BUILDING AWARENESS
Using existing standards and regs for a security program

CLOUD MIGRATIONS
Deciding vs. deploying solutions to complete a digital transformation
MPOWER

OCTOBER 16–18
MGM GRAND, LAS VEGAS

2018 Cybersecurity Summit
McAfee’s 11th Annual Security Summit

LEARN from McAfee CEO Chris Young and other thought leaders on how a strong cybersecurity posture is an essential component of any innovation.

HEAR from the man who literally wrote the book on innovation, Walter Isaacson, and Sir Tim Berners-Lee, who invented the World Wide Web.

DISCOVER the latest trends and best practices across some 90 technical breakout sessions.

NETWORK with your peers from across industries and learn directly from other McAfee users.

EXPERIENCE our closing event featuring the Grammy Award-winning rock band Weezer!

MPOWER 18 features targeted, highly technical sessions guaranteed to provide valuable, tangible knowledge to help you maximize your security solutions and tackle today’s greatest security challenges, while the breakouts offer insights and best practices to help you optimize your security and compliance initiatives. The Sponsor Expo will feature an extensive lineup of McAfee partners, including some of the industry’s most successful businesses. Don’t miss out on this unique opportunity to meet with key players in the cybersecurity arena—all in one location.

To learn more about MPOWER 18, please visit www.mcafeempower.com

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!

SAVE $100

As an (ISC)² member, you can save $100 off your registration by using promo code MPWR18!
features

INCIDENT RESPONSE

18 One Year Later
What have we really learned from the Equifax breach?
BY JOYCE FLORY

GRC

26 Building a Platform
Knowing what’s mandated—and what’s not—can help update or re-create a solid security awareness program.
BY STEFAN BEISSEL, CISSP

CLOUD SECURITY

30 Our Journey to the Cloud
(ISC)²’s COO explains why the organization decided now was the time to press forth.
BY WESLEY SIMPSON

departments

4 EDITOR’S NOTE
Mind the Gap
BY ANNE SAITA

6 EXECUTIVE LETTER
Taking Your Professional Development to the Next Level
BY MIRTHA COLLIN

8 FIELD NOTES
Newest cybersecurity advocate; five CPEs per book read; cast your vote in the annual (ISC)² board of directors election; highlights from 2018 Cost of Data Breach Study; Recommended Reading and more

14 #NEXTCHAPTER
(ISC)² Singapore Chapter

16 ADVOCATE’S CORNER
On African Safaris and Attribution
BY JOHN McCUMBER

34 CENTER POINTS
The Missing Piece (and How You Can Help Supply It)
BY PAT CRAVEN

36 COMMUNITY
Is the New CISSP Format Better?
Members weigh in on this as well as on listing certs in email signatures.

4 AD INDEX
Mind the Gap

As someone who’s devoted a considerable portion of her career to covering information security, I’ve been on a mission to promote—in word and deed—the non-tech skills now needed for career advancement (even survival). Becoming competent, let alone fluent, in so-called “soft skills” is hard work. Employers still value coding over communications skills. And too many of us are more comfortable mining event logs than mingling at actual events.

Promoting interpersonal communications to cyber professionals has never been an easy sell. But there are signs the working world is now providing an assist. A few months ago, Jeff Weiner, the CEO of LinkedIn, told a morning news program that interpersonal skills—communications, reasoning, team coordination, etc.—are now the number one quality sought by employers.

“That’s interesting because a lot of people are fixated on technology, and rightfully so. It’s an increasingly important part of how companies do business,” Weiner said. “But what we found when we did our skills gap analytical work is [with] interpersonal skills, the gap there is roughly three times higher than software engineering in the United States.”

That observation reminded me of a conversation I overheard decades ago when I was a junior attending an “engineering school.” A student newspaper editor was arguing on the phone with her computer science professor about an overdue assignment. I don’t recall the exact words she used, but in essence she told the teacher her future career didn’t rest on whether or not she passed Fortran. It did matter if she aced the communications classes competing for her time.

Everyone within earshot was a little in awe of the editor’s moxie and dedication to her craft. Perhaps what we should have respected back then was the importance she placed on a skill the rest of us tended to downplay. Especially given none of us ever had to program in Fortran.

Anne Saita, editor-in-chief, lives and works on the U.S. West Coast. She can be reached at asaita@isc2.org.
Join us at the (ISC)$^2$ Secure Summit EMEA
15 - 16 April | World Forum, The Hague

Our annual flagship event Secure Summit EMEA will bring together hundreds of security professionals from across Europe, Africa and the Middle East.

It will be two days of insightful discussions, workshops, panels and best practice sharing to stimulate feedback, challenge thinking, create debate and enable networking.

Learn more at:
secursummits.isc2.org
executive letter

BY MIRTHA COLLIN

Taking Your Professional Development to the Next Level

As we approach the last quarter of the year, you may have already reached many of your professional goals. But there’s still time for self-improvement while earning all of your CPEs. We’re excited to be hosting the 2018 (ISC)² North America Security Congress in New Orleans and have a multitude of robust learning opportunities throughout the week.

Our commitment to your professional development doesn’t stop with Security Congress. Training and education are the cornerstone of what we do at (ISC)² and we’ve recently updated several of our certification education products and launched several new CPE courses—all designed to be even more engaging for our members.

In keeping with our theme of “Enrich. Enable. Excel.” much of what we’ll be focusing on in the upcoming year is creating more customized professional development for our members. While certification is a huge accomplishment, it’s quite another to continue upon your individual path of learning to support career growth. In 2019, (ISC)² will become a go-to resource not only for certifications, but also for continuing development and self-improvement. The information security landscape is constantly changing; we all need to keep pace. (ISC)² wants to be there throughout your career, helping you remain relevant and on top of current industry trends.

After hearing feedback on your learning needs, we are committed to providing more self-paced learning opportunities, helping you to learn in your own time and in your own environment. These courses are more engaging and leverage state-of-the-art instructional design techniques. They include clearly articulated learning objectives, audio content, graphics, videos, readings, assessments and immersive interactive experiences designed to enhance the overall learning experience. The best part: these are free to members! Among the new curriculum offerings are:

- GDPR for Security Professionals
- DevSecOps – Integrating Security into DevOps
- Building a Strong Security Culture

Besides self-paced additions to our training suite, we’re introducing some in-person workshops in conjunction with (ISC)² Security Congress, (ISC)² Secure Events and other third-party hosted programs. The newest additions to our portfolio include a workshop specifically for executives wanting to learn more about the organizational value of a strong security team and an OWASP Top 10 workshop designed specifically for security professionals.

And finally, many members have said they’d like to see security awareness training that they can pass along to others in their organizations. They know that the number one threat faced by organizations today often comes from non-malicious and unaware employees. To answer that need, I am pleased to announce that (ISC)² has developed an interactive training course targeted at the layperson that can be shared widely within your organizations.

This easy-to-understand training lasts approximately two hours and is based on real-world scenarios users face in their daily lives. It includes important topics such as phishing, drive-by downloads, ransomware and other cybersecurity threats commonly found in the workplace.

As you can see, we’re excited about the enhancements we’ve made to our professional development portfolio, both in terms of content and ease of access. We look forward to hearing your feedback on these new offerings and to continuing to develop our programs to give you the best learning opportunities to excel as a security professional who helps ensure a safe and secure cyber world. For more information I invite you to visit learn.isc2.org.

Mirtha Collin is the Senior Education and Training Manager at (ISC)². She can be reached at mcollin@isc2.org.
One stack to secure your digital transformation.

THE POWER OF THE QUALYS CLOUD PLATFORM:

• 2-second visibility across all your global IT assets

• Continuous assessment of your security and compliance posture

• Identify zero-day vulnerabilities and compromised assets

• See the results in one place, in real time

• Drastically reduce your spend

Try it free at qualys.com/trial

© 2018 Qualys, Inc. All rights reserved.
Meet (ISC)²’s Newest Cybersecurity Advocate

(ISC)² RECENTLY NAMED Tony Vizza, CISSP, CRISC, CISM, as cybersecurity advocate for the Asia-Pacific (APAC) region to work with corporations, governments, academic institutions and others to collaborate to create the strongest cybersecurity policies. In addition, he recruits and develops cybersecurity professionals.

Vizza has more than 25 years of experience in information technology and information security. He has a B.S. in computing science from the University of Technology Sydney, a Global Executive MBA from the University of Sydney and is currently studying for a Juris Doctor degree at the University of New South Wales. He has provided expert services to several government agencies as well as professional organizations. He is an expert speaker on information security and a regular contributor to several publications in the region.

“Tony will be a key addition to our growing team in Asia-Pacific and an excellent advocate for the security profession in the region,” said (ISC)² CEO David Shearer, CISSP. “His varied experience in the regulatory, legal, computer science and information security fields gives him a well-rounded perspective on the challenges that our members face and will help further our mission to inspire a safe and secure cyber world.”

“Information security is all about people, and (ISC)² is investing in and providing the tools to make us all that much smarter and better when facing the challenges before us,” said Vizza. “The skills shortage in this industry is something I’m passionate about fixing, and I’m proud to be joining an organization like this at a time when I feel it’s needed most.”

Based in Sydney, Australia, Vizza will report to Clayton Jones, the (ISC)² Regional Managing Director for APAC.

Award for (ISC)²

(ISC)² webinars recently earned an industry award for work promoting the cybersecurity industry. (ISC)²’s Think Tank webinar channel was named the 2018 Highest Growth Channel in IT by BrightTALK, an online platform that offers webinar and video products to IT professionals.

One of the organization’s free webinar channels, (ISC)²’s Think Tank features 60-minute roundtable discussions on cybersecurity challenges with key security experts. The webinar series already has more than 60,000 views this year in North America alone.

“Delivering valuable educational experiences to our membership is the central goal for our team,” said Wesley Simpson, COO of (ISC)². “BrightTALK’s recognition of the growth of our channel affirms that our members, as well as other IT and ICT professionals, are engaging in the discussions we are hosting.”

(ISC)² has five additional free webinar channels:

• Security Briefings – Hour-long webinars providing a deep dive into topics in multi-part series
• From the Trenches – Experts providing accounts of hands-on experience in cybersecurity
• EMEA Webinars – Thought leadership on topics facing Europe, the Middle East and Africa
• APAC Webinars – Thought leadership on topics facing the Asia-Pacific region
• Security Congress – Top-rated sessions from (ISC)²’s annual flagship conference

To sign up for any (ISC)² webinars, please visit https://www.isc2.org/News-and-Events/Webinars/.

Earn CPEs for Reading This Issue

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

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 homepage via the link and click on “Create User Profile” in the upper right-hand corner.

Earn CPEs by Reading—As Long as You Know What to Read

By Ben Rothke, CISSP

For many people, it’s not passing the CISSP exam that is so difficult, it’s maintaining enough continuing professional education (CPE) credits to ensure the continuation of their certification. CPE requirements vary depending on one’s (ISC)² certifications. Details about the CPE requirements can be found at https://www.isc2.org/Member-Resources/CPE-Overview. One of the ways in which to earn CPEs is by writing book reviews.

(ISC)² recently updated the CPE program and members now get up to five CPEs per book read with a summary review attached with their CPE submission. For that, it doesn’t need to be a published review. But if you’d like to write a more extensive review and get additional CPEs, read on.

If knowledge is power, then one of the more effective ways to gain that power is by reading. When it comes to information security and risk management, it is a daunting task to try to keep up with the vast and ever-growing amount of written material. So, what is a security professional to do? How do you know which books are the most significant?

Presenting the Cybersecurity Canon project (https://cybercanon.paloaltonetworks.com/), of which I’m a member. Started in 2014 by Rick Howard, CSO of Palo Alto Networks, the members of the canon identify lists of must-read books for cybersecurity professionals or those looking to get a better understanding of the security industry.

The canon-worthy books include those that focus on the core aspects of information security, are forward thinking, original and insightful. They also should stand the test of time, meaning that they should be relevant for several years. You won’t see specific technology such as those on operating systems or specific types of hardware or software.


If there is a book you think is a candidate for the canon, you are invited to nominate it for entry and write a review. The review ensures the sincerity of the nomination and demonstrates to the canon committee that the person submitting the book is serious about it and feels strongly enough about it to take the time to write a review. The review does not have to be a monograph; a few hundred words will certainly suffice. There are plenty of good books out there to be read, so submit as many nominations as your time permits.

For more information or if you want to contact the canon, check out the Canon FAQ (https://cybercanon.paloaltonetworks.com/cybersecurity-canon-faq/). Looking forward to your review.

And after your review has been published, don’t forget to submit your CPEs at the (ISC)² site (https://cpe.isc2.org/).
The Cost of a Data Breach – 2018

Highlights from 2018 Cost of Data Breach Study: Global Overview, an IBM-Ponemon Institute study of nearly 500 companies worldwide.


AVERAGE COST OF A DATA BREACH

$3.86 MILLION

Up 6.4% (from the 2017 report)

ROOT CAUSES

- Malicious or criminal attack: 48%
- Human error: 27%
- System glitch: 25%

AVERAGE COST OF A DATA BREACH BY REGION

<table>
<thead>
<tr>
<th>Region</th>
<th>Cost (Millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td>$7.91</td>
</tr>
<tr>
<td>Middle East</td>
<td>$5.31</td>
</tr>
<tr>
<td>Canada</td>
<td>$4.74</td>
</tr>
<tr>
<td>Brazil</td>
<td>$1.24</td>
</tr>
<tr>
<td>India</td>
<td>$1.77</td>
</tr>
<tr>
<td>Australia</td>
<td>$1.99</td>
</tr>
</tbody>
</table>

INDUSTRY SECTOR

- Highest per capita cost of a data breach:
  - Health: $408
  - Financial: $206
  - Services: $181

INFOSECURITY PROFESSIONAL

Recognized for Editorial and Design Excellence

InfoSecurity Professional took two awards in the 2018 TABBIES, presented by the Trade Association Business Publications International.

The magazine’s design team, including art director Maureen Joyce and photographer Matt Greenslade, received an honorable mention for Design/Open Page or Spread for their work on “View from the C-Suite” in the 2017 July/August issue of InfoSecurity Professional.

The magazine feature titled “Change Management: Transforming Resistance into Acceptance,” landed at No. 18 among the Top 25 feature articles—among the most popular, and therefore competitive, categories in the contest. The article was written by Paul South and appeared in the 2017 March/April issue.

Cyber risk is not yet fully understood by people who should be in the know. Many principals at small and medium healthcare organizations simply do not fully understand the impact of a significant cybersecurity incident until they experience it.”

—Lee Kim, CISSP, from the June issue of Insights, a companion e-newsletter for the (ISC)² membership
Saluting the Finalists for the 2018 ISLA Americas Awards

**(ISC)² CONGRATULATES** the finalists for the 2018 Information Security Leadership Awards (ISLA) for North and Latin America.

Held annually by (ISC)² in cooperation with the North and Latin American Advisory Councils, the ISLA Americas Program recognizes information security and management professionals throughout the private and public sectors in North, Central and South America, with the exception of the U.S. federal government (recognized through the ISLA Government Program), for their outstanding leadership and achievements in workforce improvement.

The winners will be announced in a luncheon ceremony at the 2018 (ISC)² Security Congress in New Orleans on October 9, 2018.

Here are the 2018 finalists:

**COMMUNITY AWARENESS**
Joseph Carson, CISSP  
Chief Security Scientist, Thycotic  
Project/Initiative: Cyber Security for Dummies

Nemi George  
Senior Director, Information Security & Service Operations, Pacific Dental Services  
Project/Initiative: Okta Deployment

**INFORMATION SECURITY PRACTITIONER**
Domingo Castillo, CISSP  
AVP Regional Information Security Officer, Chubb  
Project/Initiative: Information Security Technology Convergence

Robb Van Eck, CISSP, CCSP  
Senior Information Security Architect  
Project/Initiative: ePHI Data Identification

**SENIOR INFORMATION SECURITY PROFESSIONAL**
Dave Bailey, CISSP  
Manager of Security Services, CynergisTek, Inc.  
Project/Initiative: Security Partner Network

Rinki Sethi, CISSP  
Vice President of Information Security, Palo Alto Networks  
Project/Initiative: Security Education Growth Initiative

**Additional Awards Being Presented at the Ceremony**

In addition to recognizing the ISLA Americas winners, (ISC)² is honoring other information security professionals for their contributions to (ISC)²’s efforts in creating a culture of information security:

**(ISC)² President’s Award**
This award recognizes volunteers who have made a significant impact on and/or contribution to (ISC)². Multiple recipients are chosen annually for each region at the sole discretion of (ISC)²’s CEO.

**Fellow Award**
The Fellow of (ISC)² was established to honor and distinguish a select number of elite information security professionals who have made outstanding contributions, throughout their careers, to the information security profession.

**Center for Cyber Safety and Education Awards**

*Julie Peeler Franz “Do It for the Children” Volunteer Award* honors a Center volunteer/ambassador for their work with the Garfield’s Cyber Safety Adventures program and/or the Safe and Secure Online program promoting cybersecurity efforts for children, parents, educators and seniors.

*Center for Cyber Safety and Education’s Partnership Award* is presented to a company or organization that has partnered with the Center to grow and expand its programs including education, research or scholarships.
RECOMMENDED READING
Suggested by Dr. Richard N. Knepp, CISSP

Future Crimes: Inside the Digital Underground and the Battle for Our Connected World
By Marc Goodman
(Anchor, 2016)

If you thought you knew about every cyber threat, think again. Toasters and fake USB chargers? They are just the beginning. Author Marc Goodman does an excellent job of identifying the many security threats, attacks, deceptions, hacks, ransomware extortions and other crimes that were and are being heaped upon the users of the “connected world.” And there are some threats you would not have thought about until he discusses them.

The author draws interesting parallels between the computer security industry and the medical profession based on the terminology security professionals use. Terms such as infection, quarantine, virus and users are discussed. He also proposes some interesting solutions based on the Centers for Disease Control (CDC) to help solve some of the security issues.

Goodman presents a serious eye-opening lesson about “friendly and free” service providers such as Facebook, Google, Instagram and Apple that harvest your personal information on a massive scale to sell it, and the impact of clicking on the OK button after skipping over the option to read the lengthy terms of service (TOS) agreement.

These and other companies that maintain large data repositories of customers’ personal information are at great risk for theft by what the author calls “Crime, Inc.,” encompassing cybercriminals including the Chinese, terrorist organizations, script kiddies, Russian mafia and a host of other thieves plying their expertise in theft on Tor networks.

As an example, he cites a case of theft of a manufacturer’s trademarked and copyrighted intellectual property and the Chinese customer’s subsequent cancellation of millions of work because they already had everything (stolen, of course).

In addition to covering past and present threats, the author also speculates on what may be most valuable to the reader: future threats. These include the impact of quantum computing on encryption, blockchains, artificial intelligence, robotics, biometrics and much more, such as risks inherent in DNA technology. He describes a case where DNA evidence was fabricated from DNA information stolen from a medical database.

This is an unusually long book (608 pages in paperback; the author does warn the reader at the beginning). It is detailed and well composed. The three main sections and 18 chapters are logically organized and flow nicely from one chapter to the next. The threats are well documented. Marc Goodman does an excellent job of scaring the reader.

On Cyber: Towards an Operational Art for Cyber Conflict
By Gregory Conti and David Raymond
(Kopidion Press, 2017)

Know your enemy could be the subtitle of this battle plan for cybersecurity professionals. Authors Gregory Conti and David Raymond describe today’s strategies used by nation-states to weaponize their cyber techniques and methodologies.

The key in On Cyber: Towards an Operational Art for Cyber Conflict is that security operations professionals must be vigilant, constantly aware of not just the latest threat intelligence, but also techniques used to take advantage of their in-house vulnerabilities. Virtually every system is at risk, now and in the future, warn Conti and Raymond, so immediate action is crucial to build the methodology to defend against the promise of IoT, autonomous cars and smart cities.

The authors identify, in a key table that can be implemented by the reader, the main assets of an organization in terms of logical and geographical. It is peeling back the onion and looking at layers of defense in depth that can be used to protect all the assets. Conti and Raymond
direct cybersecurity professionals to have an end-to-end mindset, that is, to connect people, process, world events and the ability of technology to mitigate security risks.

Conti and Raymond direct cybersecurity professionals to have an end-to-end mindset, that is, to connect people, process, world events and the ability of technology to mitigate security risks.

On Cyber discusses how militaries defend, fight and win in cyberspace. While there are many books on the technical measures to secure systems, this book offers a different perspective, focusing on the underlying principles that do not change with the “sands of time.” It is written for a policy maker or security professional to determine which risks need to be mitigated and how to overlay this approach with existing measures and strategies.

The authors’ professional experience certainly adds to the strength of the book. Conti and Raymond served on the faculty at West Point for a combined 20 years and helped build the U.S. Army Cyber Branch. On Cyber is a readable book with some memorable reminders that security is more than installing an .exe on a server protection. “An enemy combatant can be grandma’s toaster” and “you can’t fire cannons at the internet” are examples of user-friendly approaches for practical defense that are strewn through this valuable volume.

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

To effectively deliver value as cybersecurity professionals, (ISC)² Singapore Chapter is focusing on working closely with other Singapore cybersecurity-focused organizations. This collaboration is a clear path forward to managing and mitigating risks connected with electronic secrets, according to the Singapore Chapter’s president, Matthias Yeo. “That is what we believe cybersecurity of the 21st century needs: ecosystem partnership,” he said.

Formalization of relationships with global organizations such as ISACA and ITSMF, and local organizations such as the Association for Information Security Professionals (AISP), engages cybersecurity professionals across multiple disciplines. The opportunity to network with other practitioners and an increased variety of speakers and topics has enabled the chapter to cater to a wider variety of member interests.

As a result, the Singapore Chapter’s monthly attendance has doubled and sold-out events are becoming common. This fiscal year, there is a growing increase in both new membership and, more importantly, a 30 percent conversion rate of expired members renewing their membership. Active participation in the chapter’s online social media forums has also shown an increase.

These collaborative efforts have also provided (ISC)² Singapore the opportunity to make a bigger splash on Singapore’s cybersecurity landscape. From consulting on legislative efforts such as the Singapore Cybersecurity Bill, to closer relationships with government organizations such as the Cyber Security Agency (CSA), and increased joint events with other professional associations, the chapter has been able to offer a better value to its members while simultaneously directly influencing the direction the nation is taking. For example, the (ISC)² chapter president is an active participant in the Singapore multi-association committee, and chapter board members were included as judges in the inaugural annual Singapore Cybersecurity Awards.

The island nation of Singapore continues to evolve toward an electronically integrated, data-driven society and professional associations, including the (ISC)² Singapore Chapter, are helping lead the way to safe and secure infrastructure. By providing trained leadership and engineering expertise, the chapter helps to assure the country’s people that their information is in the hands of certified cybersecurity professionals.
How did (ISC)² Singapore Chapter begin reaching out to other cybersecurity organizations? What were the first steps?

It began with an introduction through a meeting of various associations organized by the government as well as less formal gatherings. The security field in Singapore is rather small and the leaders from the different associations (such as ISACA, AISP, Cloud Security Alliance, ourselves) are already good friends; we often meet for drinks to catch up on the latest and greatest in the security domain and to learn from each other. We also have these opportunities overseas when we are invited to speak at conferences. For example, ISACA Singapore chapter’s president and I often present in the same conferences; that’s where we start investigating possible collaborations, which later leads to memos of understanding.

Were there any concerns about diluting the efforts of (ISC)² Singapore by joining forces with other organizations?

The first objective is to understand our mandate and we often find it very complementary to other organizations’ goals. For example, AISP (Association of Information Security Professionals) is an organization that, while it does not issue certificates, actively pushes collaborations with the government. (ISC)² Singapore Chapter seeks to reach out to certificate holders (CISSP, CCSP, etc.) to make sure they keep in touch with the community. As AISP does not have the reach of those “established” cybersecurity professionals, we connect with their members who wish to deepen their knowledge through CISSP certification.

What are some accomplishments, such as events or initiatives, that the chapter has been involved with that have come about from this collaboration?

Chinese New Year Gathering 2018 was the combined effort of AISP, ITSMF and (ISC)² Singapore. This annual gathering is an (ISC)² Singapore tradition, and many members from other organizations were surprised to learn that we have this kind of activity. This sparks interest within the non-member attendees to learn more about us and, hopefully, join our chapter. This is where they realize different organizations can provide a variety of experiences and there is a benefit to joining multiple associations. That event draws about 80 attendees, including government officials.

The growth of the chapter has been a benefit of this collaboration. What other positives have you experienced?

These collaborations label us as a “connector” rather than an association that is purely interested in running our own certifications. Government representatives, especially, were excited as they felt that cybersecurity communities need to have more collaborating and sharing. For example, the Cyber Security Agency (CSA) is including us in its quarterly meetings to talk about how they are engaging the public for social awareness and getting our opinions on how they can expand community engagement, as well as planning together for Singapore activities and events.

Partnership can be hard when the different associations don’t understand the mandate. So it is important to be clear about the objectives.

What advice do you have for the leadership of other (ISC)² chapters who would like to strike up partnerships with cybersecurity organizations in their areas?

Partnership can be hard when the different associations don’t understand the mandate. So it is important to be clear about the objectives. The ecosystem that can be created can be very powerful in influencing directions and creating thought leadership discussions. Therefore, the personal and professional relationships of the executive members are crucial to forging this strategic alignment so that when collaboration discussions happen, we focus on possibilities rather than conflict.
On African Safaris and Attribution

I recently took time off for one of those bucket-list activities: a safari in Africa. This picture shows me staring down a white rhino protecting her calf in KwaZulu-Natal. I’m back, so the situation obviously ended well for both of us.

For the safari, I went off the grid for nearly two weeks. After a 16-hour flight back home, I arrived to an overflowing inbox, including a reminder to dash off this column. The email suggested I weigh in on what has been a “hot topic” for a while now: alleged Russian cyber activity on various political, economic and social fronts.

I did want to address this “hot topic,” but not necessarily along the proposed line of thought. It’s a “hot topic” for many who are pointing to sketchy experts, unsourced data and outright speculation to bolster any variety of conspiracy theories, unfounded accusations and hackneyed narratives. Most media articles are thin on facts and background data, but rife with “what this all means.” It’s a real mess.

The central problem is what we call attribution. Attribution is the practice of defining the causation or perpetrator—in this case, malevolent actors who are manipulating information sources to influence others for self-serving purposes. By naming these threats, accusers can then assign very specific intentions and motivating ideology. It becomes a model like this: threat actor -> intent -> actions (“hacking”) -> target -> impact. Problems arise either when threat actors are misidentified, or intentions are misread early in this process. When that happens, the defined conclusions and narratives quickly topple over as the foundation for the conjecture erodes away.

Attribution is a tricky business, especially in what we now call cyberspace. We can’t actually see these human threats and end up making our assumptions based on data points like digital “footprints” and the content of data packets. Of course, anyone who works in our profession for even a short time realizes how easy it is to forge and manipulate these evidentiary elements. Attribution is not a straightforward science, and running off with superficial evidence to make accusations is a fool’s errand.

I am not trying to refute any of the media hype or exonerate digital villains (no matter who they are). I am simply pointing out the fact it’s best to have strong, fact-based evidence before running to the keyboard or microphone to make accusations. Most of what you’ve read about Russian “hacking” doesn’t meet this standard.

There is still a critical service our threat intelligence people perform, but they are experts, and the ones I know remain always skeptical. It’s best to leave attribution to the professionals.

Just like the mother rhino I met who must face potential threats head-on, dealing with what’s in front of her, most cybersecurity professionals must do the same. The rhino doesn’t try to understand why I am there with my camera, or how the engine in the Land Rover works. She simply needs us to stay back as she protects her most critical asset: the next generation. We would do well to do the same.
Navigating Through the Seas of Disruption

For today's enterprise, cloud adoption has moved beyond the early adopters to encompass a wide range of mission critical business functions. Financial services, government and other industries with regulatory mandates have made significant steps into the cloud over the past year. Making this leap has required a transformation in both the technology of security and the mindset of security professionals.

Visit CSA booth #113 in the expo hall to speak with the CSA experts and learn how best practices in security can help organizations navigate through the seas of disruption.

www.cloudsecurityalliance.org
BY JOYCE FLORY | Equifax announced the data breach that shook the world in September 2017—three months after the company discovered it. Malicious actors snatched consumer data by making the most of a security flaw within a tool used to build web applications. Equifax eventually admitted that it knew of the security flaw months before disclosing the breach.

In March 2018, Equifax reported that the breach victimized 2.4 million more Americans beyond the original estimate of 145.5 million. The company had unwittingly turned over their names, addresses, ID images, Social Security and driver’s license numbers, and passport data. Equifax pledged to notify victims and provide identity theft protection and credit monitoring.
And now, a year later, Equifax awaits another set of verdicts. Will the company pay for having leaked sensitive personal information to those bent on identity theft? Will states’ attorneys general and civil lawsuits point the finger of blame at Equifax? And will a frustrated Congress piggyback on the data breach disclosure laws now operative in all 50 states? Experts continue to question if U.S.-based companies should report a data breach within 30 days and if executives should face up to five years in prison for breach concealment.

THE BREACH’S IMPACT
One thing is for sure. The Equifax breach was a watershed moment for security professionals, C-suite executives, and the public relations, compliance and legal team members who plan for and respond to data breaches. Among the key areas of impact are the following:

Assumption of accountability: Before the Equifax breach, people assumed that the company had the controls to safeguard privacy and security. Post-breach, a growing number of organizations have accepted accountability for third-party performance, according to Avani Desai, president of Schellman & Company, a security and privacy compliance assessor. The result: an uptick of internal third-party vendor management to ensure proper testing of controls.

Attention to monitoring: “Organizations are more interested in monitoring specific pieces of personal and confidential information,” says Ron Schlecht, managing partner at BTB Security, an information and IT security company. “Independent of regulations or compliance guidelines, these organizations now compel vendors to install, monitor and test adequate security protections.”

Enhanced consumer awareness: Both 2017 and 2018 were banner years for consumer awareness. For the first time, consumers developed genuine insight into the significance of safeguarding data, privacy and security. “Five to 10 years ago, consumers didn’t realize the impact of stolen data,” says Desai. “Today, they’re more mature and demanding and pose questions like ‘Are you giving my data to a third party? Will you be encrypting it?’”

Enhanced employee awareness: Workers are more in tune with the fact that every organization stores personal and confidential information,” says Schlecht. “They realize that they must protect that information and understand what must be done in the event of a breach.”

Information security insight: “The breach was a wake-up call to the security community on the potential misuse of information because Equifax is a major data broker and a lynchpin to privacy,” says Schlecht. “The breach got attention because of the unprecedented number of people who were affected.”

EQUIFAX LESSONS LEARNED
How can organizations implement the lessons learned from the Equifax breach—one year later? Following are security experts’ recommendations:

Invest in employee awareness and training—from blocking where employees can go to targeting phishing emails. "Employee awareness should be short and frequent,” says Desai, who advises CEOs to showcase cybersecurity at employee meetings and share messages like “Think before you post to social media.” Equally important is helping employees understand “why you should treat our data like your data,” says Schlecht. “Employees need to realize that they don’t just handle corporate data; they’re stewards of individuals’ personal data.”

“Employees need to realize that they don’t just handle corporate data; they’re stewards of individuals’ personal data.”

—RON SCHLECHT, managing partner, BTB Security

Install access controls: The problem is rampant. Users share usernames and passwords. Ten people share a single username and password. Organizations all too often still fail to provision usernames and passwords correctly. People have more access than they warrant or organizations forget to revoke the access of employees who no longer work there.

Strict access controls, including passwords, can prevent malware—especially at a time when the number one password is 123456, followed by 123456789, according to a password manager and digital vault company, Keeper. Equally vital, according to Desai, is multi-factor authentication provided through a key fob, biometrics or phone authenticator.

The optimum approach, according to Gartner, is to identify access and management solutions that manage digital identity and access management across systems, performing functions like reporting and analytics, auditing, role and policy management, and access requests.

Pay attention to the Internet of Things (IoT): Invest in patching peripheral systems. “IoT devices, which sometimes come from manufacturers with passwords installed, generate sensitive personal data that deserves protection,”
Third-party assessments: More organizations will retain third parties to perform enterprise-wide security assessments, predicts Avani Desai of Schellman & Company. Independent third parties or audit and security firms will report on system strengths and weaknesses and generate certificates.

Attacks on low hanging fruit: Attacks on “low-hanging fruit” often are easier and more anonymous through cryptojacking, says Oleg Kolesnikov of Securonix. For this reason, while malicious actors are still using exploits made famous in the Equifax breach, some of the latest attack payloads tend to leverage cryptojacking malware, which is anonymous, easy to deploy, and makes attacks highly profitable.

Revenge through ransomware: Ransomware attacks have been on the upswing in recent years, says Kolesnikov, but the latest trend is for attackers to use cryptojacking instead of ransomware. As the security community adapts, we are likely to see attackers use other creative ways to monetize security breaches in the future.

Intelligent cybersecurity automation and blindspot reduction: “On the defense side, expect to see more intelligent cyber security automation and orchestration (SOAR) systems connecting the existing security components and technologies, more systems addressing potential blind spots, including those helping increase visibility into the networks,” predicts Kolesnikov. “This will help increase chances of early detection and response and ensure that security tools work well together.”

Systems on top of systems: “Expect to see more systems built on top of existing security configurations and technologies,” says Kolesnikov. “This will ensure that all security tools work well and work well together.”

Increased investment: As breaches grow in scope and breadth, board and C-suite executives will ensure that the CSO, CIO, and public relations, compliance and legal professionals have the resources they need to combat security problems, says Ron Schlecht of BTB Security. Cybersecurity will emerge as an enterprise-wide priority.

Accelerated responsiveness: “You’ll see faster response times to breaches,” forecasts Ouellette. “What was once a week will now be handled in days. What was days will be handled in hours.”

Narrative control: “Most organizations are eager to control the breach narrative, but that shouldn’t be the immediate focus,” says Jason Ouellette of Text100. “If you respond in a timely manner, are as open and transparent as you can be, those affected by the breach will cut you some slack and appreciate the immediacy you’ve brought to the situation.”

Crisis planning prioritized: “Organizations that think they can deal with a crisis as it surfaces are in for a rude awakening,” says Ouellette. “Reduce your response time by making crisis planning a priority. By crafting a crisis communications plan now, when the time to act comes you can focus on the breach, the remedy, and ultimately what you say to your audiences.”

EMERGING TRENDS
FROM THE EQUIFAX BREACH

says Desai. “The key question is whether standard identity and access management solutions can manage IoT.”

In recent years, IoT security has gained importance as a growing number of breaches now involve web-enabled devices, making it mandatory for organizations to patch technologies ranging from cameras and swipe cards to printers and projectors connected to networks.

Invest in enterprise risk assessment: Understanding risks associated with data requires re-examining every corner of an organization—from HR and IT to finance and operations—and asking: What are the data risks to customers? What’s the likelihood of a breach? And how will the breach impact the business? Organizations have multiple options, according to Desai: Accept the risk; mitigate the risk via cyber insurance or a DLP (data loss prevention) system; or reduce the risk via outsourcing.

Desai recommends risk assessments each time an organization goes through a major change or implements a new system. The goal: Create a dynamic document for widespread review and use within IT and security, the C-suite, board, operations and finance.

Just as important, says Schlecht, is assembling a response team that knows existing technologies and is prepared to function according to a plan that empowers them to respond—quickly and effectively—to the breach.

Test and simulate: Remediation after a hack or breach
TIMELINE

EQUIFAX BREACH

MARCH 8, 2017
The U.S. Department of Homeland Security Computer Emergency Readiness Team ("U.S. CERT") sends Equifax and many others a notice to patch a vulnerability in certain versions of Apache Struts software, which Equifax used in its online consumer dispute portal.

MARCH 10, 2017
Equifax is breached.

MARCH 13, 2017
Attackers install persistence web shells.

JULY 29, 2017
Equifax’s security team observes suspicious network traffic associated with its U.S. online dispute portal web application. In response, the security team investigates and blocks suspicious traffic.

JULY 30, 2017
Equifax patches the vulnerability.

SEPTEMBER 7, 2017
Equifax makes the breach public and says it impacts 144 million Americans, resulting in an initial stock loss of $4 billion.

SEPTEMBER 8, 2017
News outlets report three Equifax executives sold stock days after internally learning of the breach. Press and social media also begin criticizing the company’s efforts to help victims through a special website rife with issues and a credit monitoring service owned by the same company.

SEPTEMBER 12, 2017
Equifax announces its CIO and CSO are retiring.

SEPTEMBER 29, 2017
Equifax opens an investigation into executive stock sales that took place in August.

OCTOBER 3, 2017
Equifax’s former CEO, Richard Smith, testifies before Congressional representatives.

MARCH 1, 2018
Equifax finds approximately 2.4 million additional U.S. consumers were impacted by the data breach, bringing the total number of consumers affected to more than 146 million. The total direct cost of the breach to Equifax after insurance reimbursements was more than $114 million.
demands data backup and testing to uncover useable data and backups. Desai suggests “a mature backup and restoration process—especially in cases involving ransomware.” While most companies do annual testing of backups, quarterly testing is the preferred practice.

“Security tools must be continuously monitored, to make sure their effectiveness hasn’t deteriorated over time due to vendor quality or configuration issues,” says Avi Chesla, co-founder and chief technology officer of cybersecurity provider empow. “Constant, active supervision of the security platform is essential to ensure that security tools work well and work well together.”

Schlecht agrees. “Adversary hacking simulation has helped organizations identify problems before the bad guys arrive,” he says. “There isn’t an organization out there that doesn’t do proactive security assessment, evaluating threats and understanding weaknesses.”

Oleg Kolesnikov, who leads cybersecurity analytics and threat research at Securonix, advocates a security profile and baseline of the environment. “If you baseline the behavior of the attacked systems and environment, the attack in many cases will stand out as an anomaly,” he says. “If Equifax had used its technology to baseline the environment, there is a high chance it could have detected the 2017 exploit as an anomaly.”

In addition to baselining the environment via machine learning/artificial intelligence tools, Kolesnikov recommends continuous validation of security controls through ongoing breach and attack simulations as well as incident response drills. “Security teams may be overwhelmed by...
JOIN THE CONVERSATION on the (ISC)² Cybersecurity Community!

community.isc2.org

CONNECT. COLLABORATE. SHARE. DEVELOP.

Earn specialty badges for participation!

(ISC)² Community
alerts but they can use automated tools to baseline, identify the most critical alerts and pinpoint anomalies,” he says.

Experts also recommend making security an organization-wide priority by focusing on roles and responsibilities:

**CSO/CISO: This is job one.** “CSOs need to ensure that everyone understands how security risks could put the business at risk,” says Schlecht. “They must be transparent about security status, telling executives what they need to hear about the possibility of a breach, how to minimize that possibility and how to respond effectively.”

**CIO: Drive readiness for security.** “Cyber crimes are becoming a cost of business,” says Schlecht. “Board members, C-suite executives and shareholders must understand the nature of risk, including organizational vulnerabilities, level of susceptibility to a breach and the breach’s impact on business, brand and reputation.”

**CMO: Leverage the power of language.** Whether communications professionals sit in marketing, public relations or the C-suite, they often function as “the voice of reason,” according to Jason Ouellette, managing consultant at Text100, a technology public relations and marketing communications firm. “They must direct and manage external and internal communications regarding the breach—even with their own C-suite.”

**CEO: Champion cybersecurity.** “Based on the lessons we learned from the Equifax breach, the CEO should make cybersecurity a priority and should be in contact with the security team on a regular basis—having “nominal” meetings once or twice per month may not be sufficient,” advises Kolesnikov. “If the CEO lacks a technical security background, he or she should work closely with an internal security expert to help translate technical security requirements into business requirements and establish the appropriate cybersecurity tone from the top. If no internal security experts are available, the CEO should retain an external consultant to learn best practices and how to work with the security team most effectively.”

**C-Suite: Stay involved in security issues.** “Senior executives are more involved in security than ever before,” says Kolesnikov. “They understand the importance of early detection, containment and breach response, which creates momentum around investment in technologies that detect and respond to security threats automatically.”

**Employees: Practice good data and security hygiene.** Schlecht advocates tapping personal connections and education to bridge the gap between what people do personally and what they do in the workplace. “Teach cybersecurity etiquette and best practices, making sure employees understand both the good and the bad within the workplace, at home and in their personal lives,” he says.

**COMMUNICATE!**

Communicate with extreme caution: The Equifax breach confirms the adage: It’s not always what you say, it’s how you say it. “In today’s day of cybercriminals, no company is safe,” says Ouellette. “But because of the vast amount of information Equifax holds, there were more eyes on it and more interest from the public, which is why the way the company mishandled the communications around the Equifax breach exposed millions of driver’s licenses, phone numbers, emails

Equifax taps former IBM executive Bryson Koehler to lead technology efforts

Concerned by Equifax, lawmakers make credit freezes free
https://www.apnews.com/60dc619d98474096910742210a93d7cb

Equifax sends some consumers hit by its data breach wrong letters

Consumers have filed thousands of complaints about the Equifax data breach. The government still hasn’t acted

Equifax’s data breach has cost it $242.7 million

Thousands of companies are still downloading the vulnerability that wrecked Equifax
breach is what will be remembered. Equifax waited too long before informing the public and the problem only got worse as time went on. By then it was too late to regain trust.”

**Communicate with context:** “Acknowledgement and communication of a breach are effective only if security controls provide situational awareness that reflects the potential impact of the breach,” says Chesla. “Equifax didn’t know the incident’s size and its potential impact, which made its communication response ridiculous.”

**Communicate with candor and empathy:** “Send candid, supportive communications to employees, consumers, the media and anyone else affected by the breach,” advises Desai. “Just as important, identify the causes and extent of the breach and specific vulnerabilities along with a pledge to prevent further data exploits.”

**Communicate with the future in mind:** “Make sure you give out accurate information, but with a disclaimer that the investigation has just begun and will be ongoing,” says Schlecht. “Continue to offer updates but own up to the breach right away.”

**Communicate with simplicity:** The message of a hacked organization is simple, says Desai. “We’ve identified the nature and size of the breach. We know and understand what and who caused it and we’ve closed the exploit. We’re now in the process of outlining next steps and conducting research to upgrade security systems.”

**Communicate with timeliness and transparency:** “Be the professional who explains the downside of waiting or not disclosing information in a timely manner,” advises Ouellette. This is especially true in the new era of the EU’s GDPR, which requires organizations to report breaches in a timely manner and allow EU citizens more control over how their personal data is used and stored.

“Organizations have an obligation to be open and transparent,” Ouellette continues. “Customers expect transparency and a communications team needs to function as the voice of the customer when the communications plan is being put together.”

JOYCE FLORY, Ph.D, is a freelance writer based in Chicago.
Knowing what’s mandated—and what’s not—can help update or re-create a solid security awareness program

BY STEFAN BEISSEL, CISSP

SECURITY AWARENESS is vital at all levels of an organization. Implementing appropriate measures to create that awareness among all employees will lead to the desired behavior in security-relevant situations. Awareness also is addressed by ever-expanding information security-related regulations and industry-specific standards.

Why not use the rule sets that companies must meet to influence the design of your organization’s security awareness program?

This summarized overview of the most popular legal and regulatory requirements and standards can help you design or update your own internal security awareness programs.

ILLUSTRATION BY L.J. DAVIDS
KNOW WHAT IS REQUIRED
A company should be clearly aware of which regulations are relevant and applicable. In general, applicability depends heavily on the business, which means companies are often affected by different requirements at the same time.

While regulations are mostly mandatory, companies have no legal obligation to adhere to standards. However, there are peculiarities among standards that lead to a virtual obligation because ignoring them could lead to disproportionate disadvantages, including extensive financial and reputational damages. The number of aggregated requirements for a single company is often very comprehensive. Not only the IT area, but other areas like accounting and production can be affected.

Here are security awareness requirements from some of today’s most popular laws.

LEGISLATIVE COMPLIANCE

GDPR
The General Data Protection Regulation (GDPR) was published by the European Union in 2016 and has been enforced since May 25, 2018. It addresses the data protection and privacy for all individuals within the European Union. The GDPR affects not only European companies but every company that collects personal data or behavioral information from someone in an EU country.

Those companies must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. This represents an indirect requirement for implementing security awareness since awareness measures are generally considered common organizational measures. In addition, companies must develop binding corporate rules that address security awareness. Specifically, there must be rules to ensure appropriate data protection training to personnel having permanent or regular access to personal data.

HIPAA
The Health Insurance Portability and Accountability Act (HIPAA) applies to all U.S. companies in the healthcare sector, including concerned business associates, to ensure the confidentiality and security of protected health information (PHI). With regard to security awareness, HIPAA requires that a program be implemented for an organization’s entire workforce.

Specific security and privacy aspects must be addressed during implementation, in particular: security reminders, protection from malicious software, log-in monitoring and password management. It also requires that periodic awareness updates are performed.

FISMA
The Federal Information Security Management Act (FISMA) addresses the secure handling of U.S. government data and, therefore, primarily concerns federal agencies. The law requires security awareness training for all personnel to inform them about risks and responsibilities.

GLBA
The Gramm-Leach Bliley Act (GLBA), also known as the Financial Services Modernization Act, requires U.S. financial institutions to protect consumers’ confidential banking information. Affected companies are directed to establish appropriate administrative, technical and physical security safeguards. Although security awareness is not explicitly addressed, it can be considered a common administrative safeguard.

SOX
The Sarbanes-Oxley Act (SOX) regulates the risk management of all U.S. publicly owned companies to strengthen the confidence of investors. Security awareness is only indirectly addressed in SOX. Information about internal control measures that ensure the appropriate disclosure of material information must be included in periodic reports. This can be interpreted as an awareness task, which also applies to material information relevant to information security.

A report on the responsibility of management for establishing and maintaining control measures must be prepared. Considering that management must be aware of information security to fulfill their responsibility, this requirement also implies a need for security awareness.

STANDARDS FOR INDUSTRY COMPLIANCE

ISO – The International Organization for Standardization
Among ISO standards, the ISO 27k series is a collection of standards specifically designed for information security management. The two most important standards in this series are ISO 27001, which describes requirements for the creation of an information security management system (ISMS), and ISO 27002, which addresses specific information security control measures.

The control measures are divided into different areas, like security guidelines, access control, cryptography and operations security. An indication of security awareness can be found in both standards.

In ISO 27001, there is only a general reference to awareness needs: Chapter 7.3 requires employees to be aware of information security policies, ISMS effectiveness and implications of nonconformity. However, ISO does not define time, frequency or type of appropriate awareness measures.

ISO 27002 provides more detailed awareness in the form
of control measures, including the requirement for appropriate awareness education and training for all employees. This should include campaigns and issuing booklets or newsletters. In addition, role-specific awareness measures are required, which should not only be carried out during new hiring, but also regularly repeated and updated. The content to be included is management’s commitment, valid rules, responsibilities, procedures, controls, and contact points and resources for additional information.

ISO also emphasizes the importance of employees’ understanding of security.

**NIST**
The National Institute of Standards and Technology (NIST) publishes many different standards. With regard to information security, the standard 800-53a (Security and Privacy Controls for Federal Information Systems and Organizations) is considered here. In this standard, security awareness is addressed in the form of a controls catalog.

The four relevant controls are:

- **Policies and procedures with appropriate content must be created.** These must be disseminated within the company, regularly reviewed and updated.
- **Training must be carried out for new employees, in case of relevant changes to information systems, and repeated in a defined frequency.** It is recommended to include simulated cyberattacks, as well as detection and reporting of threats.
- **Role-based security training must be conducted,** e.g., for software developers or personnel administering security systems.
- **All training activities should be documented, monitored and individually recorded.**

**PCI**
The data security standard of the payment card industry (PCI) is an industry-specific standard for payment card transactions. Only those companies that store, process or transfer cardholder and authentication data are affected by this standard. The standard was upgraded to version 3.2 in 2016 and addresses six topics:

- Network and systems security
- Protection of cardholder data
- Vulnerability management
- Access control
- Monitoring and testing networks
- Policies

Security awareness is required: “Employees must be educated upon hire and at least annually. Multiple methods are required, e.g., posters, letters, memos, web-based training, meetings and promotions.” In addition, it should be verified with interviews whether training is carried out and employees are aware of the importance of security.

**CONSOLIDATING REQUIREMENTS MAXIMIZES EFFORTS**

Security awareness is addressed very differently within regulations and standards (see Table 1). An analysis and differentiation of the regulations and standards can be very helpful to meet compliance requirements more efficiently.

The relevant requirements for security awareness within regulations and standards can be assessed as follows:

- Direct requirements for security awareness cannot be found in all relevant regulations and standards. In some cases, only indirect requirements exist, which can be referenced to security awareness only by interpretation. SOX and GLBA can be connected to security awareness only indirectly. All other mentioned regulations and standards include direct requirements.
- The target group orientation ensures that employees are addressed with relevant content. A related requirement can be found in the ISO and NIST standards, which explicitly require the consideration of roles or target groups when communicating awareness content.
- The usage of multiple methods is only required by ISO and PCI. They require that different methods are used to increase the impact of awareness measures. They even provide concrete examples within the standards, e.g., brochures, web-based training and posters.

### TABLE 1: SECURITY AWARENESS REQUIREMENTS

<table>
<thead>
<tr>
<th>Security awareness requirements</th>
<th>Regulations</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct requirement</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Target group orientation</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Multiple methods</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Measures upon hire</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Periodic updates</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
• Awareness measures upon hire should be a matter of course for every company. Otherwise, there would be a high level of risk posed by newly hired employees, due to ignorance of company-specific processes, structures and systems. ISO, NIST and PCI explicitly require that newly hired employees participate in an awareness action. This avoids awareness measures for new employees being postponed until the next regular awareness activity.

• Periodic awareness updates are important, too. Otherwise, the level of awareness among the employees would steadily decrease, due to employees’ lack of knowledge of security changes and their waning interest and attention. To counteract this, periodic updates are required in HIPAA as well as in ISO, NIST and PCI standards. However, it mostly remains unclear how “periodic” should be interpreted. The only requirement with a time specification is included in the PCI standard. According to PCI, periodic updates should be carried out at least once a year.

LEVERAGING WHAT YOU NOW KNOW
A company that plans to improve its security awareness program may find interesting approaches and suggestions from the knowledge gleaned from the variety of mandates and recommendations. In all cases, security awareness measures tend to be much more effective and efficient if preceded by diligent planning, which should be founded on appropriate information around security awareness and relevant regulations and standards. 

STEFAN BEISSEL, Ph.D, MBA, CISSP, CISA, PMP, is the head of information security and risk management at AGES Maut System.
Our Journey to the Cloud

(ISC)²’s COO WESLEY SIMPSON explains why the organization decided now was the time to press forth

MOVING TO THE CLOUD is no longer a question of if, but has become a part of our lives both personally and professionally. We are all cloud-based consumers whether we like it or not, and we’re surrounded by its daily use with every action we take (i.e., either online or by interacting with kitchen appliances).

As an organization, supporting and running IT functions is not a competitive advantage that we need to be known for, nor is it where we want to spend our finite time and resources. But by acting as a Sherpa of sorts and pulling our entire infrastructure ecosystem up the mountain and into the cloud, we were able to focus on what really matters to us: our members.

As technology leaders, we are continually challenged with making the right decisions for the betterment of our organization’s bottom line, growth, employees and, at (ISC)², our members’ professional development. By harnessing the power of cloud-based services, we were able to set ourselves up for success across all of those areas. By asking the right questions and understanding the impacts to the business through active employee engagement, we are better able to deflect the inherent risks and stack the odds in our favor as we move toward a cloud-based digital transformation.
NO BETTER TIME THAN NOW
In case you are one of the last holdouts on moving to the cloud, I applaud your risk tolerance for keeping your company safe and secure. But in reality, in order to stay competitive, there is no better time than the present. Our work environment has evolved quite a bit over the last 10 years and, given what our employees and members look for in an organization, we knew that we had to evolve with them to keep pace. Many of the concerns, uncertainties and cost impediments have diminished. It was the right time for (ISC)² to adopt cloud-based solutions.

As the executive sponsor and a strong proponent for this initiative, I had to not only be visible but vocal. The C-suite must fully understand the ultimate business value that the cloud brings to an organization and be ready to articulate it in a way that everyone in the organization can understand and support. The cloud has improved our work life by removing the technological tediousness that plagues so many companies today; it’s also enabled us to become a work-from-anywhere organization.

Technical operations leaders should heavily consider cloud services that are made up of orchestrated technology and/or application elements, not just the individual technology components. Employees display higher levels of motivation on the job when they feel their efforts are closely tied to the organization’s goals and core values. Making the tie to each employee and member can be the spark to sharing how the cloud can help each of them succeed along with the company.

Another driver for us was the need to be more fluid and agile to increase our cyber resilience against breaches. Training our staff to be cyber-conscious when handling company data was a must. Education and security hygiene reinforcements were not optional; they were fundamental to increasing our security readiness to deal with potential attacks, as well as implementing disaster recovery/business continuity plans for hurricane season in Florida, which in the past has temporarily disrupted our headquarters operations.

Technical operations leaders should heavily consider cloud services that are made up of orchestrated technology and/or application elements, not just the individual technology components. There is a range of ways to consume these services, from internal IT teams to third parties providing private or public cloud services.

There are endless reasons for cloud migration—and chances are by now you’ve heard many of them—but only you can decide what is right for your organization, your clients, your members and your level of risk tolerance. Don’t be forced to make a decision just because everyone else is doing it.

1. Lower costs and faster time to market
2. Greater agility to adapt to market changes
3. Faster data consumption
4. Easier adoption of and migration to new technologies
5. A more member-centric approach
6. Lower support costs
7. Unlimited storage
8. Automatic software updates
9. Integration with other cloud-based applications
10. Scalability to innovate to all levels
11. Work from anywhere—access to your desktop and network anytime on any device
12. Disaster recovery and automated backups
13. Increased collaboration
14. Greener technology—provides cost savings on power
15. Remote worker program baseline to drive down office costs and enable a more diverse workforce
16. More efficient storage solutions—many cloud services charge a premium for mundane tasks like attachment storage

—Wesley Simpson

THE INCREASING ROLE OF CASBs
Even though adoption of cloud services is increasing, your future may most likely involve hybrid cloud deployments that increase complexity and the need to strategically handle the delivery of a suite of cloud services. A Cloud Access Security Broker (CASB) is a must-have
tool to provide visibility into cloud instances for security, data loss prevention and other threats. Coupling a CASB with other available tools helps to manage all these complex environments and provide key degradation and incident information for a coupling of cost management and high-level IT operations.

Leaders also should consider the financial drivers for the enterprise. Do we need to work in an Operating Expense (OpEx) or Capital Expense (CapEx) environment and what is the long-term impact of each? Moving to a cloud infrastructure can have a larger OpEx spend, but once the initial projects are completed to move away from on-premises, there is very little to depreciate, and you only pay for what you use rather than having to guess. These are not necessarily negatives if that is the overall strategy of the company and in many cases will be a great driver to balance costs year over year. Imagine not needing to request a brief every three years for new servers and storage, and being able to present a smoother and more consistent IT budget that only grows as the enterprise adds capabilities.

Another key benefit of this model is the lack of outages required to replace older, conventional hardware. By moving these services into the cloud, the cloud provider takes on the responsibility for newer, faster hardware with no downtime needed.

By moving these services into the cloud, the cloud provider takes on the responsibility for newer, faster hardware with no downtime needed.

ENDLESS POSSIBILITIES

Cloud computing has several advantages, from its ability to support bandwidth-intensive applications to its added agility in business processes. But in order to select the right cloud program for your company, it’s important to understand the basics. Cloud storage comes in a variety of service options, including:

- **Software as a Service (SaaS):** Applications are hosted on a cloud infrastructure that can be accessed over the network or program interface, usually through a license model
- **Platform as a Service (PaaS):** Allows organizations to build, run and manage applications without using any IT infrastructure
- **Infrastructure as a Service (IaaS):** Providers deliver computing infrastructure as a part of the service, allowing organizations to self-service via remote data center infrastructure

With cloud computing services, our employees gained the ability to access data and work from anywhere in the world. This flexibility creates collaboration across geograph-
ically dispersed teams, increases operational agility and shortens time-to-market with products and services.

Another benefit we realized was that by removing the physical components to develop and support these on-premises systems, employees could be shifted to other areas within our company to work on initiatives that are truly core to us and tie back to our IP and competitive advantage. We wanted to free up resources to work on those things that would provide the greatest benefit to our members and not get stuck on manual outdated IT technical debt.

CRITICAL QUESTIONS TIED TO CLOUD SUCCESS

Whether you are still weighing your cloud options or committed to a digital transformation (maybe one already well underway), there are some common, important considerations you must make as an organization.

Based on our own experiences at (ISC)², here are questions to ask and amply answer:

• What are your business needs and budget restrictions?
• What security requirements are necessary for your information? Every company must assess its own data and necessary level of protection.

• What role will cloud storage play in the development of your company’s future goals?
• Can your current IT infrastructure and employee skill sets support cloud connectivity?
• What is your company’s risk tolerance if the data is breached?
• What does the transition look like? Full cloud or hybrid deployment?

Whatever you decide with respect to cloud migration, your decisions eventually boil down to understanding your business needs and where you want your teams to spend their time. Cloud capabilities are evolving every day, and no matter what your infrastructure and operations strategy is, there is a cloud solution for you.

For us, it was a logical decision. We wanted to create an environment that would grow with our members and offer global capabilities.

WESLEY SIMPSON is chief operating officer of (ISC)².
FOCUSING ON EDUCATION AND RESEARCH INITIATIVES

BY PAT CRAVEN

The Missing Piece (and How You Can Help Supply It)

IN RECENT YEARS, your Center for Cyber Safety and Education has skyrocketed to success, not just with the addition of Garfield, but in all areas.

The Global Information Security Workforce Study is the largest, most comprehensive look into the changing cybersecurity workforce. Nearly 20,000 professionals from 170 countries participated in the study, which offered a new look into the industry from different angles, including women, millennials and minorities. Every day, someone quotes the results of the research, using it to inspire more people to consider a cybersecurity career.

Just a few years ago, we were excited to have 60 young people apply for our (ISC)² scholarships. This year, that number hit 1,000, thanks to the expansion of the program with corporate support. We have awarded more than $1.2 million in aid. Another positive: more women than ever are getting financial help to earn their degrees.

We have revamped our (ISC)² Safe and Secure Online educational program with new media, materials and messages for parents, senior citizens and children. In 2016, we unveiled our first of three Garfield’s Cyber Safety Adventures that allow a teacher or group leader to provide basic, engaging cyber safety messages to younger children, with better-than-expected results. In fact, we just completed a year-long study of 500 students to measure if the Garfield lessons are really making a difference.

After just 30 minutes, a student’s cyber safety knowledge climbed 28 percent. In some cases, only 30 percent of students could answer a cyber safety question correctly. After the course, the percentage shot up to 90 percent.

We are on a roll, but there is one missing piece of the puzzle. Like (ISC)², the Center is a nonprofit organization. But as a registered charity, the Center relies on donations to meet our budget and grow. So far, we have been able to develop these new programs with the generous financial support of (ISC)², Raytheon, Engility, Pearson and others. But it isn’t enough to realize our vision. We need your help.

The Center currently operates on about a $1 million annual budget, half of what we need to deliver the program internationally. Funding is the major hurdle. Unfortunately, nothing is free, including a safer cyber world.

We have awarded more than $1.2 million in aid. Another positive: More women than ever are getting financial help to earn their degrees.

NO GIFT TOO SMALL AND A PURR-FECT PERK

Donations of any size make a difference. In fact, if every (ISC)² member donated $20, we would raise $2.7 million. Many schools don’t have the funds to teach cyber safety. Your support helps ensure an international reach. Just go to our website www.IAmCyberSafe.org and click on the DONATE button on the top right corner. You can contribute with a credit or debit card, either as a one-time gift or regular monthly donation.

For every $100 donated by December 2019, you will receive a Jim Davis autographed copy of a Garfield Cyber Safety comic book. If you donate $300, you will receive all three books signed by the legendary cartoonist. For $500 or more, contributors get a signed comic strip lithograph, perfect for framing; Jim’s way of saying thanks.

Honestly, I hate asking for money, but it’s the reality of running such a great organization with a vital mission we all share. I hope you will join us in spreading our message. ✧

Pat Craven is the director of the Center for Cyber Safety and Education and can be reached at pcraven@isc2.org.
In 93% of confirmed data breaches, it takes attackers “minutes or less” to compromise a system. It’s critical that you arm yourself with the latest information about the industry.

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

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

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

* 2016 Verizon Data Breach Investigation Report

© 2018 TechTarget Inc.
QUESTION:
Does Adaptive Exam Devalue the CISSP?
I was very surprised to see the exam (English language) is now 100-150 questions. While the material is still demanding, I think the CISSP had a strong reputation as the premier information security certification because it was so rigorous with 250 questions. It was a long, tough exam. And people respected (sometimes grudgingly) those who passed. At 100-150 questions, does this devalue the CISSP? The Security+ is 90 questions. People used to believe the CISSP was several notches above Security+. Now people might think the CISSP is just one notch above, or lump them together. I’m not trying to take anything away from those who passed the adaptive exam. I’m concerned about the long-term implications this has on the value of the CISSP certification in the eyes of IT security professionals.
—Submitted by gphalpin

SELECTED REPLIES:
I believe the new test focuses on content and removes the factor of test-taking skills. Its new format gives you no place to hide. It finds your weakness and keeps up the pressure. The goal of the test is to ascertain the knowledge of the candidate and I believe the new test format does that.
—Posted by Gary23

I prefer the long format. There are a lot of domains to cover in the CISSP. It’s not like a more focused certification and my concern would be that a right guess on a hard question could help you more than hurt, especially if there is a limited pool to cover all domains.
—Posted by CZ

I (provisionally) passed my exam (CAT) today and I can say: [T]hat was some serious sh**! :-) To my mind there is no difference in asking 250 random questions in six hours or 100-150 questions targeting on your weak points.

CISSP is definitely not a certification you can get by just by memorizing books and questions. A strong background/working experience and understanding of information security is essential no matter how many questions there are or how much time you have to answer. I’m now really looking forward to the endorsement process—can’t wait to be a certified (ISC)² member!
—Posted by dersven

The [linear] exam was difficult for me. Not due to the difficulty of the questions; I was well prepared and I answered the vast majority of them with a high degree of confidence. I didn’t rush, I read every question carefully. After answering each one at a time I had 11 minutes left on the clock. I didn’t go back to review my answers, I was too tired. I felt like I ran a mental marathon. I certainly had the knowledge to pass but there was no getting around six hours of testing. That was the hardest part. I feel like a CAT test would’ve been a breeze for me or anyone else who was well prepared.
—Posted by meincke

I give a lot of pushback to those who would suggest that the CAT version is somehow “easy” compared to the legacy linear tests. You got more time on the linear 250-question test and there was the added advantage of going back and changing your answer on the linear test. All of these advantages have been taken away in (ISC)²’s switch to the CAT format. Furthermore, I see no reduction in the amount of “whiners” since the CAT format has been offered. This tells me that the CISSP certification maintains its integrity!
—Posted by Lamont29

I give a lot of pushback to those who would suggest that the CAT version is somehow “easy” compared to the legacy linear tests. You got more time on the linear 250-question test and there was the added advantage of going back and changing your answer on the linear test. All of these advantages have been taken away in (ISC)²’s switch to the CAT format. Furthermore, I see no reduction in the amount of “whiners” since the CAT format has been offered. This tells me that the CISSP certification maintains its integrity!
—Posted by Lamont29

Find this complete and updated thread here: https://community.isc2.org/t5/Certifications/Does-Adaptive-Exam-Devalue-the-CISSP/td-p/9612

QUESTION:
Should there be a standard when listing certifications and degrees in signature blocks or on business cards?
Many of us have received business cards or correspondence that included a line of acronyms following the individual’s name. There doesn’t seem to be an acceptable standard on what should or shouldn’t be included…. So far, the only place I have found it necessary is on my résumé so I can get through the HR filters. The position I am in now requires I maintain a certain baseline, so I do not feel it is necessary to list that information anywhere.

—Posted by Lamont29
The 2018 report reveals:

- the latest data points and trends in cloud security
- how your peers are approaching security
- valuable benchmark data that will help gauge how your own organization stacks up compared with others

Get Your Copy ➔
My past experiences have led me to believe that listing my certifications and education is unnecessary. Recently, however, I have begun to wonder if we as a community are missing an opportunity to open lines of communication by not advertising all the different ways to contribute to the field. I look forward to your responses.

—Submitted by DAlexander

SELECTED REPLIES:

In my correspondence, I don’t list anything. I do this for one particular—and a little selfish—reason: I want my discussions, arguments and statements to be judged on their own merit rather than be defended by a qualification. When I succeed, I often get asked something along the lines of, “Where did you learn that?” That is the opportunity to discuss qualifications, learning paths and life experiences.

—Posted by Boechle

When I see someone with the alphabet soup, I look to see what I have in common with that person and use the language of a cert to establish a connection. I also see a person with certs as someone who is taking a role seriously and who is working on staying current and valuable.

—Posted by PlannerKSH

In several countries it is common to use the academic or other title as a means of introduction. Instead of saying “Mr. X,” we use “Engineer X” if they have technical education, “Magister X” if they have humanities-based education. I feel I have to honor this code and list my highest professional credential (in my case, SSCP). I got asked once how I should be introduced; in the end, the host insisted on calling me “Mr. Sedlacek, system security certified professional.” So, it depends on culture basis as well.

—Posted by Illsteward

When I read certs in a signature, I like it. It’s a way of establishing a baseline of knowledge I can (often) assume they have to start a conversation. If it’s a cert I’ve never seen before, I now have something to talk to them about and a way to get to know them a little better.

—Posted by crossmage

Find this complete and updated thread here: https://community.isc2.org/t5/Career/Listing-Certifications-and-Degrees-in-Signature-Blocks-or/m-p/9820

Find the Root Cause of Your Vulnerabilities

Most penetration test providers only report on vulnerabilities. Our penetration test analysts use a thorough discovery process to uncover weaknesses and report on why you are vulnerable.

Let’s talk about your penetration test needs info.securitymetrics.com/isc2-pen-test
AWS Security Automation and Orchestration (SAO) offers secure, automated deployment and continuous risk treatment for 11 common security frameworks.

SAO methodology enables AWS customers to constrain, track and publish continuous risk treatments (CRT) configurations.

SAO assimilates DevOps CI/CD philosophy into a Type Accredited secure AWS architecture which is configured to converge common security frameworks like PCI-DSS, FedRAMP, DoD CC SRG, IRS 1075 and more through the use of security as code practices.

The initial 11 type accreditations not only accelerate the Authority to Operate (ATO) for the customer, they also create an automated pipeline to ensure that our customers can keep the accreditations intact while they deploy agile software development and release management practices.

This accelerates both AWS adoption and customer value by streamlining the accreditation and compliance process, while providing a defined workload migration and modernization platform.

Fast Track
Secure automation deployment for regulated verticals like PCI-DSS, FedRAMP, DoD CC SRG, and IRS 1075.

Increase Speed
For AWS customers to achieve Authority to Operate (ATO).

Assimilate
SecOps and DevOps practices into a Governance as Code (GoC) cycle for secure operations and orchestration, as our customers look to become more agile in their adoption of AWS.

Type Accredit
Automation packages through APN Consulting Partners like Anitian and Coalfire.
Sunshine State of Mind

See you in Orlando 2019

October 28-30

Walt Disney World Swan and Dolphin Resort
Orlando, Florida

Register Now for Advanced Savings
$100 OFF thru Dec. 31 on 2019 All Access Pass with code ALLACCESS100.

congress.isc2.org | #ISC2Congress
Are you short on time or in-house talent and need help?

Get expert white paper writing and design services

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

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

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

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

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