybersecurity program, we wanted to introduce another way to get through to people, whether they have returned to the office, remain at home, or adopted some hybrid work habit.

You've likely already heard this, but it bears repeating: It's OK to not be OK. What's not OK is to pretend that everything is. It's not. We're not. But with time, reflection, acceptance, appropriate action and some self-care, we will be. ■

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

©Rob Andrew Photography

InfoSecurity PROFESSIONAL

(ISC)^2 MANAGEMENT TEAM

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

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

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

CORPORATE COMMUNICATIONS LEAD
Kaity Eagle
727-683-0146
keagle@isc2.org

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

TWIRLING TIGER MEDIA MAGAZINE TEAM

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

ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org

EDITORIAL ADVISORY BOARD

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

SALES

VENDOR SPONSORSHIP
Lisa Pettograsso
lpettograsso@isc2.org

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

Prepared, or Are You?

by Bruce Beam, CISSP

"**WHAT DO YOU MEAN WE ALL HAVE TO WORK FROM HOME?"** How many times do you think this phrase has been uttered in the last several months? Apprehension welled up in many IT and security professionals as they thought of the entire workforce operating remotely off systems that had never been tested at this scale. Which organizations will survive this test through 2020 and beyond? Hopefully, all will. But I fear several will not because they never fully developed or exercised a business continuity plan (BCP).

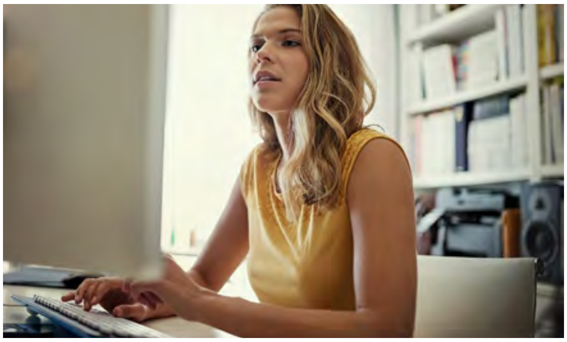
If you talk to many IT professionals, they will tell you they have a BCP and they are ready for any event. Did they test that BCP? Did they move it through the full course and correct any discrepancies? Or was it a walk-through to say it was completed? They are now finding out if it really worked as expected.

(ISC)² embarked on our digital, end-to-end transformation program more than four years ago, and it was designed with business continuity in mind as a cloud-first architecture. Utilizing this architecture enabled the enterprise to seamlessly shift from our offices to remote work locations with less than .05% of the employees initially reporting an issue associated with the new environment. This design enabled full functionality for the remote workforce without sending our IT resources scrambling for cover.

Another critical area where our digital transformation design proved itself was in the security arena. Our cloud-first approach enabled the team to operate securely in an environment where the threat has increased drastically. With all applications behind multi-factor authentication and numerous security features (such as geo-location) funneled into a common collector analyzed by the remote security operations center, the result was great visibility across the entire "network."

Bruce Beam, CISSP, is CIO and vice president of (ISC)². He can be reached at bbeam@isc2.org.

As the landscape changed quickly to send workers home, there was almost no change in the business-as-usual posture for the security team. Instead of working on numerous connections or access issues, the security team was able to focus on the quickly emerging threats, working closely with our SOC to ensure we remained secure. It also afforded the team the time to fine-tune endpoints and alert parameters to further protect all workers now joining from different home networks all over the world.



Getty Images

> **If you have not started the journey, now is the time to transform your business to meet this new, emerging environment.**

Times have changed, and they will remain in this state to some varying degree. If you have not started the journey, now is the time to transform your business to meet this new, emerging environment.

"Plan for the worst, hope for the best" is an approach now needed to ensure your business is ready for any challenge. Work closely with the business leaders in your company to develop a roadmap to meet all requirements while managing risk, IT and security costs, and the growing world of compliance. This is not the time to decide if you need to transform. This is the time to transform or risk being left behind. ■

RETURN TO CONTENTS

ELEVATE Your Skill Set with the CCSP

CCSP® Certified Cloud Security Professional

An (ISC)² Certification

CCSP is on the rise as our fastest growing certification. That's not surprising, given that cloud security is the area where cybersecurity professionals are in greatest demand.

The CCSP shows you have the advanced technical skills and knowledge to design, manage and secure data, applications and infrastructure in the cloud using best practices, policies and procedures. If you're ready now or even just a little curious, the Ultimate Guide to the CCSP is a great place to start.

THE ULTIMATE GUIDE TO THE CCSP
Be a Leader in the Field of Cloud Security

Ready to elevate your skill set?

GET YOUR GUIDE

field notes | EDITED BY DEBORAH JOHNSON

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

PANDEMIC DIARY

#OneWorld: How We All Initially Coped in the Face of a Global Outbreak

We reached out to (ISC)² chapters around the world to ask about their experiences in the immediate aftermath of COVID-19's global spread. Here are some of their stories.

Victor Wolfe, former president, (ISC)² Hawaii Chapter

I contracted the COVID-19 virus while traveling from Colorado back to Hawaii on March 28. I made it out the other side OK, and I am well now. We held our March and April meetings virtually and will be holding our meetings virtually for the foreseeable future. We use Google G Suite products, including the updated version of Hangouts called Meet. It is a convenient way to conduct meetings while having administrative control over who enters the rooms, so we can mitigate any "zoombombing"-style attacks on our meetings.

April was my last meeting as the chapter president as I am an active-duty Army officer scheduled to be stationed at Fort Bragg, NC, this summer. The chapter is being left in good hands and I thank everyone for their support during my leadership.

Darwin Tang, president, (ISC)² Guangzhou, China, Chapter

Even though it's had an adverse impact to the economy, we see more opportunities on the cyber side. More companies are working remotely and online. So there is more work for cyber professionals. From the chapter side, we are organizing more online activities.

Günter Aigle, secretary, (ISC)² Germany Chapter (Düsseldorf)

We had planned our first nationwide chapter meeting for April. Because of the shutdown here in Germany, we had to cancel everything and are now planning for late Q4 in 2020. As an option, we currently are evaluating a web-based meeting, at least for the members meeting we have to perform according to the German law for registered associations.

Our advice to the other chapters would be: As you have to stay home, don't forget to stay connected! Interaction, chats and talks are even much more important in those times of personal isolation.

What we see happening in many companies, unfortunately, is the sacrifice of painfully achieved security measures to the needs of the remote work (which is called "homeoffice" funnily enough here in Germany). Just one example: OWA (Outlook Web Access) had been denied in many companies due to the potential security risk, as OWA usually is just 1FA (username/password). The phishing of credentials has been used very successfully by the "bad guys"—despite security awareness measures—so companies shut down OWA and made email access only available for those who need it externally via a 2FA VPN connection.

Now, in coronavirus times, there was a desperate need for everyone to be able to communicate, so OWA was turned on again, resulting in users accessing OWA from any kind of device, regardless of the security level of the device(s). The door for the "bad guys" was wide open again. So the advice would be not to sacrifice every previously achieved goal in IT security to the coronavirus needs. Otherwise, you might regret the results and the effects on your corporation.

Hernán Colonel, Asociación Civil Profesionales de Seguridad de la Información, (ISC)² Argentina Chapter (Buenos Aires)

Argentina declared total quarantine in March. In my IT professional work, I have to say I feel very privileged since I work at a regional level covering many countries in the Andean region of Latin America. So, my job has been impacted very little, if at all, from a day-to-day perspective. We did see an impact shifting the demand from our typical line of business to remote access and scaling websites' capacities in a short period.

On a personal level, my daughter is attending virtual school

RETURN TO CONTENTS

with possibly more activity than when attending personally, so she is eager to go back to the previous model. My wife and the rest of the family are doing well, only affected by the little mobility available. I have been taking care of a close family member with health issues. In my absence, our local chapter team has done an excellent job holding meetings remotely as usual with little to no impact in attendance.

Ping Jing, membership chair, (ISC)² Chengdu, China, Chapter

The most significant impact on our chapter is we had to suspend our F2F technical sharing conferences every month, which we planned to start in March. Most members expected activities to resume ASAP. But we're still waiting for more positive indicators.

We have a dedicated WeChat group for our chapter. Fortunately, our chapter members are all safe and healthy. While being isolated and staying home, many members engaged in self-development and improvement during the "long vacation."

The impact on a personal life may be more obvious than a professional life for many of our members, as we can survive working remotely in many cases. Isolation brought many inconveniences in daily life, e.g., you cannot gather, you cannot easily visit your friends and even family members. Kids have to stay home for a long time as schools are closed. People have been fearful and anxious, especially at the beginning of the pandemic. Fortunately, we have passed through the most difficult time and are beginning to step toward recovery. We sincerely appreciate the people who help to make the turnarounds.

Felipe Castro, (ISC)² Chile Chapter

The chapter had been looking for a new venue due to the Santiago riots going on since 2019. The arrival of COVID-19 actually solved this problem for us: We jumped to cyberspace and are already holding our officers' meetings and chapter meetings via videoconference. Professionally, COVID-19 is a mixed bag. While badly hit industries like travel/tourism scale down and even lay off cybersecurity pros, those organizations that are going full digital are scrambling to protect their new cyber assets, such as payment pages, government permits or online education—with some learning in pretty spectacular fashion. I've hunkered down at home with my family, discovering a brave new world that includes The Division, Scrabble, Westworld and a few world-class musicians living within earshot (special kudos to that saxophonist, whoever you are).

A Snapshot of the Pandemic's Impact

An (ISC)² COVID-19 Pulse Survey of 256 cybersecurity professionals taken in April offers a glimpse of the early challenges faced and actions taken.

90% were working from home

47% were taken off security duties for other IT tasks

23% of organizations experienced an increase in cybersecurity incidents

32% were aware of someone in their organization who contracted COVID-19

Additional survey results can be found here.

James Packer, president, (ISC)² London Chapter

These certainly are extremely challenging times for the (ISC)² London Chapter, with arguably the biggest impact to our operations being that of time. Our officers generously give their free time to support the chapter; however, the concept of free time is somewhat of a distant memory of late. From an increase in COVID-19-related attacks at work to a loss of childcare, to caring for vulnerable family members, this pandemic is diverting attention to the much more immediate spheres of life for the team.

However, our officers are finding ways to overcome these challenges through our favorite secure conferencing service, Teams! (Bet you thought I was going to say Zoom.) We are busy planning our virtual meetups, with our usual lineup of industry speakers and partner organizations but condensed into a much smaller, bite-sized event that can fit into our members' hectic schedules. Our officers are still very much out in our communities promoting our cause through online presentations, talks, podcasts. And even as NHS (National Health Service) responders are on the other end of the phone to help those most in need.

In all, we've learned that we are in a brave new place as a society, where there is a new normal and it is OK that things work a little differently. People get it. Hawaiian shirts are now acceptable videoconference attire, you will hear the occasional screaming child in the background on calls, and people are generally a little more numb to shocking news. We are being tested as individuals and a wider society, and it's OK to just

Getty Images

RETURN TO CONTENTS

stay afloat, and perhaps come out the other side a little worse for wear. Because come out the other side we will. And if you do emerge feeling dazed, confused and like you've not really achieved much in recent memory, in that feeling you will not be alone.

Christopher Hails, president, (ISC)² New Zealand Chapter (Auckland)

Our Auckland Chapter responded quickly to the evolving COVID-19 situation by moving to virtual meetings in March. It's likely we will be under New Zealand's national security lockdown regime for some time to come, so we have looked to provide free webinars to all information security professionals, not just chapter members, with a rise in interest. This will likely continue to later in the year (https://www.isc2chapter-auckland.org.nz/events/), although New Zealand has gotten off relatively lightly to date on number of coronavirus cases.

Personally, I have been tasked with supporting our national transportation network response efforts helping our National Emergency Response Team (NERT) with intelligence capabilities over cybersecurity and physical security issues around supply chain, public transport and road safety for essential workers.

We have moved all staff (close to 3,000) to working from home and have supported efforts, to secure our networks and data, provide new remote working solutions (new SaaS platforms) and escalate delivery of major projects to facilitate remote call center functionality, amongst others.

It will be interesting to watch how the world evolves as we work together to tackle the pandemic. Will businesses continue to let many staff work remotely with associated increased risk? Will the perimeter security model look even more irrelevant as huge swatches of the workforce utilize SaaS, BYOD and consumer—not enterprise—technologies to continue being productive? ■

RECOMMENDED READING

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

Governance in the Digital Age

BY BRIAN STAFFORD AND DOTTIE SCHINDLINGER

(Wiley, 2019)

THIS AGE OF SOCIAL MEDIA, streaming and advanced software presents challenges to boards of directors, perhaps even disrupting their strategic goals. In *Governance in the Digital Age*, authors Brian Stafford and Dottie Schindlinger examine how corporate leadership can adjust to the ever-changing business landscape. From a security point of view, the authors suggest that directors, as part of the governance function, must be aware of impending risks, threats and issues relating to security, social media and technology that affect their firm's strategic objectives. New technology can be a disruptive force, and a diligent director needs to have a vision of how it may impact the firm's bottom line and growth trajectory. In the case of a breach, boards are held accountable for the control posture that failed at the time. Directors must plan ahead, anticipating threats and risks, and develop remediation strategies. By not adjusting to the changes, they are not fulfilling their role as "trusted advisors."

Through interviews with corporate directors, the authors survey the landscape and offer guidance and insight into navigating the governance paradigm. Stafford and Schindlinger offer suggestions on how directors can better work together, sharing different viewpoints in order to stay relevant and offer value in their new roles. "Embrace innovation," the authors advise. They provide guidance on soft skills and some hard skills to help a forward-thinking board make "the shift from cautious to innovation catalyst." Bravo! ■

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

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

Earn Two CPEs for Reading This Issue

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

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

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&ACTION=SI&CatRedirect=10846%7C10846

RETURN TO CONTENTS

MEMBER'S CORNER

The *Real* Threat to the Threat Intelligence Community

BY THOMAS McNEELA, CISSP

IF YOU'RE AN INFORMATION SECURITY PROFESSIONAL, you've likely at some point had to weigh the pros and cons of establishing a threat intelligence program at your organization. In my opinion, such a program can be valuable—if you know how to operationalize it. However, some of the common poor practices in the threat intelligence community today hinder the overall benefits that can be gained from participating in it. The following are some of the top grievances and how to address them.

Hanging on to your IOCs for dear life

The whole point of a threat intelligence program is to obtain advance knowledge of threats before they hit your organization, allowing you to take proactive defensive measures. Indicators of compromise (IOCs) are the main way such threats are communicated to participants within a threat intelligence community. Some examples of IOCs would be a malicious IP or domain name, a phishing email address, or a malware file hash.

Most organizations today that are part of a threat intelligence community ingest IOCs they receive, but then don't share IOCs they detect to others in the community. There is some irrational fear that sharing them too widely could harm the originating organization, but this fear is generally unfounded. Most IOCs are simply labeled with no context other than type, category, impact and confidence level. There is no requirement that disclosures detail how the threat was detected, and if it was part of a breach or bounty from threat hunting. None of that information is needed or really relevant to other organizations, so it shouldn't be included. That should reduce the risk of reputational damage that worries those in fear of sharing an IOC.

When in doubt, just set your Traffic Light Protocol (TLP) level to amber or red. That way you can share what you found with your immediate community but limit or prohibit re-sharing outside of it. For a quick introduction to the TLP, go here: https://www.us-cert.gov/tlp.

Not providing enough context with shared IOCs

As I mentioned above, there's no reason to share too much information about your IOCs if it could potentially damage your organization. However, the more context about the nature of an IOC that you can safely provide, the better. So instead of simply sharing something like "This IP address is bad," you could say "This IP address seems to be part of a botnet focused on DDoS attacks using UDP flooding on port 8443." That way, fellow community members can decide what security tool(s) to adopt and deploy to better protect their organizations.

ISAC woes

A great source of free or low-cost threat intelligence data that is particularly relevant to your organization is an Information Sharing and Analysis Center (ISAC). This is a closed community of organizations in a related sector that shares threat intelligence. They require an invitation or an application, which must be approved by the current members in order to join. The problem with ISACs is that sometimes their speed to share intel is not ideal. Some ISACs only share intel via manually sent emails. This is where a threat intelligence platform (TIP) comes in handy. A TIP usually comes with premium intel sources and makes intel sharing quick, easy and often automated. I think everyone running a threat intelligence program should use one—especially those belonging to an ISAC. Anomali has published a fantastic article explaining the capabilities of a TIP at https://www.anomali.com/resources/what-is-a-tip.

But even if they don't use a TIP, I've found that ISACs often have some of the most detailed and valuable intelligence around. And if they partner with any government agencies, you may even receive some sensitive intelligence far in advance of the general public. If you're interested in joining one, the best place to find your ISAC is through the National Council of ISACs at https://www.nationalisacs.org/member-isacs.

THOMAS McNEELA, *CISSP, MSIS, CEH (Master), is an experienced information security professional and continuing education instructor currently working for an information security software and services firm in the Chicago area.*

To learn how the author operationalizes his own threat intelligence program, be sure to read the June issue of Insights, from which this is excerpted.

RETURN TO CONTENTS

Guiding the Next Generation of Cyber Professionals

An NGO reached out to the (ISC)² Ghana Chapter and members stepped up

A PARTNERSHIP HAS DEVELOPED in Accra, Ghana, that is giving (ISC)² members the chance to share their knowledge and experience with up-and-coming cybersecurity professionals. It's a major need in the community, according to chapter President Stephen Cudjoe-Seshie in an interview via email. "It has to do with creating the right level of security awareness for the various user categories (children, parents, professionals, etc.) that interact with today's IT-driven systems, to drive safe practices."

Chapter President Stephen Cudjoe-Seshie

The opportunity to help train others on safe cybersecurity practices arose when Cudjoe-Seshie was contacted by Maxim Nyansa, a nongovernmental organization (NGO) that aims to create career opportunities in information technology for young Africans. As part of a cybersecurity boot camp for young IT graduates from underprivileged social backgrounds, Diana van der Stelt, a co-founder of Maxim Nyansa IT Solutions Foundation, invited Cudjoe-Seshie to talk about the job market in the Ghana area. "As the cybersecurity profession in West Africa is rapidly growing and the need for experts is high, we felt it would be of mutual benefit to engage our trainees in the (ISC)² chapter in Ghana," van der Stelt explained.

Maxim Nyansa co-founder Diana van der Stelt

From that initial interaction, the partnership developed. "Chapter members are willing to support Maxim Nyansa cybersecurity trainees in exam preparations for CISSP while they are also acquiring their first year of work experience," van der Stelt said. She adds that trainees are invited to chapter meetings and events. "Participating in network meetings of the chapter will give them valuable contacts." The chapter members also benefit, Cudjoe-Seshie believes. "It offers a direct opportunity to share our knowledge, skills and experiences with the next generation of cybersecurity professionals, thereby contributing to the growth of a pool of skilled individuals."

(ISC)² Ghana Chapter members

Chris Owusu-Ansah, senior associate in information protection and business resilience at KPMG

Chapter member Chris Owusu-Ansah had the opportunity to engage with some of the trainees. "[It] was indeed a privilege for me as a professional." Owusu-Ansah is a senior associate in information protection and business resilience at KPMG in Accra. "Their enthusiasm and curiosity were mind-blowing and the desire to know more and explore the opportunities that come their way was exciting to watch."

And there are plans for the future, according to van der Stelt. "In Ghana, we intend to train 10 to 20 new young cybersecurity specialists every year. (ISC)² chapter members will join European volunteer trainers in the next cybersecurity boot camp that is planned to start in Accra in September 2020." Cudjoe-Seshie also sees a positive impact. "It is a viable path to grow the membership of the chapter." ■

> **"Their enthusiasm and curiosity were mind-blowing and the desire to know more and explore the little opportunities that come their way was exciting to watch."**
>
> *—Chris Owusu-Ansah, (ISC)² Ghana Chapter member*

RETURN TO CONTENTS

Understanding the ‘P’ in CISSP

A veteran (ISC)² member on what it means to be a “professional”

BY WILLIAM K. CAMPBELL, CISSP

THE “P” IN CISSP is there very deliberately. It’s incumbent upon those who *profess* to be professionals to understand what we, as a *profession*, agree on what the term means, to do our level best to live up to the expectations of the profession and, of course, to use the term in accordance with the accepted definition.

In common usage, the word “professional” has taken on a simplistic meaning: a person paid for what they do. Indeed, professionals are in fact paid (often handsomely) for their work, but to be a professional in the sense that we use the word in (ISC)² is much more than that. To be granted entry into the association of professionals with the CISSP certification, a candidate must:

1. Demonstrate knowledge by passing the exam.
2. Attest to a minimum amount of education and professional experience.
3. Be endorsed by other professionals.
4. Not have a history of serious crime.
5. Subscribe to the Code of Ethics.

The first two points speak to proficiency and capability. It’s probably obvious to you that it would be unprofessional to take on an assignment that you lacked the knowledge or experience to properly complete.

Professionals hold themselves to a higher standard. They put the interests and needs of society, their principals and their colleagues ahead of their own.

The third and fourth points speak to reputation. We do not admit individuals into our profession unless another professional, personally acquainted with the candidate, will recommend the candidate. And we ask applicants to disclose any criminal history, which is reviewed by the (ISC)² Ethics Committee.

Finally, to *subscribe* to the (ISC)² Code of Ethics means that the professional makes a solemn commitment to abide by its ideals, both letter and spirit.

While professional ethics, as articulated in the code, are the core of our aspirations as professionals, there are additional ideals we associate with professionalism. Here are just a few examples of principles to which true professionals adhere:

- **Professionals are courageous.** They do the right thing even when their employer, client, friends or family are encouraging them to do something expedient. They will sacrifice employment, compensation, opportunities and friendships before sacrificing their principles.
- **Professionals hold themselves to a higher standard.** They put the interests and needs of society, their principals and their colleagues ahead of their own. They avoid even the mere appearance of impropriety.
- **Professionals don’t make excuses for ethical lapses or poor performance.** If we are busy, tired, ill, angry or frightened we account for that and step up, regardless. We accept the consequences for our decisions and actions. ■

WILLIAM K. CAMPBELL, *CISSP, is member of the (ISC)² Ethics Committee. This an excerpt from his article* Professionalism and Ethics for the CISSP, *2018.*

(ISC)² Code of Ethics Preamble

The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons

I. Protect society, the common good, necessary public trust and confidence, and the infrastructure.

II. Act honorably, honestly, justly, responsibly, and legally.

III. Provide diligent and competent service to principals.

IV. Advance and protect the profession.

RETURN TO CONTENTS

A Hollywood Production Company Tackles Remote Working

THE COVID-19 GLOBAL LOCKDOWN forced companies to secure an entirely remote workforce—and quickly. Among them was 250-employee, Los Angeles-based The Third Floor, which provides digital visuals for films in production.

Jeremy Oddo, director of technology at The Third Floor, explained in a webinar and subsequent Q&A with *InfoSecurity Professional* how his company was able to get back to work on highly secretive projects for clients like Marvel, Disney and Lucas Films in less than a week.

How did The Third Floor move to securely work remotely in less than a week?

For us, the crisis started a bit earlier than it did in the United States. We had just opened our first permanent office in Beijing. Once the virus started spreading beyond Wuhan, we closed the Beijing office and started a virtual communications plan. The lessons from that helped us deal with the situation in the U.S. as well as our London office. Importantly, we learned that we can be just as effective remotely as long as we have secure access to the internet. We worked diligently with our IT team and other experts to get the right systems in place to make that happen.

Why is it so important for your company to operate with secure remote access?

Secure remote access is essential because we're creating intellectual property. Our artists work with major movie and production studios every day to create the next blockbuster. We need to protect that IP while still enabling our artists to do their work.

What security model made this transition possible?

We adopted a zero-trust security model. Your employees only have access to the specific resources they need to do their jobs. Everything else on the network is invisible. This dramatically reduces the attack surface in the event of a cyberattack. With so many people working remotely now, we realized that attempted hacks would increase, so we had to mitigate that risk.

What specific technology do you find helped accelerate this process?

We used AppGate SDP to secure access. It enabled all of our employees to work remotely from their homes while maintaining the highest level of security required by our clients. This technology was more suitable for us than a VPN for quickly moving employees to a work-from-home scenario.

Getty Images

I think the positive takeaway is that you can do the seemingly impossible if you have the right tools, partners and leadership. We've learned how to adapt while preserving our creativity and culture.

What concerns did you have around remote access?

We were concerned about security and ease of use. We needed to make security a priority without inhibiting the team's efforts. We were able to accomplish both with this particular software-defined perimeter solution.

How will this impact the future of Hollywood blockbuster production?

I think the positive takeaway is that you can do the seemingly impossible if you have the right tools, partners and leadership. We've learned how to adapt while preserving our creativity and culture. This should give us greater opportunities to support production requirements in the future—no matter where our customers or employees are located. ■

Wearing it with Pride

A chance meeting demonstrates the power of our (ISC)² credentials

by Tony Vizza, CISSP, CCSP

MY INTEREST in IT began in second grade. The teacher did not know how to use the single Apple computer we had in our classroom, so I ended up teaching her. From there, computer studies became my focus, through high school and college and my post-university jobs.

In 2014, I settled on a career in cybersecurity when I had the opportunity to work with Symantec through the University of Sydney's Executive MBA program, which also included a stint at Stanford University in California's Silicon Valley. This marked a significant turning point for me. It was during this time that I met George Maculley, who was Symantec's director of product management and particularly knowledgeable about cybersecurity. George and I struck up a conversation and he gave me his business card: George Maculley, CISSP. I connected with George on LinkedIn. Once again, he was listed as George Maculley, CISSP.

At this stage of my career, while I was aware that cybersecurity certifications existed, I didn't know much about them—what they meant and which were recognized by the industry as valuable. Meeting George changed that.

I resolved to find out what that "CISSP" thing that kept coming up at the end of George's name was all about. I did my research. I learned that achieving the certification was challenging and that it would be an invaluable asset to my cybersecurity career.

Tony Vizza, CISSP, CCSP, is the Director of Cybersecurity Advocacy for (ISC)²'s Asia-Pacific region and is based in Sydney. He can be reached at tvizza@isc2.org.

It took almost a year after meeting George to take the path he unknowingly set me on. Being told by the official at the Pearson VUE testing center that I passed the CISSP exam remains, to this day, one of the proudest moments of my professional career. Little did I know that, a few years later, I would be working for the association that administers the CISSP, among other certifications, and would be an advocate for cybersecurity across the Asia-Pacific region.

Gaining the CISSP has broadened my horizons. I completed my CCSP cloud security certification and a number of other certifications. I'm studying for a privacy-related certification and am also pursuing a law degree in the interest of cyber law. I have written articles, presented on cybersecurity countless times, was involved in numerous audits, assessments and incident responses and have counseled men and women in careers in cybersecurity.

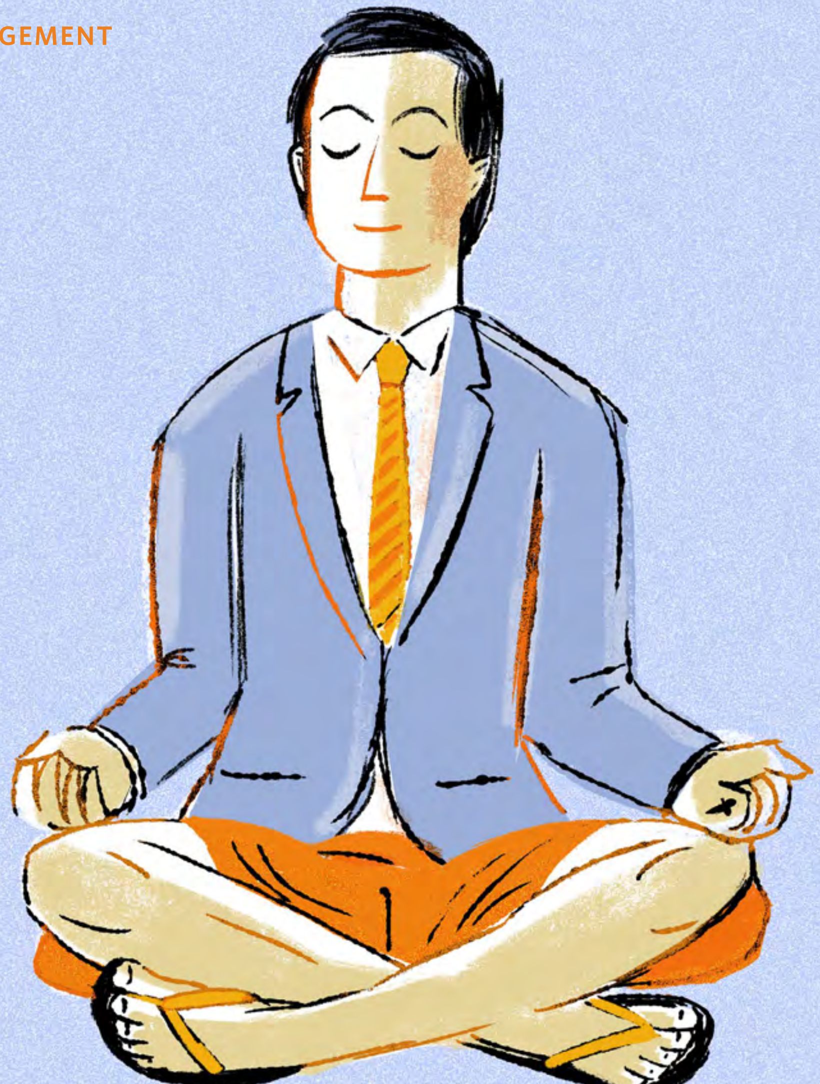
> **I learned that achieving the certification was challenging and that it would be an invaluable asset to my cybersecurity career.**

This journey continues to be amazing. And it all started by meeting George Maculley, CISSP. If it were not for George proudly and loudly wearing his CISSP, who knows where I would be working today.

Those who know me know that I wear my CISSP and CCSP certifications with pride. They are on my business card, my email signature and on my LinkedIn profile. My certifications are listed in my presentations, in my articles and I mention them in podcasts. I wear my lapel badges on my suit jacket.

If showing off my certifications with pride piques the curiosity of just one person to help them discover their interests and decide on joining our industry, it has been well worth it. I encourage you to do the same. ■

RETURN TO CONTENTS



UNDER PRESSURE. UNDER CONTROL.

How to stay sane and manage stress during a most unusual time, no matter where you live and work. BY DEBORAH JOHNSON

EVERY DAY, cybersecurity professionals face pressure, from the daily demands of protecting data and people's privacy to the worst-case scenarios of a breach's financial and reputational repercussions.

That's nothing we didn't already know. But what's changed in the past six months is the level and severity of those demands since the world's response to COVID-19 required companies, citizens and cybersecurity professionals to abruptly pivot in almost all ways.

"Security professionals are very aware of what the risks are."

—Lucie Hayward, CISSP, CISA, PMP, senior vice president of cyber risk, Kroll

"For a lot of folks, it's losing focus. They're working really hard, but they're not really being effective with their work."

—Leah Aguirre, licensed clinical social worker

"Many of the clients that I see have anxiety about performance ... whether or not they're meeting their marks."

—Kevin Chapman, clinical psychologist

"Is there any way you can work smarter? Increasing your exercise, turning to people you're close to for support. Perhaps taking up meditation."

—Melanie Greenberg, Ph.D., clinical psychologist

Managing added levels of stress takes some internal assessment: What's causing it? What can I do about it? Do I need professional help? And how do I determine what stress reducers work best for me?

RECOGNIZE THE SIGNS

Even before a pandemic forced a new way of life, cybersecurity leaders were feeling the pressure. Of 400 CISOs surveyed prior to the coronavirus outbreak for The CISO Stress Report 2020 commissioned by London-based Nominet, 88% considered themselves to be under moderate or high stress.

"Security professionals are very aware of what the risks are," says Nashville, TN-based Lucie Hayward, CISSP, CISA, PMP, the senior vice president of cyber risk at Kroll. "A good security professional is always ahead of the latest news, trends."

The responsibilities at work can sometimes overwhelm and lead to frustration, says Leah Aguirre, a licensed clinical social worker and psychotherapist based in San Diego. "For a lot of folks, it's losing focus. They're working really hard, but they're not really being effective with their work."

Psychologists and other clinicians offer clues that your stress level may be entering dangerous territory:

- Difficulty in concentrating, inability to retain information
- Constantly worrying, expecting the worst
- Feeling isolated

Everyone experiences these symptoms at some point in their life or career. This includes cybersecurity professionals pressed into action to lock down systems without locking out remote workers during sudden shutdowns.

Anxiety on and about the job tops the list of symptoms, says clinical psychologist Kevin Chapman. "Many of the clients that I see have anxiety about performance, whether that be social, or negative evaluation from superiors or colleagues, whether or not they're meeting their marks." The anxiety is also carried home, adds the founder and director of the Kentucky Center for Anxiety and Related Disorders in Louisville. There's "also the financial reality of needing to provide for their families."

The challenge is how to manage the stress associated with chronic or acute anxiety.

TAKE CHARGE OF YOURSELF

The Nominet survey revealed 48% of CISOs reported stress had affected their mental health, and 35% said it affected their physical health.

"Is there any way you can work smarter?" clinical psychologist Melanie Greenberg, Ph.D., based in Mill Valley, CA, asks. "Increasing your exercise, turning to people you're close to for support. Perhaps taking up meditation."

Greenberg, author of *The Stress-Proof Brain*, says that while you may not be able to change your workday, you need to "try to be a little bit creative" to make time for yourself, such as finding somewhere to eat your lunch

RETURN TO CONTENTS

rather than at your computer.

Aguirre, the licensed clinical social worker, agrees. "If you're sitting at a desk all day long, it's good to have a change of scenery. Go for a walk." And, she advises, don't forget to eat regularly and drink lots of water. "People neglect their appetite and basic needs when they're stressed, focusing on prioritizing work."

The American Psychological Association suggests an online tip sheet to adequately respond to increased stress. "It's not always possible to escape a stressful situation or avoid a problem, but you can try to reduce the stress you are feeling," an APA web post says. "Evaluate whether you can change the situation that is causing you stress, perhaps by dropping some responsibility, relaxing your standards or asking for help."

Making time for yourself can help manage the stress:

- Find personal outlets, such as exercise, meditation, diving into a new hobby like crafting or model building—all to engage you beyond work.
- Break up the day when possible with mini exercises and walk breaks.
- Eat lunch somewhere other than your workstation.
- Don't forget to eat regular meals and drink lots of water throughout the day.
- Analyze the stressful situation for options.

Fortunately, these can still be done when ordered to shelter in place to help stop the spread of a killer virus. But the sudden disruptions COVID-19 caused and the ongoing fallout, especially for those on the front lines, can make it difficult to follow these simple-yet-proven tactics.

If you continue struggling to manage your stress and address your anxiety, it's likely impacting your personal relationships and job performance—creating the exact conditions you want to avoid. According to the Nominet survey, nearly a third of CISOs reported that stress affected their ability to carry out their jobs, up from just a quarter in the previous year's survey. (This figure likely has risen since the pandemic hit businesses in a big way.)

UNDERSTAND 'OFFICE' DYNAMICS

Whether you're a manager or a team member, knowing what is expected of you, as well as your expectations of others, is another key to handling stressful situations.

As a manager, all eyes are on you.

"Whatever your title is, people are looking to you to be calm, logical, provide answers," Ping Look, a senior director of Microsoft's Detection and Response Team in Seattle, says.

There also are those who may take on too much.

"It becomes overwhelming. People want to 'boil the ocean'—'I want to solve all the problems, all the time.'" What's necessary, advises Look, is prioritization. "What's really important [is] ensuring that your workforce has what it needs. In the end … you have accountability for your decisions, and you have to think about the meaningful impact that you're making."

"Whatever your title is, people are looking to you to be calm, logical, provide answers."

—Ping Look, senior director of Detection and Response Team, Microsoft

Communication is another key to helping ease the stress. As a manager, Kroll's Hayward advises: "Definitely make sure that you are planning for employee communications and how you're going to keep them in the loop."

Share your plans with the full staff, she adds, even those who are not directly involved in a crisis but who are worried about completing their own assignments and even getting paid. "Really be transparent with employees to the extent that you can. They should be reassured by their employer that you've got things under control."

Team members, says Microsoft's Look, also need to have an open line to managers by keeping their leadership informed and communicating things, such as "This is what we're doing and this is how we're accomplishing everything."

But what if things are not working out? "It is unfruitful to just complain and say, 'We just can't do it.'"

The better course, she advises, is compromise. "Speak with your managers. Speak with your peers. Compromise to come to a solution." But beware, she adds, of the "blamestorm—people finding something to blame."

And, finally, learn to let it go. "There is a moment when you have to say, 'OK, we're just going to move forward. I'm going to do the best with what I have,'" Look advises.

When a major incident occurs, a key action to help manage stress is to show coordinated leadership, advises Diana Contesti, CISSP, chief operating officer, DL Consulting. When leadership isn't clear, "the stress level for the team goes through the roof because they don't know who to listen to." Once team members know "who they are supposed to take directions from, the tech team has one less stressor."

THE HOME OFFICE TRAP

Even before the COVID-19 pandemic, working from home was a growing trend. A 2019 survey by the International Workplace Group revealed that 54% of the 15,000 profes-

RETURN TO CONTENTS

sionals who responded from different industries worked remotely at least 2.5 days a week.

By the time the novel coronavirus spread across the globe in the first quarter of 2020, companies large and small sent many, if not most, of their employees home to work.

Working from home has unique challenges and stressors. It requires structure and balance.

"If you have a family, there are so many distracting things," Aguirre says. She urges setting up a daily routine. "It's hard to stay motivated without routine and structure. People aren't showering as often because they don't need to. Wearing pajamas all day … those things make it hard to stay motivated and focused."

Also crucial, she says, is a dedicated workspace. "I know a lot of people who will answer work email from bed and the thing about that is that your bed becomes associated with work. Your bed is supposed to be for rest and sex. It's supposed to be where you decompress. We have all this technology that allows us to work from anywhere, including the bedroom, that can create a weird, blurred boundary between work and personal life."

Another stress-inducer when working from home is getting work done, warns Greenberg, the clinical psychologist. "There may be some less accountability at home. Meetings may not be as productive. Sometimes people may be doing something else during the meeting." A solution, again, is structure. "Set specific goals for yourself—and for your team as well, such as 'What do we want to accomplish this week?'"

WHEN HELP IS NEEDED

For some (perhaps many) professionals, self-help might not be enough. Psychologist Kevin Chapman says there are clear warning signs. "When

4 REASONS YOU MAY BE STRESSED OUT

EVEN BEFORE THE PANDEMIC, cybersecurity professionals were experiencing record levels of stress on an ongoing basis, just in the course of doing their jobs. Chronic stress not only takes a physical toll, but it can ruin relationships at home and at work. Which, of course, just adds to the anxiety and pressures. Here are some reasons why we are so stressed now.

1. Resource Shortages

More than half of CISOs surveyed by Nominet do not believe they have enough resources to address security vulnerabilities, let alone address expanding threat vectors. This is supported by the 2019 (ISC)^2 Cybersecurity Workforce Study, which reported a global workforce shortage of more than 4 million cybersecurity professionals.

2. Internal Pressures

Cultural battles directly contribute to security job stress. According to an ESG-ISSA Life of Security Professionals Report, 38% of cyber pros say they're frustrated with trying to educate end users to change their behaviors.

Additionally, pressure comes from the top. The Nominet survey revealed that 94% of 400 C-suite respondents said their CISOs could do a better job at demonstrating their value. Meanwhile, 29% of CISOs said dealing with the board of directors is one of the most stress-inducing parts of the job.

3. Overwhelming Workloads

Incredibly, 73% of security practitioners surveyed by the Ponemon Institute say an ever-increasing workload is causing burnout. That suggested three out of four of members is really struggling with finding joy in their jobs.

The overwhelming majority of cybersecurity pros (88%) admit that they work more than 40 hours each week, according to the Nominet study. Another 71% say that the 24/7/365 nature of security is "painful."

The stress leads to dissatisfaction with the job or organization, with 65% of security analysts considering a job or career change due to workload pressures.

4. Mental Health Risks

Some 48% of CISOs in the Nominet study revealed that stress had impacted their mental health, and 23% reported turning to medications and/or alcohol to help.

WHAT YOU CAN DO

Recognize you need a break.

"You owe yourself a break to take care of yourself in order to do what you want to do and succeed at the goals you're after."

—Leah Aguirre, psychotherapist

Take a step back.

"Take a broader view. Are you seeing only the negative? Meditation can help the way you relate to everything. With regular meditation, you're less fussed with your worries because you can be in a calmer state."

—Melanie Greenberg, clinical psychologist

Be aware of changes in yourself or others.

"The red flag is when there's a significant change in the normal, day-to-day interaction with others. Personality shifts, changes in behavior, productivity changes—those are moments to intervene."

—Kevin Chapman, clinical psychologist

—D. Johnson

RETURN TO CONTENTS

anxiety meets a threshold and crosses it to the point that it’s messing up things like sleep, concentration, ability to eat, fatigue and a whole host of symptoms, that’s when it crosses over into getting professional help.”

> **“When anxiety meets a threshold and crosses it to the point that it’s messing up things like sleep, concentration, ability to eat, fatigue and a whole host of symptoms, that’s when it crosses over into getting professional help.”**
>
> *—Kevin Chapman, clinical psychologist*

Other signs to watch for, adds Aguirre, include “being consumed by thoughts related to work. Having less interest in things you used to enjoy. Not engaging with your support system.”

Chapman adds that it might take more to get someone to seek help. “In most work settings, and I know that cybersecurity is no exception, it’s a very team-driven work environment that requires everyone to participate.”

The cybersecurity professional’s world—from data breaches to daily maintenance—is rife with stress land mines that each of us should avoid or address when we encounter them. As Microsoft’s Ping Look reminds us: “Sometimes people get bogged down with the assumption that just because they work in a technology field, it’s really about software, hardware, machinery. But it does come down to a people business.” ■

DEBORAH JOHNSON *edits Field Notes and columns for* InfoSecurity Professional. *Her last feature for the magazine, which appeared in the September/October 2019 issue, was on how to avoid a layoff.*

RETURN TO CONTENTS

The No.1 Training Myth?

All certification trainings are endorsed by (ISC)².

It's true that many training companies offer exam prep for (ISC)² certifications. But did you know not all of them are affiliated with us? To protect your investment, choose an (ISC)² Official Training Provider.

FACT In addition to offering our own training, we partner with leading training providers around the world, so you and your team have convenient access to official courses. All instructors are verified security experts, authorized by (ISC)² to deliver the most relevant, up-to-date course content developed by (ISC)².

Enlist an Official Training Provider in Your Region

North America

Asia-Pacific

Latin America

Europe, Middle East, Africa

Beware of training myths…
If you're ever in doubt about a provider's status, check our website.

CISSP. SSCP. CCSP. CAP. CSSLP. HCISPP.

(ISC)²® TRAINING OFFICIAL PROVIDER

KEEPING YOUR CUP FROM OVERFLOWING

Understanding stress models can build a more resilient, higher-performing workforce—even during 'black swan' events

BY MICHAEL M. HANNA, CISSP

DEFENDERS OF THE CYBER DOMAIN carry a significant weight because of the demands placed upon them. In addition to the technical skills needed to protect companies and entire communities, cybersecurity professionals must have the know-how to protect information systems and data that support national security requirements, critical infrastructure and/or sensitive customer details. Our actions directly serve to protect and support our families, significant others, friends and colleagues. These responsibilities surely carry a weight for us all and incur considerable stress. How could they not?

The stressors we experience on a daily basis can influence our well-being, on and off the job. Compound these daily stressors with "black swan" events such as the COVID-19 pandemic, and we have a recipe for significant mental hardships.

ILLUSTRATION BY ENRICO VARRASSO

RETURN TO CONTENTS

Inappropriately managing stress within security departments and teams invites unwanted consequences and results. Organizations may suffer from decreased levels of trust, lower performance and productivity, and higher instances of illness among employees. This, in turn, may result in higher risks to the organization and its employees.

Life hacks provide some benefits in managing stress through high-level tips, but by truly understanding stress models founded in psychology, leaders can establish appropriate practices and promote behaviors to better support the wellness of their cybersecurity professionals.

CRUSHING WORK CONDITIONS

Stress does not discriminate based on job ranks. It affects all levels of the team and is caused by different concerns and responsibilities. A report by ESG indicated that more than 36% of cybersecurity professionals are stressed from their workloads, communicating with business leaders, ineffective collaboration between security and other departments, and keeping up with security demands across IT initiatives. The latest CISO stress report from Nominet depicts a very concerning and disheartening picture of CISOs' well-being. According to the study:

- 88% believe that they operate in a moderate or high stress environment
- 48% stated that their encountered levels of stress have negatively impacted their mental health
- 35% stated that their encountered levels of stress negatively impacted their physical health
- More than a third admit missing a family vacation, child's event, or major family milestone

While any professional can suffer from chronic stress, those in cybersecurity may pay a higher toll if relentless or acute pressure is not relieved. By understanding how stress functions, we can mitigate the mental anguish, physical health decline, interpersonal tensions and reduced productivity that are common in our profession.

DIATHESIS-STRESS MODEL

Diathesis refers to an individual's susceptibility to developing a pathological state. According to research, most diathesis-stress models agree that neither a person's diathesis nor prior experiences to stress are enough to produce a disorder or psychological event on their own. Think of a spark as stress, oxygen as diathesis and a fire as the psychological event. The presence of both stress and diathesis are necessary to develop mental health issues, burnout, and poor or decreasing job performance.

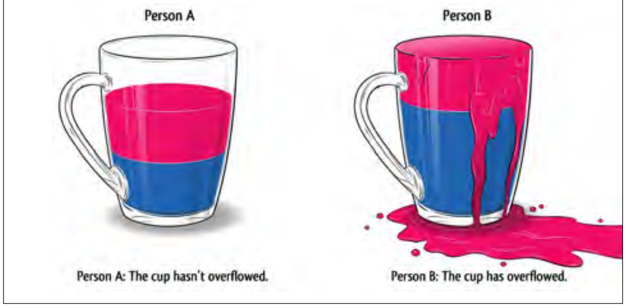
A person's diatheses include genetic, physiological, cognitive and behavioral factors. Physiological and psychological stressors are common during major life disruptions, such as a death in the family, divorce or financial insecurity. For cybersecurity professionals, stressors may come from unreasonable executives, long hours at work resolving an information assurance event, or the constant belief that the security of the organization is solely up to you.

A great way to visualize the diathesis-stress model is with a simple analogy *(see Figure 1, below)*. Let's assume that Cup 1 represents Person A and Cup 2 represents Person B, with both cups holding the same volume of liquid initially. Assume that Person A is less vulnerable to entering a pathological state than Person B. Think of diathesis as the blue-colored fluid in the cup. Since Person B has a higher level of vulnerability, they have more fluid at the bottom and less remaining space in the cup. Next, let us assume that both individuals encounter the same level of stress (pink-colored fluid), but since Person B had a higher level of diathesis (vulnerability), their cup overflowed, and a psychological event occurred. From this analogy, Person A's cup did not overflow, and they were able to handle the stress event. Two things to keep in mind here. First, a stress event can be a prolonged period of experienced stress or a singular event. Second, this is a very simplified explanation of the theory, but it helps drive home the point represented by Figure 1.

The diathesis-stress model also has been used to explain common conditions such as insomnia, depression and anxiety, all of which may have been experienced by cybersecurity teams. Ask yourself: When was the last time you had difficulty falling asleep or staying asleep because of the demands placed on you as a cybersecurity professional or your personal life? For anyone in the thick of it, the response is likely: "Very recently."

With this stress model, acute insomnia and the harm it inflicts is influenced by diathesis components such as cognitive, behavioral and environmental factors. Cognitively, we

FIGURE 1 **REPRESENTING DIATHESIS-STRESS WITH THE CUP ANALOGY**


Person A
Person B
Person A: The cup hasn't overflowed.
Person B: The cup has overflowed.

may toss and turn in bed worried about a breach or internal forensics investigation. Environmentally, we may look through our phones or tablets while in bed in the name of needed research. Neither of these activities quiets the mind enough to doze off to sleep. And, if too many evenings go this way, it becomes more difficult to break the cycle, thereby causing more harm to both body and mind.

KEEPING THE CUP FROM OVERFLOWING

Although genetics and predisposed conditions influence diathesis, scientists believe diathesis may be changed over time. But we do have more immediate control of the stress component of the diathesis-stress model. Don't get me wrong though: Taking actions to mitigate against personal vulnerabilities, such as speaking with a mental health specialist, can go a long way. Going back to the cup analogy, managing stress is like scooping out portions of the pink fluid with a spoon and discarding it over the side before the cup overfills. If we handle stress appropriately, we keep the cup from overflowing and maintain our well-being.

So, how can we each create an environment that fosters flow and reduces stress. According to Paul Zak, the founding director of the Center for Neuroeconomics Studies and a professor of economics, psychology and management at Claremont Graduate University, we need to create a high-trust environment. This involves a company's leadership building and maintaining a culture of trust throughout the entire organization.

In examining these high-trust organizations, researchers have found:

- 74% of employees experienced less stress
- 50% were more productive and 29% expressed higher job satisfaction
- Sick days dropped by 13% and self-reported employee burnout by 40%

The next question we must ask is: How do we promote a high-trust environment? Building upon Zak's recommendations and incorporating various psychological principles, cybersecurity teams can promote high-trust environments by doing the following:

- **Inducing stress through work challenges that are both achievable and meaningful**. Achieving meaningful challenges also improves self-efficacy and may result in other benefits, such as increased performance.
- **Allowing for autonomy and job crafting.** Cybersecurity professionals should be given freedom to operate within their job descriptions and volunteer for projects that interest them. The Job Characteristics Model delineates that autonomy and task significance (belief in the importance of work) have been shown to improve employee performance.
- **Focusing on relationship building.** The chemical reactions from social belonging have been shown to reduce stress, increase performance and improve well-being. Building relationships aligns with Maslow's Hierarchy of Needs and the Existence, Relatedness and Growth models that express the importance of human belonging.
- **Promoting whole-person development.** High-performance psychologist Michael Gervais points out that as human beings we can improve physically, mentally and in our trade. Undoubtedly, the cybersecurity community places great value in improving our craft, but very little in our physical and mental development, which are important in achieving high performance and well-being.

One thing that I enforce is a "Wellness Day" in which my team members are allowed to take one day off each month to do whatever wellness means to them. It could be spending time with family, going out for a massage, or taking a long bike ride. I must advise against changing the name because it diminishes the intent of the day. Don't be afraid to stand up for whole-person development.

POSITIVE PSYCHOLOGY AND FINDING YOUR FLOW STATE

Positive psychology focuses on enhancing the individual or community through all aspects of life, and it aligns with some of the examples we have discussed. Within positive psychology, a flow state is the feeling when you are in the zone and performing at your highest level. You are fully focused and immersed only in the present. It feels like nothing else is going on except for what you are doing at that moment. It's our highest performing state. We all would love to be in a constant state of flow, but that's not practical nor sustainable. Top athletes and performers only spend a fraction of their time in flow state because of several factors, including the difficulty of achieving flow. Figure 2 (*see p. 27*) provides a graphical representation of the challenges and skills that must be balanced for cybersecurity professionals to achieve flow.

To help promote flow for yourself and your security teams, it is beneficial to:

- Have and delineate concrete goals.
- Pursue activities, projects and jobs that you enjoy.
- Ensure that work is appropriately challenging and based on skill.
- Give yourself and your security team the opportunity to fight through challenges and develop.

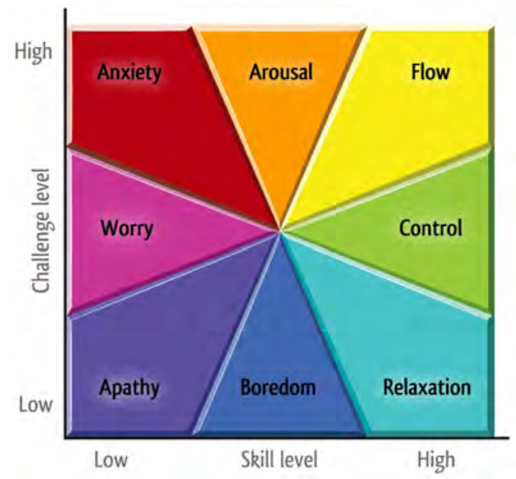
WHAT NEEDS TO BE 'STRESSED'

If you are in a leadership position or have direct reports, challenge yourself to promote an environment of high trust, focus on relationships instead of solely being task-driven, and develop teams that consider everyone's well-being before, during and after a stressful event, or series of them.

We are certainly faced with a workforce shortage that naturally induces stress. Add in unique events like the anxiety-inducing pandemic we're all living (and working) through, and it's no surprise stress levels are at an all-time high.

Like a fixer-upper home, sometimes the best results come from refining and improving an existing structure, rather than just tearing it down and starting from scratch. Build on what you have, within your teams and within yourself. Personally challenge yourself to develop more than just your trade craft. Push to improve physically and mentally. The benefits of whole-person development are significant and will bring out the best in you and your teams, while contributing to your well-being. ■

FIGURE 2 **FLOW STATE MODEL DIAGRAM**



MICHAEL HANNA, *CISSP, is a member of the U.S. military. 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.*

Need (ISC)^2 Training in EMEA?

Official Training Providers are there to keep you moving forward.

If you are based in EMEA and pursuing an (ISC)^2 certification, (ISC)^2 Official Training Providers are there to help keep goals on track. We partner with leading training providers around the world so you have convenient access to official training that fits your location and schedule.

All instructors are verified security experts, authorized by (ISC)^2 to deliver the most relevant, up-to-date course content developed by (ISC)^2.

Official Training Provider Services include:

- Training and exam voucher packages
- Training in local time
- Delivery options such as bootcamp-style, face-to-face classes and online training
- Accept payment in local currency (check with your local provider)

Find a Training Provider in Your Region ⊳

(ISC)^2 is there for you too! | **Contact us at +44-203-960-7800 or info-emea@isc2.org.**

WE NEED TO HAVE A SERIOUS TALK

BY PERRY CARPENTER

EPISODE 2 (SECOND IN A SERIES):

TROJAN HORSES FOR THE MIND

I think I know how we can do that.
We just have to get them to care.
I'm listening, Katie.

PREVIOUSLY IN THIS SERIES:

Two days ago, Acme Corporation suffered a data breach. During the initial investigation, Mike, an IT security manager, and his team discovered that the cause tracked back to a phishing email that slipped through email filters … and that their CEO, Jerry, just happened to click on. Now, Acme Corporation's CISO, Jim, along with Mike and his team are on a quest to determine what happened and what lessons they can learn from the event.

Did they already have a security awareness program in place? Of course they did. But it had some fatal flaws that will soon be uncovered.

THURSDAY 1:55 P.M.
ACME CORPORATE HEADQUARTERS

"It's time," Mike said, poking his head into Krish's cubicle.

"OK. Good timing. Katie and I just finished correlating the end user awareness survey results. You guys aren't going to like them," Krish said as he stood and grabbed his laptop. "I just texted Katie to meet us in Jim's office."

Just as Mike and Krish reach the CISO's office door, Katie scooted up whistling "Whistle While You Work" from Disney's *Snow White and the Seven Dwarfs*.

Mike stopped before opening the door and gave her a look of mild irritation. "Why must you whistle that song all the time?"

"It's not all the time. Only when I see you two. I've got names in my head for each of you, but I'll keep those to myself," Katie deadpanned. She looked around dramatically before hunching her shoulders and conspiratorially lowering her voice to a stage whisper, "because HR is listening."

Then, straightening her body and snapping back to regular volume, she said: "Now let's go in and get this over with."

ILLUSTRATION BY TAYLOR CALLERY

RETURN TO CONTENTS

"So, what's the status?" an anxious Jim asked the trio as the door closed behind them. "Do we have any idea why?"

"You mean, why people aren't doing the things we hope they'll do after completing our security awareness training?" Krish asked.

"And why they keep doing the things we don't want them to do ... even after they complete our training?" Katie chimed in.

Not to be outdone, Mike added, "And why they do—or don't do—all those things even when they've signed policies that clearly outline what they should do, what they shouldn't do, and who they should talk to if and when they feel like doing the things they shouldn't do? Or when they don't want to do the things that we want them to do?"

"Um ... yeah," Jim responded, "Like maybe why our CEO ended up as the poster child for all of those things?"

"So, here's the deal," Krish started. "The surveys indicate that they know the things that we are training on. They're just not acting on them."

"Right." Katie said. "They're aware, but they don't care."

"Wait!" Jim interrupted. "You can't say that our CEO doesn't *care*. I can't tell Jerry that our root-cause analysis uncovered that he just didn't care enough to do the right thing."

Katie continued, "Well, yeah. That *is* actually what I'm saying; although he may truly *believe* that he cares. Let me explain. We clearly see that people are pretty familiar with what a phishing email looks like. And, yes, Jerry even passed the quiz at the end of our training module on phishing."

"So, I still don't get what you are getting at," Jim interrupted. "We let them know what's expected, and then they just decide not to do it? Even when it's an understood part of their job? Even our *CEO???*"

"What I'm getting at is actually pretty simple," she responded. "We've got two problems. First, the information we give doesn't feel relevant and is sometimes quickly forgotten—and, yes, sometimes even ignored. Second, even when people intend to act on the information we provide, they just don't do it when it counts. That's what our survey results are telling us. And those findings seem to be consistent with some research I've been doing into learning science and behavioral science. Traditional awareness programs really didn't account for either of these."

"Any thoughts on how to fix this? What we should be doing differently?" Mike asked.

Krish's hand shot high up in the air as if trying to desperately catch the attention of a favorite teacher. *"Ooooo.* Pick me!"

Jim and Mike sigh in unison, then humor their colleague by formally calling on him.

"Thank you. We just have to get them to care about things that they don't care about and do things that they don't normally do. Easy peasy," Krish said as he sat back in his chair, smiling.

"I think I know how we can do that." Katie said, pausing for effect. "Jim, who do you know in our *marketing* department?"

WELCOME to our second installment in a series all about building transformational security awareness programs. As we just read, Jim, Mike, Katie and Krish have uncovered the fundamental truths that I briefly mentioned in the first installment. Specifically, they came up against what I call the *Three Realities of Security Awareness*. They are:

1. Just because I'm *aware* doesn't mean that I *care*.
2. If you try to work *against* human nature, you will *fail*.
3. What your employees *do* is way more important than what they *know*.

In our security awareness programs, human nature reigns supreme. We can't expect humans to behave like anything other than humans. And, let's face it, most traditional security awareness programs seem to be built on the assumption that people are like computers.

Such programs operate on the premise that if you give people the right information, they will naturally assimilate and adopt the associated beliefs and actions. That approach is, of course, poppycock. And we have decades' worth of data breaches to prove it.

INFORMATION ALONE IS NEVER ENOUGH

Even the old G.I. Joe public service announcements said that "Knowing is half the battle." So, what's the other half? This brings us back to the *knowledge-intention-behavior gap* that I mentioned in the last issue. If knowing is half, then the remainder is intention (caring) and behavior (action). I'll touch on the intention/caring part and then pick up the behavior aspect in the next installment.

When it comes to information, we face a few problems. First, our ability to retain information from training is horrible. If not immediately applied in some practical way, we will quickly forget up to 90% of the information presented to us during training events.

This retention issue is referred to in learning science as the "decay of knowledge." And so, here is the dismal truth: When we do once-per-year awareness programs, we are setting ourselves up for failure.

As an example, even if your training program has the

RETURN TO CONTENTS

best advice in the world about how to create and remember good passwords, your efforts will be futile because the vast majority of your people won't need to change their passwords that day. And so, they will quickly forget your best practices because their minds filed that information in the bucket labeled "Irrelevant."

So, one way to immediately increase retention is to conduct training at points in time when the information is directly relevant to the employee. And, when that isn't immediately possible, you can increase retention by conducting simulations so that employees can put the knowledge to use.

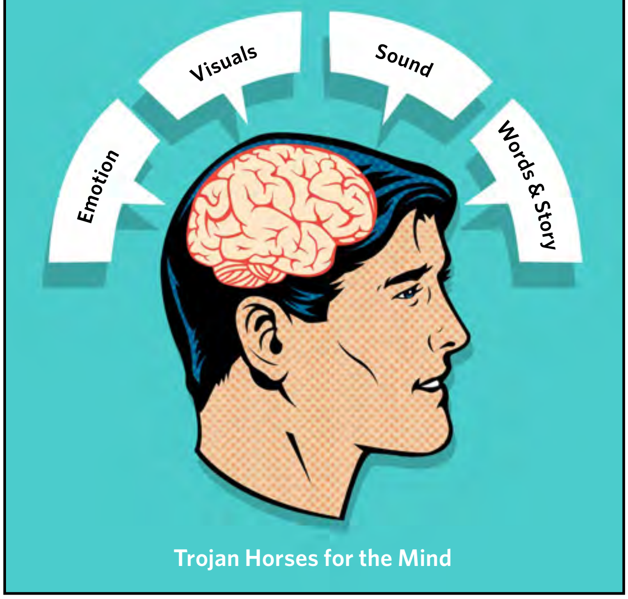
You can also work to craft your information delivery (messaging) in ways that will dramatically improve your chances of creating the associated beliefs, value systems and internal motivations that you seek. And you can do that with the help of what I call Trojan Horses for the Mind.

MAY THE 'HORSE' BE WITH YOU

In my book, *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors*, I describe four trojan horses for the mind. *(See Figure 1, below.)*

People have a really hard time caring about things that feel irrelevant, distant and removed. So, if something feels like it is just data or information, it's likely that they just won't care. And if they don't care, they won't remember or act on that information. So, how do you make people care? You need to find a hook. And that's where the trojan horses come in. Let's quickly think through each of these four horses.

FIGURE 1 **WAYS TO HOOK USERS INTO FOLLOWING SECURITY BEST PRACTICES**



Trojan Horses for the Mind

Source can be found here.

YOUR HOMEWORK

1. Pay attention to all the different things that are being "marketed" to you. How are each of the trojan horses being used? How are they used in your favorite ads?
2. Write down your five favorite TV commercials. Find the story and emotion within each of them.
3. Pay attention to the great stories that you encounter in TV, movies or books. What commonalities do you see?
4. Spend time parsing the ways that visuals and sound/music are used in marketing and in other storytelling modes. What patterns/commonalities do you notice?
5. Now review your critical security awareness messages. Choose three critical messages and brainstorm ways to apply the trojan horses to make these messages meaningful. If you were an advertising agency, how would you advertise the security values associated with these three critical messages?

STAY TUNED

In the next episode, we'll be diving into the world of behavioral science and behavioral design. I'll introduce you to a few behavior models, including the Fogg Behavior Model and Nudge Theory. I'll also show you specifically how to use those models to work with human nature rather than against it. ▪

—P. Carpenter

Emotion: If you can tie your message to a feeling, then it will be memorable. However, resist the urge to only tie information to positive, happy feelings or only using humor to make your messages feel more relatable. Why? Because if you can add a mix of emotions (like moving from happiness to tension, fear, sadness, etc.) then you have an even greater chance of making the message relevant. Psychologically we are wired to remember the lessons of things that take us below our emotional baseline because those things tend to be more critical to our survival.

Visuals: We can pack *a lot* of meaning into a simple visual. That's why logos and branding are so important to organizations. Images are like a compression algorithm for our minds. We see them and instantly unpack all the rich meaning that has been encoded in them. And this can also include any history, emotion or stories that we've associated with the image.

Sound: Sound can be powerfully leveraged to aid in memory, or to convey/enhance emotion. Additionally, it is very easy to encode messages within sound … like that Spice Girls song that you *really, really want* to get out of your head.

Words and Story: Since the dawn of human history, we've learned and passed down information through story. Story draws us in. It gives us characters and situations to care about. And great stories implant values within us. They have the capacity to shape the way that we think about and interact with the world around us. That's why morality tales, parables, fables and children's educational programming all use stories and characters.

So, guess what field uses all these tactics effectively? Just as our character Katie suggested, it's marketing. And that leads us to our homework (*see p. 31*). ■

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

HAVE A QUESTION FOR PERRY?

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

RETURN TO CONTENTS

Award-winning Garfield Programs Now Available at Home

by Pat Craven

IT IS HARD TO BELIEVE, but this October marks four years since we launched the first in the popular series of *Garfield's Cyber Safety Adventures*. While I have acquired more gray hair thanks to this lazy cat, he hasn't changed a bit. Nor has the importance of the more than 100,000 internet safety lessons he and his friends provide each year.

In 2016 and 2017, we created Garfield-inspired lessons on privacy, safe posting and cyberbullying. All three have won multiple educational awards, including the Teachers' Choice Award for the Classroom, the Smart Media Academics' Choice Award, the Modern Library Award, and most recently, the Mom's Choice Award.

What makes the program so successful is how easy and comprehensive it is. The Educator Kit is full of everything a teacher or group leader needs to teach internet safety to 30 children at once. It incorporates all the ways that children (and adults) learn. They love watching the educational cartoon, listening to the leader, discussing the topics, taking the quizzes and reading the comic book, all of which helps assure kids retain the messaging.

When the COVID-19 global outbreak forced families to shelter in place, and children to learn from home, we began offering free online lessons as our way of giving back. The response has been overwhelming, with thousands of families using the basic online program. The feedback was so positive that we decided to do a total makeover of our digital offering. Now, we are thrilled to be rolling out a new and exciting online program that meets children's online safety needs and works anytime, anywhere.

The Garfield at Home program is available on a subscription basis to individual children or families. Each subscriber receives a secure link and password-protected access to digital materials for all the lessons. There are three levels of subscriptions you can now receive.

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

Intro Level

- Access to a new online platform
- Three interactive *Garfield's Cyber Safety Adventures* cartoons
- Digital badges
- Monthly parents newsletter with new tips and activities aimed at keeping families safe and secure online

Starter Level

- Everything in Intro Level
- Three new digital "find and click" storybooks
- New games and puzzles
- New *Parents Internet Safety Guide*

Explorer Level

- All of the above
- Lesson 4 (never released) Garfield comic book—*Downloading Disaster!*
- Printed copies of all three current Garfield comic books on privacy, safe posting and cyberbullying
- 24 pages of activities, games and puzzles
- New Garfield cyber safety coloring book
- Large Garfield and Friends cyber safety wall poster
- Special edition collectors' card
- 10% off educator kits for school classroom
- Regular updates of new games and activities
- Free shipping in continental U.S. Extra fee for Alaska, Hawaii and international

Our award-winning Garfield classroom program is still available to schools and businesses as it always has been, for when restrictions ease and we can return to some semblance of our previous lives. We are excited to expand to a digital format and confident this new offering will allow even more children around the world to become cyber safe.

To learn more, or start your new home subscription, go to https://iamcybersafe.org/s/garfield-at-home.

RETURN TO CONTENTS

(ISC)^2 community | SHARING INSIGHTS FROM BUZZWORTHY THREADS

Join the (ISC)^2 Community

Advice on Protecting Data Files, Securing At-Home Desktops

The (ISC)^2 Community has more than 27,000 cybersecurity professionals connecting, sharing knowledge and offering solutions in the online forum. Note that the questions and responses may have been edited for clarity and brevity.

QUESTION:

I am looking for a solution that can monitor an NAS [network-attached storage] file storage and can quickly identify files that were affected by a malicious activity. The idea is to efficiently identify and recover only specific files rather than a whole drive, to identify who performed the malicious act, and to alert for quick action.

—Posted by bsdulay

SELECTED REPLY:

The top of the list is, normally, Tripwire but, to be quite frank and objective, everyone must be trained to use it correctly. However, in my case, I put through a different recommendation based on NTT Change Tracker R2, as it was far more economical for this particular client and included some good AI capabilities, great reporting facilities and integration with good support, and the overall resources requirements were ideal for the use cases.

—Posted by Caute_cautim

Find this complete thread here.

QUESTION:

In a COVID-19 emergency, there could be a situation where some changes are requested for agent desktops to allow member service agents to work from home. The changes allow the identity to be confirmed without the caller speaking their SSN, DOB, etc., and without the agent being able to view the caller's SSN, DOB, etc.

I think one of them is OTP [one-time password]. The way the change works involves new APIs that create a 10-digit, one-time password that the caller tells the agent over the phone to confirm the identity.

Is there any better way of doing it with 2F [two-factor] authentication?

—Posted by iluom

SELECTED REPLY:

You first need to ask yourself why the agent working from home is raising new PII [personally identifiable information] concerns. If you do not trust your agent to have PII access in the first place, you need to consider measures like you are suggesting even when they are in the office. If you do not trust the house, you need to figure out how to enhance that trust (e.g., send corporate laptops home; use VDI solutions; enable MFA on your corporate mobile VPN solution; provide corporate network assets; purchase home shredders, etc.).

—Posted by denbesten

Find this complete thread here.

QUESTION:

I'm an aspiring information security practitioner looking for an opened door to join your professional ranks. It is amazing how businesses lament left and right that there are severe staffing shortages in the field, but even positions that are purportedly "entry level" usually list three to five years of experience as a prerequisite. I probably will not hit the ground running on day one, but I can definitely do a brisk walk and will not take long to pick up the speed. Perhaps, you have a suggestion.

—Posted by Belg

SELECTED REPLIES:

You are sadly hitting a very common problem. I think you will find there are two types of companies out there. One expects you to know everything they use and be able to hit the ground running. With such a wide range of technologies, this will be next to impossible. The other type of company, and I would say the one where we all want to be, sees how you are able to understand things and knows you will be able to ramp up rather quickly.

—Posted by JKWiniger

You may already have more relevant experience than you realize. It would probably be worth doing a full inventory of your skills and experience against a published skills framework in the security field. You don't have to be "expert" in each area. Just be honest with yourself, as it's the first step to thinking through how you could get more relevant experience for when the economy improves and you can change careers.

—Posted by Steve-Wilme

If you see a job listing where you have at least 50% of the skills and have the ambition to learn the rest, then apply. Or if it is in a specialty that you have a lot of experience in but lack a lot of the other duties, apply for it. Don't count yourself out if you don't have everything or do not feel like you are a guru at some of the items.

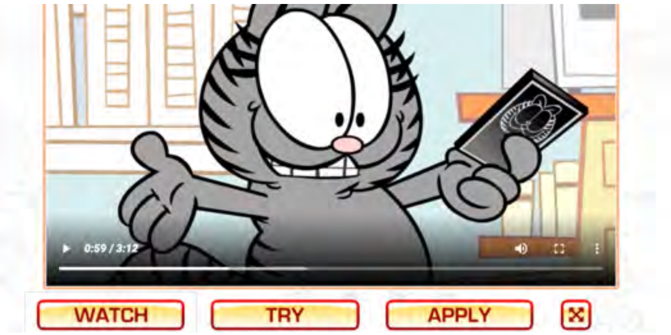
—Posted by CISOScott

Find this complete thread here.

NEW

ORDER NOW

GARFIELD AT HOME



- Never seen before adventures
- Find and Click Storybooks
- Garfield Coloring Book
- Game-based learning
- Parents Internet Safety Guide

20% OFF

USE PROMO CODE:

ISC2GARFIELD

IAMCYBERSAFE.ORG/GARFIELD-AT-HOME

CENTER FOR
**CYBER SAFETY
AND EDUCATION™**