‘WEIGHING’ IN ON NEW EXAMS

WHAT LIES BENEATH
The Shadowy Side of IT

CREATING YOUR PERSONAL LEARNING NETWORK
WRITING A BOOK IS FAR FROM CHILD’S PLAY

also
AMERICAS ISLA WINNERS
LETTING GO OF LEGACY NIPS
5 MINUTES WITH TUSHAR GOKHALE
GET EMPLOYERS’ ATTENTION

CREDENTIALS THAT SET YOU APART

EARN UP TO THREE NSA DIGITAL BADGES on your way to a degree at a nationally recognized university. Badges are offered for these information assurance and security (IAS) programs:

<table>
<thead>
<tr>
<th>PURSUE A DEGREE IN:</th>
<th>EARN AN NSA DIGITAL BADGE IN:</th>
</tr>
</thead>
<tbody>
<tr>
<td>🎓 Bachelor’s in IT – IAS</td>
<td>🗡 Information Assurance and Security</td>
</tr>
<tr>
<td>🎓 Master’s in IAS – Digital Forensics</td>
<td>🗡 Digital Forensics</td>
</tr>
<tr>
<td>🎓 Master’s in IAS – Network Defense</td>
<td>🗡 Security Incident Analysis and Response</td>
</tr>
<tr>
<td></td>
<td>🗡 Network Security Administration</td>
</tr>
<tr>
<td></td>
<td>🗡 Network Security Engineering</td>
</tr>
<tr>
<td></td>
<td>🗡 System Security Engineering</td>
</tr>
</tbody>
</table>

Capella University has been designated by the National Security Agency (NSA) and the Department of Homeland Security as a National Center of Academic Excellence in Information Assurance/Cyber Defense for academic years 2014-2021.

GET RECOGNIZED FOR WHAT YOU KNOW. START TODAY.
CAPELLA.EDU/ISC2 OR 1.866.933.5836
FEATURES

› TECHNOLOGY
15 What Lies Beneath
It’s time to cast a stronger light on the shadowy side of IT.
BY JAMES HAYES

› PROFESSIONAL DEVELOPMENT
21 It’s Not Just Who You Know ...
... or maybe it is. Expand your professional potential by building a Personal Learning Network.
BY KERRY ANDERSON

› PROFESSIONAL DEVELOPMENT
24 Playing by the Book
How an (ISC)² member creates children’s books also meant for their elders.
BY CHRIS GRECO

Cover image: JOHN KUCZALA. Image (above): ROBERT PIZZO.
WHAT ‘KIND’ OF INFORMATION SECURITY PROFESSIONAL ARE YOU?

Of all the excellent advice delivered during a Security Congress session on building and retaining security teams, the piece that stood out most to me came from Deidre Diamond, founder and CEO of Cyber Security Network. Her secret tool to hold on to good employees: kindness.

“It’s the number one thing that everyone wants from an employer,” Diamond says in an abbreviated transcript of the session published online.

If kindness is all it took to keep top talent, you’d think no one would leave. But, it turns out, compassion and consideration become more scarce as people rise in rank. UC Berkeley psychology professor Dacher Keltner discovered that as people gain power or privilege, they are less likely to demonstrate empathy, collaboration and openness toward others—not just in politics and professional sports, but in the workplace too.

How can you tell if you practice empathy, gratitude and generosity—three cornerstones of kindness? Consider your own behavior toward your colleagues and direct reports. “Studies show that people in position of corporate power are three times as likely as other employees to interrupt coworkers, raise their voices, and say insulting things at the office,” Keltner writes in the October issue of Harvard Business Review.

And the result? “In a recent poll of 800 managers and employees in 17 industries, about half the respondents who reported being treated rudely at work said they deliberately decreased their effort or lowered the quality of their work in response,” Keltner reports.

This gives credence to Diamond’s recommendation and should serve as a warning to anyone in, or seeking, a senior-level position, today or 10 years from now. If you aren’t already, learn how to listen earnestly to others. Deliver thoughtful thank yous. Acknowledge good work and those who did it. Give praise generously (and genuinely).

Do this for both your present you and your future you. After all, as the famous saying goes, “Be nice to those you meet on the way up, for they are the same people you’ll meet on the way down.”

—Anne Saita

ADVERTISER INDEX

For information about advertising in this publication, please contact Tim Garon at tgaron@isc2.org.

Capella........................................................................ 2  
(RSC)^2..................................................................... 12
RSA ............................................................................ 5  
Center for Cyber Safety & Education............. 13
(RSC)^2................................................................. 7  
(RSC)^2................................................................. 20
Pearson ................................................................. 9  
Twirling Tiger Media............................................. 29

© Rob Andrew Photography
ATTEND RSA CONFERENCE 2017 FOR LESS!

Save $200 with your (ISC)² member discount code.

From February 13–17, the (ISC)² community will come together in San Francisco at RSA Conference 2017, the world’s largest infosecurity event.

Join your peers and discover:

- Over 555 sessions covering a range of topics to help you stay on top of threats and solutions.
- (ISC)² CCSP Two-Day Crash Course covering the six domains in the Certified Cloud Security Professional CBK.
- (ISC)² CISSP Two-Day Crash Course covering the eight domains in the Certified Information Systems Security Professional CBK.
- More than 550 exhibitors in two Expo halls.
- Four days of enlightening and inspiring keynotes, led by speakers such as Dr. Neil DeGrasse Tyson, Amit Yoran and many more!

Visit www.rsaconference.com/isc2 to register today!

Use code 1U7ISC2FD when you register to save $200 off a Full Conference Pass.
Furthermore, we seek to assess test takers by asking questions to measure a latent psychological trait: in our case, the vast knowledge and practice of securing information.

While examinations and their development need to be secure, they don’t need to be a mystery. To this end, (ISC)² for the first time recently approved publishing examination domain weights. Now candidates will know not only the content areas to be assessed, but also what proportion of an exam will be dedicated to these sections.

Publishing the percentages of items dedicated to each exam domain is not only good testing practice, it is a giant leap forward in providing necessary clarity to ensure that our standards of validity and reliability continue to stand up to public scrutiny.

(ISC)² cares a great deal about its certification programs. We have sought ANSI 17024 accreditation for nine of our 10 professional certifications. How difficult is it to earn this mark of excellence? Of the more than 3,000 certification programs in the United States alone, fewer than 200 reportedly are ANSI-accredited.

In obtaining this prestigious recognition, we must demonstrate that (ISC)² adheres to the highest industry standards in examination development, administration and security. We subject our programs to continuous third-party audits to demonstrate that our exams are valid, that they actually measure what they intend to measure, and that they are reliable. Indeed, the examination development at (ISC)² has always been world-class on these important psychometric principles. Now, we hope to improve on how we talk about these concepts.

Dr. Casey Marks, a 20-year psychometrist, is the director of examinations and customer experience at (ISC)². He can be reached at cmarks@isc2.org.

Now candidates will know not only the content areas to be assessed, but also what proportion of an exam will be dedicated to these sections.

Publishing domain weights at this time provides necessary guidance and focus for candidates in their educational preparation. Additionally, it provides a convenient remediation heuristic for candidates who do not pass an exam on their first attempt.

Rest assured, the exam is certainly not any easier than when you passed it. As what is “testable” in information security continues to grow, so will our focus on certifying professionals who are best able to help us inspire, and create, a safer and more secure cyber world.
Are you getting the most out of your (ISC)^2 membership? Whether you are looking for CPEs to maintain your certification, avenues to network with your peers, or resources to help you stay on the cutting edge of information security, your membership provides these benefits and more.

- Free Digital Member Magazine
- Digital Badges and Certificates
- Free Online Events
- Access to Exclusive Information Security Reports
- Vulnerability Central and many more

Member Benefits

(ISC)^2 continues to strive to partner with industry leading organizations to deliver discounts to provide more value to your membership. These help you stay relevant in your career, introduce you to the top resources, and help you save money and time.

- Discounts on Industry Conferences, such as BlackHat and RSA
- 1-Day SecureEvents
- Service and Subscription Discounts
- 50% Off on (ISC)^2 Official Books, Study Guides, and Other Resources

Member Discounts

www.isc2.org/member-benefits.aspx

www.isc2.org/member-discounts.aspx
(ISC)² SALUTES THE 2016 AMERICAS ISLA WINNERS

The Sixth Annual Americas Information Security Leadership Awards (Americas ISLA®) were presented at the 2016 (ISC)² Security Congress in Orlando. Americas ISLA, part of (ISC)²’s Global Awards Program, recognizes the achievements of outstanding cybersecurity professionals who have led a workforce improvement initiative, program or project in Central, North or South America.

Jim Davis, the creator of Garfield®, provided the keynote address during a banquet ceremony. Garfield, the iconic cartoon cat featured in the Garfield & Friends series, is the spokesperson for the Center for Cyber Safety and Education’s Safe and Secure Online program.

“We are excited to honor the Americas ISLA recipients once again this year,” says (ISC)² CEO David Shearer. “These professionals are advancing our industry and truly making a difference in the cyber world.”

The 2016 Americas ISLA winners are:

**Senior Information Security Professional**
Diego Andres Zuluaga Urrea, Information Security Officer, ISAGEN S.A. (Colombia)
**PROJECT:** Colombian Energy Sector Cyber Security Improvement

**Information Security Practitioner**
Mack Bhatia, Senior Practice Director, Enterprise Integration (U.S.A.)
**PROJECT:** Enterprise Integration – SOC 2 and SOC 3 Compliance

**Up-and-Coming Information Security Professional**
Jennifer Chermoshnyuk, Paralegal, Davis Wright Tremaine LLP (U.S.A.)
**PROJECT:** Continuing Legal Education Program

**Community Awareness**
Sandra Toner, Senior Technical Specialist, ICF International (U.S.A.)
**PROJECT:** Online Cybersecurity Awareness Tools

For more information on the Americas ISLA program, please visit www.isc2.org/aila.

IN REMEMBRANCE
(ISC)² BANGALORE CHAPTER PRESIDENT SHEKHAR BOSE

Shekhar Bose, president of the (ISC)² Bangalore Chapter in India, died unexpectedly on Sept. 3, 2016.

An (ISC)² member since June 2007, Bose was the founding president of the Bangalore Chapter. With his and the chapter officers’ efforts, the Bangalore Chapter grew from 43 members in 2014, to 63 members in 2015. In an interview for the March Chapter Connections online newsletter, Bose spoke of wanting to increase the chapter activities by providing more member benefits to the local community. His energy and enthusiasm will be greatly missed.

He is survived by his wife and daughter.

**Top 10 Wearable Technologies and Capabilities for 2017 and 2018**

1. Biometric authentication
2. Mobile health monitoring
3. Energy boosting using harvesting
4. Virtual personal assistants (VPAs)
5. Smart coaching
6. Embedded security
7. Conformal electronics
8. Wearable processors
9. Virtual and augmented reality
10. Accurate motion recognition

Source: Gartner, August 2016 Report
100% Online Master of Science in Cyber Security

The front lines of digital defense are looking thin. **Become an in-demand expert.**

CNBC estimates a need for **30,000 top-level security experts** worldwide. Those experts are consistently earning more than six figures annually, according to payscale.com. The numbers don’t lie – there has never been a better time to specialize your skills. Elevate your technical abilities in booming areas like cloud security, wireless network security, and mobile device hacking. Housed within the John E. Simon School of Business, Maryville University’s Online Master of Science in Cyber Security program helps you develop the business literacy to influence, and even enter, the C-suite.

Earn your advanced degree. [START TODAY](ONLINESECURITY.MARYVILLE.EDU/STARTTODAY)

- Graduate in as few as 18 months.
- Complete your coursework 100% online, on any device.
- Use our Maryville Virtual Lab as a professional training ground.
- Learn from a faculty dedicated to the profession.
CHAPTER SPOTLIGHT: (ISC)² CHILE CHAPTER

CYBERSECURITY: CRUCIAL IN EVERY LANGUAGE

SANTIAGO, CHILE HOSTED the first Spanish-language secure event, (ISC)² SecureChile, organized by (ISC)² Chile Chapter in partnership with the (ISC)² Latin America Office. “Information Security: A Task of All” was attended by 100 information security professionals, from management to C-level.

The keynote speaker, James Harris, a former senior management official from the U.S. Federal Bureau of Investigation’s Cyber Division, briefed the audience on a project studying why users make bad choices when it comes to cybersecurity and how training and education can improve their decision-making.

Other presenters included representatives from major businesses, including Telefónica, Neosecure, Deloitte Chile, Assertiva and Grupo SURA as well as (ISC)² Chile Chapter officers, who emphasized the importance of (ISC)² certifications and the initiatives in Latin America to increase awareness of (ISC)². The day wrapped up with a panel featuring three female CISOs representing their companies, CODELCO, NEXUS and SINACOFI, who discussed security management challenges in BYOD, big data and IoT.

“It was an honor and privilege to have been part of this first Secure event in Chile. The experience was enriching, both for the content of the presentations and for the great opportunity of networking with other professionals. This is an initiative that must be repeated every year,” said Javier Toro Rodríguez, head of regulation and security compliance and risk and security management for RedBanc.

“Carrying out the first Secure event in the Spanish language in Latin America was a major achievement for the (ISC)² Chile Chapter. Definitely, the success achieved will encourage the professional community to join the activities of our chapter, and also demonstrate the high quality of the professionals that are part of the (ISC)² membership. There is no doubt that (ISC)² SecureChile met the needs of non-commercial events at the international level,” said Wilson España, president of (ISC)² Chile Chapter.

27 percent of corporate data traffic will bypass perimeter security by 2021, up from 10 percent today.

210 percent increase in the adoption of bug bounty programs since 2013.

Source: Gartner, August 2016 Report

Source: Bugcrowd’s 2016 State of Bug Bounty Report released in September

(ISC)² CHILE CHAPTER CONTACT INFORMATION

Chapter President: Wilson España
Email: isc2chilechapter@gmail.com
Website: http://www.isc2chile.cl/
PITTSBURGH HIGH SCHOOL STUDENTS TACKLE THE DARK SIDE OF CYBER

REAL-WORLD SITUATIONS provided the material for high school students to test their cybersecurity know-how in a series of exercises, including a hostage rescue operation presented by experts at Carnegie Mellon University’s Software Engineering Institute. Seventy-five Pittsburgh students, from freshmen to seniors, got a firsthand look at the dangers lurking in cyberspace, including identity theft, social engineering attacks, malware, and its cousin, ransomware. They learned how to protect computer systems using the latest Windows and Linux security tools and techniques and state-of-the-art network simulators.

(ISC)³ board member Dave Kennedy from the security firm TrustedSec spoke to the teens about his early days of hacking.

For the hostage rescue exercise, students, assisting a Navy SEAL team, hacked into the power grid and disabled the building lights where hostages were, and at the same time defended their drone infrastructure from attacks, all the while providing cyber support for the SEALs.

The competition event, co-hosted for the second year by SEI’s CERT Division, featured US$1,500 in prizes provided by TrustedSec.

“This competition reflects the commitment of the SEI, (ISC)³ and TrustedSec to providing opportunities for STEM education and experiences to young people,” said Chris May, technical director of the workforce development team in the SEI’s CERT Division. “Events like these help address a gap in teen education and inspire the next generation of cybersecurity professionals.”

Jonathan Frederick, cybersecurity exercise developer for the SEI’s CERT Division and vice president of the Pittsburgh Chapter of (ISC)³, added, “Since its inception, our chapter’s primary focus has been to provide outreach to the Pittsburgh region. IT security professionals from businesses throughout the area collectively realize the importance of educating our successors.”

For more information on this event visit http://isc2chapterpittsburgh.com/, https://www.trustedsec.com/, http://www.cert.org/.

9 Highest Paying IT Jobs
(2016)

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Average Annual Salary (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud computing</td>
<td>$115,826</td>
</tr>
<tr>
<td>IT architecture</td>
<td>$113,499</td>
</tr>
<tr>
<td>IT security</td>
<td>$104,949</td>
</tr>
<tr>
<td>Business technology</td>
<td>$101,663</td>
</tr>
<tr>
<td>Java developers</td>
<td>$99,763</td>
</tr>
<tr>
<td>Project/program management</td>
<td>$98,607</td>
</tr>
<tr>
<td>Data warehousing/business intelligence</td>
<td>$93,522</td>
</tr>
<tr>
<td>Business application development</td>
<td>$92,037</td>
</tr>
<tr>
<td>Voice engineering</td>
<td>$91,489</td>
</tr>
</tbody>
</table>

RECOMMENDED READING

Cloud Computing: Assessing the Risks
By Jared Carstensen, Bernard Golden and JP Morgenthal

Suggested by Larry Marks, CISSP

AS THE CLOUD becomes a partner in more and more enterprises, the need for in-depth information on the benefits and risks grows as well. This book, though a few years old, is a good investment, especially for those professionals working to bring cloud computing to their companies. The authors provide step-by-step guidance to the various components, governance and liabilities that may impact performance. The authors identify the top security risks related to the cloud, the impact of DevOps, and the risks of auditing application security.

The authors highlight the means of performing forensics in the cloud and reviewing the location of the data in regard to international requirements such as EU Privacy Directive 2002/58/EC. They make a point of indicating that the information security professional has to collaborate with the business or process owner to help these stakeholders better understand their risks related to cloud, and better grasp the concepts.

Real-life scenarios are presented, such as: When I am done, how do I de-provision and transition assets out of the cloud vendor to another location of another context? Also included is an overview of cloud deployment models and other cloud concepts so the reader has the proper foundation. I found this book to be a practical guide that can apply to a variety of cloud possibilities that any employer will consider. It is a good supplement to any understanding of the risks that professionals should concern themselves with when reviewing security for the cloud.

(ISC)² MEMBERS

Download Your Certificate DIGITALLY

Based on member feedback, you can now download a digital PDF certificate!

Your digital certificate is available under My Profile.

Download my certificate
It’s easy to see that teachers, librarians, and media specialists need more quality information and resources to address cyber safety in the classroom and at school!

We believe everyone has the right to access the internet without fear of compromising their safety or identity. However, in the Center’s 2016 study of children grades 4-8 we found a few alarming results:

- **62%** Went to adult websites after a search
- **21%** Watch adult programming online
- **49%** Are online at 11pm or later on school nights
- **40%** Have connected with or chatted online with strangers
- **11%** Met a stranger in person after meeting online

You can choose to support any of the following:

- **Child** – 1 Individual Packet
- **Classroom** – 1 Educator’s Kit
- **Grade** – 3 Educator’s Kit
- **School** – 15 Educator’s Kit
- **Girl Scout Troop** – Patches for a Troop of 10 Scouts

(*Quantities are not limited*)

Please click here to make a donation. **Donate Today!**
Why Your Legacy Network IDS/IPS Needs to Be Replaced ... NOW

BY RODRIGO CALVO

GHOSTNET, STUXNET AND DUQU are just a few examples of advanced persistent threats (APT) that demonstrate the complexity used by hackers to exfiltrate information from internal networks. We’ve all heard about these attacks, but are we prepared to prevent them?

Let’s assume that our perimeter is full of firewalls and network intrusion prevention systems (NIPS) based on stand-alone legacy and not OSI Layer 7 technologies. Is that enough?

I asked a lot of colleagues about the best defense for APTs and confirmed with the Gartner MQ for IPS from 2015 this common perception: NIPS, with the technologies that we recognized five to 10 years ago, cannot provide comprehensive protection. It’s necessary to have additional support that can handle analysis of advanced threats and interact with other security tools. That kind of protection has many names: UTMs, NGFWs, NGIPSs and ATPs.

Yet legacy tools exist because many of us work for organizations that lack the resources to fully replace them. In those instances, we must find better solutions that complement our current corporate security model. Figure 1 graphically demonstrates the idea of protecting the environment and minimizing the risk with a solution that can collect security data at multiple levels, prioritize and provide intelligence from email, endpoint and network events. Even better if the solution can integrate actions for a quick incident response.

A use case of such multilevel integration on a single solution could include:

- Correlated information from multiple sources. But in contrast to a SIEM solution, the technologies being used could block malicious traffic, suspicious files, or send a command to the endpoint protection solution in order to isolate it and let the security team analyze the evidence for further actions.
- Use of reputation services from the cloud to compare against network events.
- Alerts of events from the host IDS/IPS in order to bypass SSL traffic (or any potential attacks across that channel).
- Network events in which host IDS/IPS information will feed back to the solution’s infrastructure to determine if there is some sort of advanced attack going on.

The time has long passed when the IT department just waited for the antivirus provider to get a virus definition (or vaccine like many people called it a few years ago) for a virus. Now it’s necessary to have more information to understand at least:

- Source of the attack
- The logic of malicious code attacking the company (files, registry creation, network connections, etc.)
- Actionable recommendations

No doubt APT protection solutions add crucial benefits for customers. So, as budget seasons are underway, it may be time to evaluate the market and find the best option for our companies.

FIGURE 1: Comparative between Legacy NIPS and Modern ATP approaches

Legacy NIPS
- Classic malware detection
- Signature database

Modern advanced threat protection approaches
- Advanced persistent threats-based detection
- Cloud-based sandboxing and/or payload detonation services
- Advanced evasion techniques detection
- Protocol anomalies detection
- Behavioral monitoring or heuristics
The cloud has a dark lining. Shadow IT, or stealth IT—those enterprise computing solutions created and deployed by end users without approval of IT management—has made its way into the cloud, uncontrolled and unchecked. The 2015 Global CIO Survey, conducted by New York-based Logicalis, has suggested that shadow IT is “now a fact of life for the majority of CIOs,” with 90 percent of IT chiefs polled admitting that they are “now bypassed by line-of-business colleagues at least occasionally.”

So what’s a cybersecurity professional to do about it?

It’s time to cast a stronger light on the shadowy side of IT.
TWO SIDES TO A SHADOW
As its proponents seek to re-label shadow IT less threateningly as “flexible IT” or “devolved IT,” caught-in-the-middle CIOs are being advised to stop trying to quash the trend, and instead enfold it into their management plans. More fatalistic IT chiefs have thought hard about bringing shadow IT into the sphere of progressive enterprise IT strategies, but may retain an anti-shadow stance toward C-suite executives susceptible to sharing shadow’s perceived business benefits.

Corporate information security specialists and their security teams are less likely to be beguiled by claims from pro-shadow lobbyists; rather, as an expectation arises that—even though they have no innate influence over, or knowledge of, shadow IT adoption—they should bear responsibility for defusing security-related incidents where shadow is the known source. As shadow IT proliferates, so too will the system security-related issues that it is likely to cause.

“We are seeing that shadow IT concerns are now growing, due in part to the realization that the enterprise IT function cannot evade having to take on some ownership of the problem,” says Nigel Hawthorn, EMEA marketing director at Skyhigh Networks, based in Campbell, Calif. “This is because other enterprise departments—such as risk and compliance, as well as external auditors—are increasingly demanding information on shadow IT usage.”

SAVING MONEY—OR RISKY BUSINESS?
“It is tempting to see shadow IT as a way of cutting costs,” says Owen Wright, assurance director at London-based Context Information Security. “But in my experience, a short-term saving can be undone several times over if there is a security breach, or if a shadow system [that becomes business-critical] later needs significant refactoring to be integrated with the rest of a company’s IT systems.”

Addressing the shadow IT issues on a variety of fronts will also entail additional costs across the business, predicts Andy Buchanan, area VP at RES Software, based in Radnor, Pa. “Infosecurity professionals understand that IT environments are more vulnerable to attacks than ever, and are therefore focusing heavily on internal and external audits—which are extremely time-consuming and costly,” he says.

“With new government regulations—notably, the forthcoming EU General Data Protection Regulation—the cost and burden of compliance is going to rise, especially if shadow IT increase continues. Ultimately, organizations that fail to rein in IT shadows will face stringent fines and punishment.”

Such turns of events may not, however, necessarily bring forth concessionary quid pro quos from unrepentant business unit managers who are signing off on shadow IT activity, points out Jonathan Sander, VP of product strategy at Los Angeles’ Lieberman Software.

Although many CIOs are now “keenly aware” of security issues around shadow IT, he says, it does not mean that they can find it when it exists.

“CIOs are now actively engaging the business—the source of shadow IT—to find things out. They are discover-
ing that they can only get answers when they ask the right questions, [so] they are now asking their business leaders [directly] about IT that is happening outside of normal channels.”

These communication shortfalls do not, of course, necessarily mean that certain shadow services buyers are also procuring their own security solutions: 52 percent of 1,200 business surveyed in an April 2016 report on cloud security by Santa Clara, Calif.-based Intel Security “still expect IT to secure their unauthorized department-sourced cloud services.”

CONFLICT OF INTERESTS?
A further complication is the possibility that a cloud service provider is working at the same time both “over the counter” with a client’s IT department and “under the radar” with separate business unit contacts.

The scope for confusion is obvious, says Skyhigh Networks’ Hawthorn. “Some cloud providers’ business models include promoting a free service to users, after which they approach the users’ IT departments to show them how many users they have, in an effort to justify it becoming a paid service.”

Having two or more “routes to market” can muddle matters, potentially leaving the company to pay for more licenses than it requires, Hawthorn warns.

“Some of the more dangerous shadow IT scenarios we have seen have involved business leads creating their own internal application development teams, and launching apps in cloud-hosting environments with little or no involvement by the IT department,” says Ben Desjardins, a Washington, D.C.-based security solutions director at Radware. “Some will even argue that SaaS providers may be better at securing data than their organization’s own IT team.”

Desjardins’ point underscores the fact that enterprise shadow IT is not confined to business workgroups; indeed, according to a 2013 report from Frost & Sullivan’s strategic forecasting practice, Stratecast, IT staffs use a higher number of non-approved SaaS applications than their colleagues. “It appears that, in acting as the guardian of corporate technology, the IT department considers itself exempt,” writes report author Lynda Stadtmueller at Stratecast.

KNOW THE RISKS
It is important when seeking insight into degrees of shadow IT risk to distinguish between the liabilities of shadow IT per se, and those liabilities arising as a direct consequence of shadow IT deployments, says Context’s Wright. The real challenges that shadow IT raises, such as lack of control

Ascertain the degree of understanding of shadow IT risk at C-suite level, and ensure that senior executives have access to guidance that informs both sides of the pro/anti arguments.

Ensure that any recommendations or proofs provided in favor of shadow IT are balanced against reliable and quantifiable information about verified security risks, and are set forth in the broad context of possible outcomes in the event of a problem.

Review enterprise IT procurement policies to identify any causes of delay that could be eliminated, providing end users with a “valid” excuse for localized IT purchase decision-making.

Ensure that standard IT procurement procedures are communicated throughout the enterprise, eliminating any possibility that shadow IT consumers can claim that they had not been made aware of official procedure toward new product acquisition.

Develop enterprise IT procurement policies and guidelines that contain provision for end-user requests for non-standard technology to be speedily brought under full consideration by the information security function.

Communicate information about potential security risks of unauthorized IT procurement, supported by examples and by commentary from directorate heads in the legal, financial and governance departments.

—James Hayes
over system configurations and failures in asset management, “are common information security manager worries.”

Michael Hack, SVP EMEA operations at Ipswitch, based in Lexington, Mass., has no doubt that shadow IT is a significant and persistent risk for information security management, but is one that is “often underplayed” because “it is seen as a ‘creeping’ problem [that] does not impact on the business in the same dramatic, headline-grabbing way that a debilitating virus or major data breach does.”

There’s an element of “reverse polarity” at play here, Hack suspects, because market studies have indicated that internal threats arising from human error or misjudgment (and many would regard shadow IT activity as such) remain at the top of the list of cybersecurity headaches for organizations of all types and sizes—and indeed pose a more acute threat than external menaces such as viruses and intrusive attacks.

“Shadow IT apps are [usually] installed with the best of intentions, and a desire to improve business efficiency,” Hack says. “This means they are not ranked as highly on the information security risk scale as Trojans, for instance, or other kinds of malware…. But their risks are potentially as devastating, particularly when it comes to a company’s ability to comply with constantly changing data privacy and protection laws or to thoroughly encrypt its data.”

THE DANGERS LURKING IN THE SHADOW

The adverse impacts of a security incident arising from a shadow IT deployment can be generally assigned to three groups. The possibility that shadow IT could provide an entrée to external cybersecurity threats is, of course, a critical concern, but ways in which proliferating, unsanctioned technology might introduce additional security-related problems also need to be factored into any risk assessment.

1. Endangering the System

Best IT management practice is about ensuring that optimal performance value is derived from IT assets in order to maximize returns on investments (ROI). Any factors that put technological well-being at risk and hamper IT management should necessarily be regarded as threats to infrastructural stability and performance, some systems experts believe.

“Use of non-approved software can have a number of adverse effects on the network [it runs over],” says Ipswitch’s Hack. “[Such software] can consume a large amount of bandwidth, for example, which in turn slows down the network, and can cause compliance and data sharing issues.”

Shadow IT at its most unrestrained can result in “unmanageable systems,” warns Context’s Wright: “For example, an organization might have fully aligned to the Microsoft stack, including .NET web applications, based on Internet Information Services and SQL server hosted in the Azure cloud infrastructure,” Wright explains. “If a business team were to deploy an application based on PHP, MYSQL and Linux into an Amazon AWS environment, they would then need to manage an entirely different stack of technology—and all of the complexity involved.”

“If a [business] team were to deploy an application based on PHP, MYSQL and Linux into an Amazon AWS environment, they would then need to manage an entirely different stack of technology—and all of the complexity involved.”

—MICHAEL HACK, SVP EMEA operations, Ipswitch

Should the respective business team move on, responsibility for this can fall back to the core IT department, resulting in systems where no one within the organization has the technical capability to manage them, Wright says, and where existing data security standards, processes and policies cannot be applied, (because) they are tailored for a different platform: “Thus, an upfront saving in time and money to deploy quickly can lead to significant ongoing expenses further down the line.”

2. Challenging Security Regulations

Shadow IT can negatively impact regulatory compliance and legislative requirements that all businesses are now subject to. In Europe, the impending European Commission General Data Protection Regulation (GDPR) intends to strengthen and unify data protection for people within the European Union. It also addresses export of personal data outside the EU, so it will affect companies and other organizations around the world.

3. Creating Breach Opportunities

The possibilities of breaches of IT systems, resulting in infiltration of an enterprise computing resource, data theft,
denial or impairment of service, and the installation of malware (such as ransomware) are well known. A high proportion of cloud apps have been found to be not “enterprise-ready,” lacking the baseline security, audit and certification capabilities required for workplace use. Unsecured applications could be used for months without the employees who set them up being aware that their cost-effective self-sourced application has been compromised from day one—even the details of the credit card they used to make the purchase online have likely been filched.

A data breach resulting from a shadow IT instance will result in financial liabilities affecting the organization’s bottom line, warns Gartner’s Brian Lowans: “Liabilities can be very large due to a mix of costs that include notification penalties, auditing processes, loss of customer revenue, brand damage, security remediation and investment, and cyber-insurance.”

WHO IS RESPONSIBLE FOR THE SHADOW’S RISKS?
The question remains: Who takes the flak when shadow IT is at fault? “If a business team has ignored company processes in order to deploy systems in contravention of company policy, then it’s likely they will bear the brunt of any immediate fallout,” suggests Context’s Wright, “but any resulting data breach is a problem for staff across an organization.” Information security will likely end up having to find time to deal with the outcome in either case, distracting them from scheduled work that might be of greater importance.

“The risks of shadow IT are quantifiable: the risk of breach, of noncompliance, of IT failure, of lack of control,” says Nathan Dornbrook, CTO at Glasgow, U.K.-based ECS. “The risks of not using shadow IT are also quantifiable—cost and time—[the difference being that] these risks can be managed…. Ultimately, business risk is owned by the business, not by IT, so violators of these policies need to be handled by the business.”

IT’S OUT THERE ... SOMEWHERE
How big of a problem is shadow IT? How widespread is its use? How can it best be managed? These questions and more pose a challenge to information security professionals seeking to introduce better security management over shadow IT. Up until now, IT managers could detect evidence of use of unauthorized cloud apps and service through usage pattern alerts, email monitoring and traffic logs. But it is getting harder for IT to detect the use of rogue SaaS, as shadow-minded users have become more covert—especially given the increase in mobile enterprise platforms that might have no direct touch on the main enterprise IT systems.

“Cloud services make it harder to discover unofficial systems associated with a company as they often do not reside within the company’s own network space,” says Wright, “making it harder to discover using common inventory management or network scanning processes and tools.”

RES Software’s Buchanan agrees. “Based on conversations we have with customers, it is becoming increasingly difficult for security professionals to discover and keep track of the shadow IT usage in an organization. This is largely due to the [the closer coupling of] cloud and mobile, as individuals, and indeed department leads, can now easily go to a cloud service and leverage their tools and services.”

Adds Ipswitch’s Michael Hack: “Monitoring shadow IT deployment and use on corporate networks is [now] one of the main reasons that infosecurity professionals need a fully integrated and multifunctional network management tool.”

“Network monitoring tools that can help safeguard the network’s performance, monitor the availability of applications and prevent misuse, continue to evolve—and even advance into the realms of bots, artificial intelligence and machine learning. But right now, network-monitoring solutions that make use of advanced visualization technology are already coming onto the market. The best of these solutions can intuitively map the user experience directly to the environment that the IT team originally created, allowing team members to easily understand irregularities—such as shadow IT deployments.”

Corralling shadow IT into a more managed context calls for revised terms of engagement between the business and the IT team, suggests David Emm, principal security researcher at Kaspersky Lab based in Woburn, Mass. One of these could include new reciprocal ground rules designed to get the message across that security policies have a critical purpose, and exist to protect all staff from threats of which they probably have limited comprehension.

“In today’s business world we have ‘always-on’ staff conducting business with an assortment of devices and solutions,” Emm says, “so businesses must be able to apply a ‘security wrapper’ around each employee—whatever device they use and wherever they work. To do this, the information security team must be able to see what is being done, manage staff and devices throughout the organization, and protect corporate data—wherever it’s held.”

JAMES HAYES is a freelance writer based in the United Kingdom. His first feature on car hacking appeared in the January/February 2016 issue.
Have confidence in your cloud security knowledge.

Become a CCSP and lead your organization to the cloud.

Be a leader in the field.

CCSPs report that in addition to employer confidence, they have gained respect, credibility, and trust across all levels within their organization. CCSP certification on your resume will demonstrate your cloud security expertise and show employers that you can fill a void in the rapidly growing aspect of information technology that is cloud security.

CCSP tops “The Next Big Thing” list as the #1 certification survey respondents plan to earn in 2016

Download the CCSP Exam Outline
IT’S NOT JUST WHO YOU KNOW… OR MAYBE IT IS. EXPAND YOUR PROFESSIONAL POTENTIAL BY BUILDING A PERSONAL LEARNING NETWORK.

BY KERRY ANDERSON

CYBERSECURITY is a discipline that requires continuous professional development to stay ahead of the new risks in the threat landscape, as well as an expanded expertise. Many of the technologies that cybersecurity practitioners must manage securely continually evolve, much as futurists like Ray Kurzweil, who in his 2001 essay The Law of Accelerating Returns predicted when he wrote that the 21st century will experience a rate of technological change that is a thousand times greater than in the prior one.

Cybersecurity teams will need to respond to new challenges while managing existing risks, such as social engineering. It may no longer be sufficient to obtain expertise after the fact; practitioners need to be able to anticipate the security repercussions of technological and societal trends, and acquire the necessary proficiencies to manage them for their organizations. Otherwise, practitioners will find themselves
constantly attempting to control the proliferation of potential insecure technology implementations, such as cloud storage or BYOD, without appropriate controls or policies in place.

Most of us already have a means of finding expert advice, whether through publications, social media or conferences. But how many of us have actually established bona fide plans to build and nurture a professional network that incorporates the most popular ways of connecting with peers?

**WHO’S IN YOUR PERSONAL NETWORK?**

Many cybersecurity practitioners face challenges to their professional development, most commonly the cost of materials and outside training and the time away from the office or home. A Professional Learning Network (PLN), also referred to as Personal Learning Network, can provide development opportunities close to home and at minimal (if any) cost.

Practitioners design their PLN to achieve a goal: become better at what they do, or what they want to do. Social media tools, such as Facebook, Twitter and LinkedIn, let (ISC)² members connect with other professionals who share a common interest or passion in cybersecurity, and exchange ideas and possible collaborations. Additionally, we have former classmates, current and past coworkers, and members of professional organizations that we can contact on a somewhat regular basis. And that’s important—to nurture a network, you need to keep in touch, though frequency rates may vary.

This brings up an important point—and distinction for those formally creating a PLN versus just becoming “more social.” We learn from exchanging new ideas, knowledge and different attitudes that stimulate learning and professional growth. It is not a one-way relationship. An enduring PLN requires communication and assistance flow in both directions. If a practitioner fails to return support to others within their PLN, members of the PLN may become reluctant to engage in the relationship in the future.

**LOADING THE PLN**

Designing a PLN requires a customized approach. It is essential to diversify the composition of a PLN. The practitioners might seek out potential contacts across many specializations, including relationships with individuals in cybersecurity-related disciplines and other fields, such as education and human resources. Sometimes the best way to learn from others is to engage others whose industries are not in competition.

There are a variety of tactics to build a core PLN under the overarching strategy of better connecting with experts in your field. For some, this might mean expanding beyond their normal comfort zone and putting more of themselves “out there”—by commenting on blog posts or articles, and attending more networking events. It all begins with establishing your professional presence, both in the physical and virtual worlds.

** Participate in local professional organizations.** Attend local chapter meetings or events of professional associations several times annually at least. Monthly meetings are often free or low cost. Events frequently offer member discounts. Get there early to network with peers, and stay for optional post-event activities when possible.

Make it a point to carry an ample supply of business cards—one from your current employer, and one with a more personal touch that includes your personal mobile phone number and email address, as well as any relevant social media profile links. Building a PLN is a lifetime investment in your career, so consider what you want to do well beyond your current position and use the personal business cards if your employer has strict rules for email and internet use done on company time. The bonus to these inexpensive personal business cards: the contact information typically stays current even if you change jobs.

**Develop your social media profile.** First, make sure your chosen social media profile is easy to find via an internet search using just your name. Don’t skimp on the descriptions sections. Your social media profile can be the equivalent of the “elevator speech,” essentially a 30-second promotion about you. People form an instant impression based on what, and how much, information you provide. It is a good idea to invest in a professional photo and a fully developed profile by listing relevant experience, certifications, education and other accomplishments, such as publications where you’ve contributed. LinkedIn features a profile strength-rating system that can be used as a model when assessing your profiles on other social media sites.

**Blog.** If you are a proficient writer, consider creating a blog. Blog posts can be short pieces on a timely topic that interests you, and are an excellent way to both develop and display your expertise. Great blog posts can grab others’ attentions and be shared via Twitter, Facebook, LinkedIn, and other popular social network platforms.

**Contribute articles to publications.** If writing is your passion, consider submitting an article to a professional association’s magazine, newsletter or peer journal. In addition to publishing your piece, these publications also typically allow you to include your blog or personal website. Every publication has its own writer guidelines, so be sure
to review those before you submit a work.

**Speak at events.** Many cybersecurity conferences and events put out a call for papers (presentations), including those hosted by (ISC)². Again, there typically are guidelines to follow, so be sure to apply properly to speak on a topic based on that conference’s criteria for presenters. Not ready for the national stage? No problem. Many chapters of cybersecurity associations look for speakers for monthly meetings and annual events. Speaking at events gives others an opportunity to get to know you and add to your PLN. In addition to speaking, some events task speakers to write a blog on their session’s topic, and this offers an additional mechanism for building a PLN.

**Join online discussion forums.** Virtual discussion groups exist all over the internet. It’s not tough to find them, but it may take some work to find one that you want to join and to which you will contribute. Be sure to read threads to make sure there’s valid information being exchanged, and that trolling or other disparaging comments are discouraged. There are literally hundreds of these groups related to information assurance and compliance areas. Some are open forums, while others require a request for membership to join.

**BUILDING A COMMUNITY**

The creation of a PLN does not replace the traditional development options of formal classroom training or conferences, but rather offers opportunities to expand knowledge and perspectives in a one-on-one manner. It is the foundational step for initiation into “communities of practice.” A community of practice is a collection of individuals who share a specific profession or area of interest. Jean Lave, a cognitive anthropologist, and educational theorist Etienne Wenger introduced this concept in their 1991 book *Situated Learning: Legitimate Personal Participation*. Wenger expounded on the topic in his 1998 book *Communities of Practice: Learning, Meaning, and Identity*. Communities of practice are pivotal in a profession like cybersecurity, where it is impossible to develop expertise in all areas.

A cybersecurity professional who does not participate in either informal or formal communities of practice, such as local chapters of professional associations, is at a distinct disadvantage in such a broad field with many sub-specializations.

Cybersecurity professionals build their own communities of practice using many of the same tools to build a PLN—developing a strong social media presence, writing and blogging, and participating in conferences. In addition to these, there are a number of virtual discussion groups on social media sites, primarily LinkedIn. As an adjunct professor, I along with my co-instructor encourage our students to participate in communities of practice by creating a class blog.

**PUT YOURSELF OUT THERE**

A significant component of adult learning is social. We learn from our interactions with others. By designing a PLN, we can proactively engage others with knowledge we need to advance in our careers, and in our lives. In turn, we can do the same for someone else by becoming part of his or her PLN.

Sound simple? It is, at least in theory. Throughout our careers, many of us unconsciously build professional learning networks and, as a result, become a member of one or more communities of practice. With PLNs—and those dedicated to sustaining them as they evolve—so too does the cybersecurity industry through stronger professional relationships and greater information sharing. So, as you plan for 2017, consider raising your personal profile—online and in real life—to help make our cyber world a little safer.

Massachusetts-based (ISC)² member KERRY ANDERSON has earned the following education and career credentials: CISSP, ISSAP, ISSMP, CISM, CISA, CGEIT, CSSLP, CRISC, CFE, CCSK, MBA, MSIA.
Playing by the BOOK

HOW AN (ISC)² MEMBER CREATES CHILDREN’S BOOKS ALSO MEANT FOR THEIR ELDERS. BY CHRIS GRECO

CYBERSECURITY CAN SEEM relatively complex to children. I know from experience that our youngest members of society view technology from a convenience standpoint—being able to connect with others, or collect information at the touch of a button. This is a generation of texters, not talkers, who rarely use a smartphone to actually make a call. Instead, they are adept at using more modern methods to communicate using social networking tools.

But this convenience comes with risks, from privacy intrusions to identity theft, cyberbullying and even extortion. That is the reason children’s books on cybersecurity are both wanted and warranted in this age of “cyber first, consequences second.”

As an author of a series of children’s books on cybersecurity, I can attest that these publications are neither simple nor straightforward to produce, but they also are one of the
most satisfying and rewarding ventures that I have ever accomplished, besides helping my wife raise our two children, of course.

**GETTING READY TO LAUNCH**

When I first started writing and illustrating cybersecurity books for children, I wanted to ensure that the character would be someone who children would enjoy “listening to,” as well as learning from.

Granpappy Turtle fulfills both needs.

He understands how to speak to the generations that followed him, by asking good, focused questions. The character is the right blend of inquisitive and knowledgeable to work for these types of books.

While the character was important, the content was key. I wanted to present a book that parents could read to their children, or that children could (eventually) read themselves to provoke thought. As a parent, I can tell you that my children might listen to what I say, but they listen to another adult with much more attention. The same is true with Granpappy Turtle and the characters that surround him.

As for the content of the books, I am still exploring the tone and volume of the written language that grabs children’s attention. I try to share my books with friends and their children to get feedback on the content and then use that feedback to refine the message.

The books that I write are not for early elementary school age, but more for 8- to 10-year-old children. I have found that 9-year-old children thoroughly enjoy the books and do not feel challenged by the language. At a recent book festival, I had a 9-year-old pick up one of my books and read it so well that I was sure that my age range was appropriate.

In addition to the content of the book, the venue is also important. I tried narrating some of my Granpappy Turtle books on shared video websites like YouTube, but the results have been mixed. I am still experimenting with all of these aspects of children’s book writing to see which ones work and which ones don’t, but the journey is well worth the work.

The topics for the books were no easy task either. The first one, on passwords, was something that we all encounter. For most of us, it’s a simple task to generate a password, which is why there are tons of easy passwords out there to break.

I wanted to ensure I got the point across that passwords are the “keys to your padlock” of information you want to keep secret. Keep in mind, we are dealing with an age in which schoolyard friendships are frequently cemented over sharing secrets.

In some cases, I have heard of children giving away their passwords to their “best friends.” Although I can understand how you want to trust people, the “best friends” in a child’s life change, sometimes daily, and that can lead to someone who is not a friend getting the password. From there they can wreak havoc on the child’s social networking site, posting comments or pictures that seem like they are coming from the child. In today’s world, the lines between real life and online personas is blurring, so what is said online can easily spill into the real world and cause needless friction and fractures.

My book, therefore, had to address both the password structure and content in easily understood terms, and underscore why it is essential to keep passwords secret—all this with colorful pictures.

**WHY CHILDREN’S BOOKS**

Someone once asked me why I write children’s books rather than books for adults. I had to smile since I actually write children’s books for adults. I know that, as an adult, I used to read books to my children at bedtime, as well as “reviewing” them before I read them.

I often found the books were as educational for me as for them, and I hope my books may also spread education by the parents “reviewing” the book prior to reading it to their children. I also expanded my offering to e-books, which helps the parent (or any adult) download the book and then use their mobile device to share it. I feel that this is the epitome of informing people about cybersecurity: using technology to teach it!

I have learned a lot by creating Granpappy Turtle books. In exploring the subject for my first book, I learned that
Becoming an author also has led me to present cybersecurity concepts at senior centers, where elder citizens, which I have named “Silver Hats,” can also learn from Granpappy Turtle about how to not fall for online scams and fraud.

some of the password techniques I have used in the past to reduce my risk did not actually reduce my risk at all, and I am a computer security professional!

The research that I have done to make these books as factual as possible, while surrounding them with turtle characters, mixes the real and the imagined so that children can adopt the character as someone that gives them information to keep them safe.

I hope that through my make-believe characters and handy delivery formats, both reading and concepts of cybersecurity are a little more enjoyable—and prompt the actions we want children to take to become safer online.

I am continuing the storytelling with more Granpappy Turtle books including a two-part series on cybersecurity (the first part is out now and the second part is coming). Becoming an author also has led me to present cybersecurity concepts at senior centers, where elder citizens, which I have named “Silver Hats,” can also learn from Granpappy Turtle about how to not fall for online scams and fraud. This, along with the writing and illustrating of other non-cybersecurity related Granpappy Turtle books, helps me to give back to the computer security community.

CHRIS GRECO, CISSP, is a senior consultant/trainer with Greco Techknowledgee (GRETECH) (www.grectech.com).

A Marketing Tip When You’re Self-Published

WRITING AND ILLUSTRATING children’s books is hard work. Marketing finished works can be just as hard, maybe even harder. It takes time and a strategy to spread the word and gain readers, especially if you are self-published and do not have a publishing company to help with marketing.

I recently participated in the Baltimore Book Festival to sell my Granpappy Turtle children’s books and found one way to attract potential customers was to have a game or contest.

During the festival many people had games of chance (usually a “spinner”) where every spin rewarded a prize. Since my main book is on passwords, I downloaded a cell phone app that would “score” a person’s password. When someone came to my booth and showed interest, usually by smiling at my book cover, I would ask them if they felt their password was strong. Most would be pretty humble and say no, to which I would ask them to put a password (not the one that they use for any of their applications) into the password meter to check the strength.

If their password was not strong, I would then show them that adding just three characters would make the password that much stronger. Their reaction was one of surprise and delight. In one instance, a young lady put in four numbers, all the same. It was the lowest score of the day. She was shocked, saying that she thought placing four of the same number would be the hardest to guess.

With that lesson, people expressed a little more interest in the book. In a sense, they all “won the prize” that day.

—Chris Greco
Raising Awareness, Scholarships and Opportunities for Future Cybersecurity Professionals

BY PAT CRAVEN

I KNOW YOU THINK I am going to talk about Garfield this month, given our big launch at September’s Security Congress in Orlando. Yes, we’ve worked hard over the past year to make the world’s most recognizable feline our Safe and Secure Online spokescat. But that isn’t all we’ve been working hard on this year.

In addition to achieving record-shattering participation in this year’s Global Information Security Workforce Study, we have revitalized our scholarship program—also to great success.

This year, with your support, we are providing some USD$150,000 in educational scholarships to help prepare the next generation of cybersecurity professionals. Last year 66 students applied for financial aid; this year we received 511 applications for our women’s, graduate and undergraduate scholarships. Of those seeking aid, 61 percent of applicants were female and 56 percent were born outside the United States. Of the 42 scholarships award, 22 (52 percent) went to females and 20 (48 percent) to males.

Applications for next year’s women, graduate and undergraduate scholarships open in January 2017. Information on all scholarships may be found at www.isc2cares.org/scholarships.

CHAPTER CHALLENGE WINNERS
This year also saw the introduction of a new three-year partnership with Raytheon. The technology organization is now providing two USD$10,000 scholarships along with a paid summer internship for two aspiring female cybersecurity professionals. We are so excited Raytheon is providing a model program that we hope inspires other companies committed to diversity within information security.

But the achievements don’t stop there. This year we challenged three (ISC)² chapters to pilot a new effort to provide scholarships to high school students in their communities. The results are in! The following chapters met the (ISC)² Chapter Scholarship Challenge by raising at least USD$1,500 in funds and expanding opportunities for high school students in their communities. Here are their fundraising totals as of October 1:
• Austin Chapter – USD$3,409
• Tampa Bay Chapter – USD$3,000
• Richmond-Metro Chapter – USD$1,500

Congratulations to these chapters for collectively raising nearly USD$8,000 toward information security scholarships.

FUTURE CHALLENGES?
Does your U.S.-based chapter want to provide local high school students with scholarships? A new fundraising period opens on November 1 and runs until July 31, 2017. That’s nine months of fundraising, and we have all the tools you need to help. Chapters will have their own personalized donation pages, where the chapter’s scholarship can be promoted on social media sites and funds can be collected online. (ISC)² will also help you get the word out by emailing (ISC)² members in your local community. It’s easy, and a great way to help impact future cybersecurity professionals.

Join in the fun and make a difference! Email us at scholarships@isc2.org for more information on how you, your chapter, or your company can play a part in preparing the next generation of information security professionals.
When did you know you wanted a career in information security?

After I completed my bachelor studies in electronics and telecommunication engineering, I started working as a network and communication engineer. I worked on several network design and technology projects, such as implementation of routers, firewalls, intrusion detection and prevention systems, etc. At that juncture, I decided to start learning more about information technology security and eventually pursued a career in information security.

After realizing that was your chosen path, how easy or difficult was it to gain entry?

I must say, it was a little difficult. Specifically in India, I remember information security was considered a branch of IT and a potential candidate for information security was expected to be best at information technology most times. An entry-level career as an information security professional was a little difficult, as in most industries and sectors, security concepts and security implementations were considered child projects of IT implementations.

What have been your biggest hurdles in your current career?

Transitioning my career from a network and communication engineer to an information security specialist was the biggest hurdle. It was more difficult than I thought it would be. Further, elevating my career path by focusing on being a technology security professional to business security professional was another challenge.

You’re originally from India. What part of the nation are you from, and how has living in India, and still visiting, impacted your career?

I am from Mumbai (often termed the financial capital of India), which is located in western India’s state of Maharashtra. There is always huge demand for great talent across all sectors and industries in Mumbai. I started my professional career in Mumbai and later moved to the United States to pursue a formal education in the field of information security. My information security professional contributions to the financial and insurance sector in Mumbai provided the groundwork for my current work in the United States and internationally. I believe the more diverse and international your experience is, the more rewarded you are.

What are you most proud of accomplishing with the group to date?

Every achievement and contribution I make to the information security community makes me feel satisfied. That includes doing my small part to help nurture others in the information security profession. I’m proud to have earned a master’s degree in information security, continue to advance in my professional career, and volunteer as a peer reviewer for academic and professional security journals and magazines. I’ve also been an instructor for security courses, judged cybersecurity contests, and held other roles that I believe contribute to making our community and industry better.

What do you believe are some misconceptions about the cybersecurity workforce in India?

Not only India, but a majority of developing nations still consider cybersecurity as only a technology challenge. Also, another misconception is that only those with a technology background and significant amount of technical experience can advance to a career in cybersecurity. This may not be always true. While cybersecurity could still be technical at its core, in wider context it is a business challenge and overlaps with governance, risk, compliance and business in addition to technology.

An expanded version of this interview will appear in the December issue of Insights, a companion e-newsletter for the (ISC)² membership.
Why blow your budget on piecemeal, ad hoc content generation?

Use our full-service creative agency dedicated to delivering your unique message

Unleashing strong ideas and creating effective content marketing that is on brand and on time is our specialty. Twirling Tiger Media, a creative agency with its roots in journalism, is a team of expert storytellers and designers who will connect your customers’ business issues to your company’s solutions through original and honest content—the type that will attract, acquire and engage your target audience.

**Drive profitable audience action with our services, which will be on brand with your company’s marketing goals.**

- Articles
- Blogs
- Case Studies
- Content Marketing
- Custom Content
- eBooks
- Infographics
- Inspirational Quotes
- Leadership Guides
- Magazines
- Newsletters
- Press Releases
- Publications
- Social and Digital Media
- Sponsored Content
- Success Stories
- Web Content
- White Papers and more!

For how our team of experts can serve you, please contact Bob Ostrow at bostrow@twirlingtigermedia.com.

Twirling Tiger Media is certified as a women’s business enterprise by the Women’s Business Enterprise National Council (WBENC) and federally designated as a Women-Owned Small Business (WOSB).