Focus 15 will offer a program packed with valuable and timely content on the ever changing security landscape.

Christopher Young
Senior Vice President
General Manager,
Intel Security Group

Steven L. Grobman
Chief Technology Officer
Intel Fellow,
Intel Security Group

Join us for Intel Security’s 8th annual FOCUS 15 Security Conference, October 26-28 in Las Vegas!

October 26-28
The Venetian and the Palazzo Congress Center, Las Vegas

Conference Highlights

• **90+ Technical Breakout Sessions**: Learn about the latest security innovations from Intel Security.
• **Networking**: Engage with some of the best minds in the industry.
• **Keynotes**: Hear from impressive industry leaders and security expert Christopher Young & Steve Grobman.
• **Other Conference Highlights**: Benefit from Targeted Group Meetings, a partner expo and much more.

As an ISC2 member, save $100 off your registration by using promo code FOCUS215 when registering!

Visit us at [www.focus.intelsecurity.com/Focus2015/](http://www.focus.intelsecurity.com/Focus2015/) to learn more.
FEATURES

› MANAGEMENT

14 Testify
A forensics expert with a lot of courtroom experience outlines ways to gain and maintain courtroom competence and composure.
BY ANDREW NEAL

› PROFESSIONAL DEVELOPMENT

18 How to Become a Security Evangelist
Seasoned speakers share what they’ve learned from a life on the stage.
BY DEBORAH JOHNSON

› RESEARCH

24 Seeing is Believing
For all of the investments in IT security, one low-tech threat is being ignored. BY ANNE SAITA

PUBLIC SPEAKING ISN’T EASY, BUT WITH TIPS FROM SEASONED PRESENTERS, IT ISN’T HARD EITHER.
PAGE 18

Illustration (above) by ©ENRICO VARRASSO
Editor’s Note

HOW TO WORK A ROOM

I LIKE CROWDS. I like them for the energy they provide and the ability they give me to blend into the background. In crowds, I never feel obligated to carry a conversation, and there are more opportunities to join one in progress.

All of us at some point in our careers are forced into social situations, such as company mixers or conference socials. Even lulls in meetings can lead to impromptu discussions, provided people aren’t catching up on their phones.

One major opportunity to learn more about your trade and your fellow members is coming this month in the way of the 5th annual (ISC)² Security Congress (congress.isc2.org) in Anaheim. The staff works hard to embed lots of opportunities to network, whether it’s informally between sessions or at the member reception.

It’s up to you to take advantage of these openings.

It’s one thing to go up to someone you already know. The hard part, of course, is when we don’t recognize anyone, and everyone appears already engaged in conversations. Sometimes I do a little eavesdropping to see if I should join a talk. Other times, I park myself at a table or couch with a plate of hors d’oeuvres and see who sits next to me as the party grows.

A conference also provides easy conversation starters—How are you enjoying the conference so far? Best sessions? Great speakers? And, especially if it’s been an exhausting day, I will stand back, take in the place and let my brain and my voice rest a bit. I also make sure to approach the hosts when I arrive and thank them when I leave.

I hope to see many of you at Congress...between and in sessions, at lunch, at the member reception, and maybe even at a panel I’m moderating on FUD and the news media. This is also the month we set the editorial calendar, so if you need a conversation opener, feel free to let me know what topics you’d like to see in next year’s issues.

> ANNE SAITA asaita@isc2.org

ADVERTISER INDEX

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

McAfee .............................................................. 2
MIT ........................................................................ 5
(ISC)² ................................................................. 7
Symantec........................................................... 9
Sunera .................................................................. 11
Guidance Software ......................................... 13
(ISC)² ................................................................. 16
(ISC)² ................................................................. 17
Capella ............................................................. 21
(ISC)² ................................................................. 23
ISACA............................................................... 27
EWF ..................................................................... 29
Twirling Tiger Press ......................................... 31
(ISC)² ................................................................. 32

© Rob Andrew Photography
“There are two kinds of companies today. Those that have experienced a security breach and those that don’t know it yet.”

Howard Shrobe
Director, Cybersecurity, MIT CSAIL

Cybersecurity starts with you. Become part of the solution.

mitprofessionalx.mit.edu

Join the new online Cybersecurity course at MIT starting September 15 and save 10% using code ISC10.

MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) presents a six-week online course that examines Cybersecurity challenges in:

- Hardware security architecture
- Resilient Software
- Public Key Cryptography
- Cybersecurity Policy

Learn the latest developments and research to help your organizations move from ‘patch and pray’ defenses to security ‘by default.’

Cybersecurity Course Start Dates:

Register today.
MORE WAYS TO EARN PROFESSIONAL CREDITS

aining a credential from our organization is a big career milestone, but the true value of the certification comes from continuing to learn and improve your value in the workplace. And that requires already busy people to find the time to stay on top of technologies and privacy and security issues.

(ISC)² has long partnered with other organizations to provide continuing professional education credits for our credential holders. Our organization does a thorough review of materials to ensure our partners meet our rigorous guidelines for quality education and training.

Today, we are providing more educational opportunities in more formats to accommodate members’ busy schedules and needs.

I’m pleased to report that these educational opportunities are expanding with our recent announcement of a partnership with a major technology publisher. Members will have even more ways to enhance their skills and earn CPEs through white papers, research documents and myriad other products.

In another initiative, the CISSP program recently received ACE CREDIT recommendation from the American Council on Education. This means professionals and students who take an (ISC)² official five-day CISSP training course are eligible to receive three college credit hours toward their degrees. The course was reviewed and validated by industry experts and academics to ensure it meets the rigorous standards the security credential demands.

More broadly, we’re partnering with other organizations’ education catalogs to help members obtain quality instruction and meaningful CPEs in popular verticals—such as health care, forensics and finance.

Additionally, we’re expanding our education and training portfolio to provide more e-learning. All of our certifications, starting with the cloud security program, will eventually offer asynchronous training programs that combine instructor-led videos with online activities and assessments.

Finally, through another partnership with a technical organization, we plan to create custom labs to offer tactile training for the professional who wants more hands-on instruction securing networks, systems and cyber forensics. This also facilitates performance-based assessments through our education and training programs.

By providing members more ways to gain quality CPEs, we fulfill our mission to create a safer cyber world, one credit at a time.

We offer these programs to all professionals, not just those who hold our certifications. It’s one way—an important one—for us to fill the shortage of skilled labor in today’s workforce.

By providing members more ways to gain quality CPEs, we fulfill our mission to create a safer cyber world, one credit at a time.

To learn more, be sure to visit our website regularly for upcoming education and training.
(ISC)² Security Congress conferences make a global impact by securing tomorrow today at each event through the multi-track educational sessions along with prime networking and career advancement opportunities. Each Security Congress will include topics on best practices, current and emerging issues, and solutions to challenges.

(ISC)² Security Congress EMEA
Organized in partnership with MIS Training Institute

20-21 October 2015
Sofitel Munich Bayerpost
Munich, Germany
emeacongress.isc2.org

(ISC)² Security Congress Latin America

24-25 November 2015
WTC Events Center
Sao Paulo, Brazil
isc2latamcongress.com
More than 20,000 future computer science undergraduates per year at 100 United Kingdom universities (http://cphc.ac.uk/) may benefit from new higher education cybersecurity learning guidelines published by (ISC)²® and the Council of Professors and Heads of Computing.

The guidelines are designed to align better academics with industry demands and to reflect broad consultation with more than 30 universities and industry bodies and support the UK government’s National Cybersecurity Strategy (https://www.gov.uk/government/publications/cyber-security-strategy). In those schools where the guidelines are implemented, students can learn a broad spectrum of cybersecurity concepts, from threats and attacks to designing secure systems and products to governance based on up-to-date industry expertise.

“The UK has a world-class cybersecurity sector, but we can only continue in this vein if we have the highly skilled workforce we need to thrive. Initiatives such as these are excellent examples of encouraging the best young people to consider careers in cyber,” said Matthew Hancock, a Cabinet Office minister.

Adds Nick Savage, head of the School of Computing at the University of Portsmouth, “The key to the cybersecurity guidelines is that content will be integral to computing courses and not just a module added on. This should be reflected in the knowledge our graduates receive; application to operating system design will be taught securely with cybersecurity implications at the front of mind. This is an important step in the approach to cybersecurity education in the UK, and we all need to be on board.”

The new “Cybersecurity Principles and Learning Outcomes” guidelines document was developed over two years through a series of workshop consultations with leading experts.

The election process for the 2016 (ISC)² Board of Directors is already underway. Don’t forget to cast your vote during the election period: November 16 to 30, 2015. The timeline for petitions and voting is as follows:

1. Sept. 17 5 p.m. EDT
   Deadline to submit petitions for ballot
2. Nov. 9
   Announcement of instructions for electronic voting
3. Nov. 16 8 a.m. EST
   Electronic voting begins
4. Nov. 30 5 p.m. EST
   Electronic voting ends
This marks a significant shift in the teaching of security in higher education; cybersecurity is now being recognised as integral to every relevant computing discipline from computer game development to network engineering.

—CARSTEN MAPLE, professor of Cyber Systems Engineering at University of Warwick and vice chair of the UK Council of Professors and Heads of Computing, on new learning guidelines for students seeking computing degrees

CPEs

When submitting CPEs for (ISC)^2’s InfoSecurity Professional magazine, please choose the CPE Type: “(ISC)^2’s InfoSecurity Professional Magazine Quiz (Group A Only),” which will automatically assign you two Group A CPEs.


Protect data and identities wherever they reside—in the cloud, on-premise, or in transit. Visit symantec.com/information-protection

#GoProtect

Go ahead, you’ve got

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
SPOTLIGHT: (ISC)² CROATIA CHAPTER

A NEW CHAPTER IS DEVELOPING A NATIONAL AWARENESS FOR CYBER SECURITY

THE CROATIA CHAPTER of (ISC)² was formed in November 2014 with 25 members. In an email interview, Chapter President Biljana Cerin, CISSP, said they started the Chapter to keep abreast of all the government, legal and corporate changes in the information security arena.

“We decided to form an (ISC)² Chapter that would enable us to keep these activities more focused and also to consistently promote good information security practices within our organizations and the wider community,” she says. Chapter members are active in national initiatives to form a better legal framework for citizens’ data protection in government information systems. For example, Chapter members provided guidance and input to Croatia’s Ministry of Public Administration’s efforts in creating the law on the state’s information infrastructure.

Cerin is also enthusiastic about their efforts in the community, especially with regard to encouraging young people to learn about careers in information security. As schools in Croatia don’t provide the appropriate courses of study, she says the Chapter is a valuable source of information, training and mentors.

The Chapter also is engaged in attracting women professionals to security. The Chapter participated in the International Girls in ICT Day (http://www.itu.int/en/action/women/girls-ict-day/Pages/2015.aspx), which provides career and organization information to young women in the community.

“The message to them was that working in ICT doesn’t mean only being isolated and surrounded with technology, but that there is a whole array of business opportunities, roles, projects and challenges where they can show their excellence as ICT professionals,” Cerin says.

Additionally, Cerin looks forward to ensuring that the Chapter members are engaged socially and professionally through regular contact and both informal as well as formal meetings.

“Together, we can make great things. We just need to constantly keep in touch.”

—Biljana Cerin
biljana.cerin@gmail.com

CISSP® TRAINING SEMINAR RECEIVES ACE ACCREDITATION

The 2015 CISSP Training Seminar has been accepted for accreditation through the American Council on Education (ACE). The subject matter expert reviewers were highly complimentary of the course materials and course assessment. They believed the five-day course was developed with such academic rigor that students can earn three semester hours credit when taking the official (ISC)² CISSP training course.

You can learn more at http://www.acenet.edu/higher-education/topics/Pages/Credit-Evaluations.aspx.

(ISC)² EARNS LEADERSHIP AWARD

(ISC)² has been named a 2015 recipient of the Colloquium for Information Systems Security Education (CISSE) Business Leadership Award - Information Assurance Education for Exceptional Leadership.

Now in its 20th year, the CISSE supports cybersecurity educators, researchers and practitioners in their efforts to improve curricula and foster discussion of current and emerging trends.

The organization lauded (ISC)² for “being a long-time advocate for information assurance/cybersecurity education and training; and for providing robust and authenticated cyber workforce certification.”

―Deborah Johnson
GLOBAL COST OF SOCIAL PHISHING ALONE EXCEEDED U.S. $1 BILLION IN THE PAST YEAR

61.3% OF MALICIOUS LINKS TARGETING BUSINESSES ON SOCIAL MEDIA ARE PHISHING AND MALWARE

THE AVERAGE TIME TO REMEDIATE A BREACHED SOCIAL ACCOUNT IS 5.5 HOURS

Source: From the 2015 white paper “The Social Takeover” by ZeroFOX
CONGRATULATIONS TO THE 2015 (ISC)²® FOUNDATION WOMEN’S SCHOLARSHIP RECIPIENTS

To encourage more diversity in the information security workforce, the (ISC)²® Foundation each year awards competitive scholarships to women with promising cybersecurity careers. Congratulations to the following recipients, and a big thank you to our Foundation donors who helped make these financial investments in our future.

ANNA TRUSS
Turkmenistan, Excelsior College
“I am the first in my family to attend a graduate school. Getting a graduate degree has always been my dream, and receiving the (ISC)² Foundation Women’s Scholarship is a great honor for me.

“Getting a graduate degree has always been my dream, and receiving the (ISC)² Foundation Women’s Scholarship is a great honor for me.” —Anna Truss

I’ve gone through a lot of difficulties in my life, and this degree could make a huge difference for my family and offer me a chance to give back to the cybersecurity field through training and consulting services. There is a lack of female professionals in the cybersecurity field, and with my current knowledge, expertise and passion, I am confident that I can make a positive impact in this field.

One of my many goals is to receive a Master’s of Science degree in Cybersecurity. This scholarship, for me, is not the end but rather the beginning of a brighter future. I would like to thank the members and staff of (ISC)² for making these scholarships available for students like myself.”

ROSE REINLIB
United States, University of North Carolina at Charlotte
“Winning the Women’s Scholarship is a great honor and is assisting me in moving forward with another year in cybersecurity studies at UNC Charlotte. I am ramping up my work with an internship this summer and courses in the fall. My mentors at my current internship are taking notice of the scholarship, which has allowed me to begin working in the cybersecurity field. I look forward to continued challenges and rewards in the area, and the (ISC)² Women’s Scholarship will help in my future endeavors in cyber security.”

FUMI HONDA
United States, Stony Brook University
“I’m very grateful and excited to be selected as one of the (ISC)² scholarship recipients. This will allow me to focus more on learning instead of funding my own education. Whenever I think of it, I feel more motivated because there is a group of people out there who sees my potential and wants me to succeed as much as I do. I believe that helping to solve challenging problems in security will be one of the best ways for me to give back. Thank you.”

MICHELLE HARDESTY
United States, University of Cincinnati
“Receiving the Women’s Scholarship has been extremely motivational, and I am thankful for the opportunities I am now able to pursue. I will be able to stay on track with taking classes to finish my degrees, continue learning and performing through internships, and complete my research. All of this leads to supporting advancements in a field that fuels my passion to learn how things work, create new things and use that knowledge to defend.” —Michelle Hardesty

YESENIA GUADALUPE TREJO ALFARO
Mexico, Universitat Oberta de Catalunya
“The Women’s Scholarship gives me hope for a better future, because today I know that there are people like the (ISC)² Scholarship Review Committee who trust my abilities. This award will allow me to continue my studies in the Master’s program in Information Security. Thank you for allowing me to turn my passion for security into an opportunity to improve my professional and personal development.”
Hone in on the real threat

Defending your organization and its data is in your blood. Every day your team and systems prevent numerous would-be attackers from achieving their goals. EnCase® Endpoint Security evolves your defensive posture so you can proactively hunt anomalies, weed out false alerts, and automate routine work so you can annihilate the real threats.

Learn more at www.guidancesoftware.com
“DO YOU SOLEMNLY swear that the testimony you are about to give is the truth, the whole truth and nothing but the truth?”

These are not words most people in the technology industry expect to respond to on a regular basis. It’s not included in many job descriptions, but if you have responsibility for information security, incident response or digital forensics, there is a distinct possibility that you may find yourself raising your right hand and giving that oath in the course of your role.

Many technology and security professionals would rather face a DDOS attack or a malware outbreak than testify in court, but, while it can be a bit tense at times, testifying in court is a skill that you can develop and even practice.
A SPIKE IN SUMMONS

With the pervasiveness of technology in our everyday lives, it should come as no surprise that issues related to technology have found their way into criminal trials, civil litigation and other formal settings. What may be surprising is the degree to which technology professionals are finding themselves involved in court proceedings.

The most obvious situation relates to technology professionals in digital forensics or incident response, where there is a presumption that evidence may be provided or testimony given based on any specific incident. Professionals responsible for information security, systems administration, software development or IT management may also find that circumstances result in a request to testify about an event or occurrence.

This article is about court testimony; therefore, it is important that I make a few disclaimers up front.

First, I am not an attorney. My knowledge is based on my experience testifying in multiple cases and on working as part of a team that routinely gathers evidence and provides testimony.

Second, this article is not about the law; it’s about the experience and demands of being called to testify.

Finally, I would encourage anyone with a high probability of being called to testify or with an interest in the subject to do additional research. Look up evidence standards such as Frye and Daubert; read the Federal Rules of Evidence; and attend a trial or evidentiary hearing so you can see how the process works. If your organization has an in-house counsel, take him or her to lunch and ask lots of questions. You won’t need a law degree to be successful, but you should be familiar with the basic terms and process.

WHERE TO START

A powerful starting point for people who may have to give testimony—either in court, through deposition or via affidavit—is this simple advice: be professional.

The best basic advice I can offer you is to apply established policy and industry best practices consistently as your minimum standard in your daily job. Keep good notes, especially if something unusual occurs or if you are actively involved in an incident. Keep your training up to date, and operate within your professional competency. Be painfully clear and honest in your communications, and keep good records.

These actions will build a solid foundation for any testimony you may be called to give. Failure to do so may result in a very uncomfortable experience. If it comes to light during your testimony that you did not follow your organization’s standard procedures, or that your handling of potential evidence did not meet minimum standards, you could find yourself off-balance and on the defensive.

When testifying, being deposed or writing an affidavit, the number one rule is to tell the truth. Answer carefully, making sure you understand the question and can answer it clearly. If the question doesn’t make sense to you, or there is no technically correct way of answering, request that they rephrase the question.

Make sure you are providing only those facts of which you are personally aware and not delivering opinion or someone else’s work. You may be able to prove that a piece of malware entered the network from Bob’s computer, but you probably can’t swear that Bob introduced the malware intentionally.

There can be pressure from all parties involved to spin the truth or jump to conclusions, but sticking to what you know to be true is the safe and ethical path.

“Keep calm and carry on”

As a T-shirt slogan, based on a World War II expression, says, “Keep calm and carry on.” Every time you are asked a question on the stand, especially if it is by opposing counsel, take a deep breath before answering, and then speak slowly.

This does several things: 1) It gives you a few seconds to think about the question and how to phrase your answer; 2) It makes you appear smarter and more deliberate in your responses; 3) Controlling the pace of the questioning will also lower the stress you may feel and help you think more clearly; and 4) It gives your legal team a chance to object to the question before you start talking.

Remember that you are not alone in your journey to court. You will be working with one or more attorneys as
the case develops and progresses. The more involved you are with them, the more smoothly your testimony will go.

Ask these attorneys questions, including what questions they will be asking you. Get them to practice with you, if they don’t ask you to do so first. It is in their best interest for you to be as prepared as possible. You can also prepare by participating in mock trial scenarios, sometimes done in classes and seminars.

A DIFFERENT PLAYING FIELD

As a technology professional, the legal environment may seem very different and can feel a bit illogical at times. As with our fields, there are terms and concepts that make no sense to the uninitiated.

The careful investigation and analysis of server logs that you think clearly identifies exactly what happened may never make it to trial. No matter how smart or how right you are, the judge makes the final decision about what evidence the court will use. It can take a very long time to resolve what seems like a simple issue. By the time a given incident has made its way through the preliminaries of the legal process and it is time to testify, several years may have passed, and the systems or personnel involved have changed.

There is a mystique, and often a little fear, around the idea of testifying in court. If you find yourself on the stand, just rely on your professionalism, keep calm and tell the truth. Yes, this advice is simplistic, but you’d be surprised how many times people ignore it and how beneficial it can be to you.

You may even find the experience to be interesting and rewarding.

ANDREW NEAL helps lead a global forensics and technology consulting team. He can be reached at aneal@transperfect.com or @theforensicals.
As a CISSP®, you meet all CCSPSM experience requirements and are immediately eligible to take the CCSP exam. Pass the CCSP exam by December 31, 2015 and the first year of your CCSP AMFs is free.

Did you know....
your CPEs for CISSP also count toward CCSP?
security conferences or listen to enough webinars, and eventually you might think to yourself, “I can do this.”

But often the thought stops there because of a fear of public speaking or a lack of time or connections to those within speaking circuits.

With approximately 350 security conferences, meetings and seminars scheduled around the world annually, surely there’s a place for you to not only help enhance cybersecurity but also your career.
CARVING OUT YOUR NICHE

It’s not enough to say, “Security awareness is important,” according to veteran security advisor Ira Winkler, CISSP, president of Baltimore, USA-based Secure Mentem and president of the Information Systems Security Association (ISSA). It’s crucial, he says, to carve out your own security career by establishing a niche, developing your reputation in a specialty aspect of security and getting people thinking.

Jennifer Minella agrees. “You have to be an expert in something.”

Minella is the VP of engineering and consulting CISO with Carolina Advanced Digital, Inc. in Cary, N.C., USA and an (ISC)² board member. “When you talk about security, it’s as broad as talking about technology.”

She advises people to develop “a competency in an area and have a little bit of depth. The more depth you have in any specific area, the more you're going to come to people's minds.”

John Papa, senior associate at Booz Allen Hamilton, provides coaching and training to speakers and presenters. He encourages his presenters to use “firsthand experience and an interesting perspective or angle that's going to be different than what's out there, rather than talking about general cybersecurity awareness.”

How to find that niche? If you have “a topic you are passionate about, information you want to share…that's the starting point,” counsels Minella. “Look at blog content, news media, hashtag topics. Get a feel for what are those [hot] topics.”

GETTING NOTICED

You've got a message, something you're passionate about, something you want to share. You've done well presenting your ideas in your work group. Now, you want to get onto that larger stage.

“Getting published, writing articles is an important step,” Papa says. “You have to write and pitch interesting abstracts … and start small.”

Winkler advocates both persistence and patience. “You have to be willing to write and write a lot and expect nobody will read it. You have to expect that maybe one out of a hundred articles might actually be notable to the general public.”

Tim Garon, media manager for (ISC)² (and publisher of InfoSecurity Professional), books speakers for webinars, panels and conferences and likes to start new speakers out at a roundtable webcast or in a live panel discussion.

“This puts them at ease because there are other people to play off of, other speakers carrying the ball.”

Minella also suggests participating in social media.

“If you're out mingling in the social community, you have the opportunity to start establishing yourself as a go-to person for that thing you are passionate about.”

Winkler, however, offers a warning about social media: “Just because you tweet a thousand times a day and people interact with you, it doesn't make you a thought leader.”

Don't, he says, “confuse quantity with quality.”

GETTING HEARD...AND LISTENED TO

Now, you have figured out what you want to say. But how you say it is just as crucial.

“The ability for somebody to be an evangelist is part expertise but much more the art of communication,” Winkler, who has been a public speaker at global conferences for decades, says.

And, he cautions, not everyone will have that talent. “They need to see if they have a good communication style. Do they relate to people? Do people want to listen to them?”

That ability to communicate also requires you to have a sense of the people you’ll be addressing.

“Understand your audience ... relate to the interests and concerns of the audience you are speaking to.”

—JOHN PAPA, senior associate, Booz Allen Hamilton

Papa says that’s key to a successful presentation. “Understand your audience … relate to the interests and concerns of the audience you are speaking to.”

Minella agrees and spends extra effort learning about an audience as part of her preparation. She describes, “I spend a lot of time talking to the organizers to understand what their goals are. ‘What are you guys trying to do? What value do you want me to bring to your audience?’”

Presentation style plays a big part in success, too. BAH’s Papa looks at how speakers perform. He asks, “Do they make eye contact [with the audience]? Are they animated? Using inflection? Telling interesting stories so their audience wants to listen to them, and not just because they have to?”

(ISC)²’s Garon looks for presenters who are comfortable in front of an audience: “I can understand a little bit of nervousness. … Can they speak extemporaneously, not just read off slides? Are they engaging with the audience?”

Minella adds that humor can help you connect with
Mistake #1: APOLOGIZING UP FRONT
Whether you arrived late, left the laptop with your presentation on it in the cab or simply forgot all those handouts you so painstakingly put together in the hotel room, never start your presentation by apologizing. It sets a negative tone for the entire meeting, and it also makes you look like you’re shirking your responsibilities.

Mistake #2: RUNNING THE GUILT TRIP
“I have 15 minutes left, and I’m only through 20 of my 58 PowerPoint slides, so I’m going to be going through this last bit a little fast.” Sound familiar? Guilt ing your audience into paying attention not only doesn’t work, it’s insulting. Don’t try to force your audience through your agenda. Your presentation needs to focus on their needs—period. If that need is wrapped up in the first slide and you only discuss this one point for an hour, then you’ve done your job.

Mistake #3: EXCUSES, EXCUSES
“I’m so tired.”
“I got in late last night.”
“I’m feeling a little under the weather.”
Who cares where you were last night, how long your flight was or how late you were up? Get over yourself, quit whining and start focusing on your audience. And no matter how tired, sick or frazzled you’re feeling—at least act like you’re excited to be there.

Mistake #4: READING BETWEEN THE SLIDES
Don’t ever let your audience see you reading from your slides! Your slides should contain key points, not elaborate prose, and they shouldn’t mimic exactly what you’re saying.

Mistake #5: FORGETTING TO SMILE
You want the audience to leave the room feeling better than they did before they interacted with you. How likely is it that they’ll be feeling happy if you’ve spent the last hour staring at them with a stern or frozen demeanor? Smile! Show the passion you feel.

Mistake #6: TURNING YOUR BACK ON YOUR AUDIENCE
Talking with your back to people—often seen hand-in-hand with looking back to read directly from your PowerPoint slides—is unprofessional at best, and outright rude at worst. Don’t do it. Ever.

Mistake #7: FAST TALKERS
Since most of us speed up even more when we’re nervous or anxious, reduce your nervousness—and your speed—by practicing your presentation in advance.

Varying the pace of your voice will also help keep the audience listening and engaged. For best results, practice your presentation into a tape recorder, then play it back to listen to yourself.

Mistake #8: GET OVER YOURSELF!
Don’t be afraid to open yourself up to your audience. Remember, they want you to have the answer to their problems. So move toward them, gesture and smile. Look at each audience member: don’t just glance distractedly around the table or into the conference room.

the audience. She comments, “Humor is huge. If you can’t educate them, entertain them, and this will keep you from taking yourself too seriously.” Just make sure your humor is well-placed and directed at yourself, she warns.

A NOTE ABOUT TECH-SPEAK (A/K/A JARGON)
“You don’t have to be the smartest person in the room,” both Minella and Garon say.

Minella adds, “Be considerate of the audience’s varied expertise. You should be able to communicate your thoughts without losing your audience in jargon.”

In other words, “Don’t use 50-cent words where nickel words will do,” advises Secure Mentem’s Winkler (liberally paraphrasing Mark Twain).

Adds Papa, “Presenters, particularly in the IT space, are used to their own language rather than the language of...

CONTINUED ON PAGE 22
THERE’S NO SHORTAGE OF CYBER SECURITY THREATS

BUT THERE IS A SHORTAGE OF IT SECURITY PROFESSIONALS

DO YOU HAVE WHAT IT TAKES TO BE PART OF THE SOLUTION?

Get up-to-date security skills with Capella University’s Master’s in Information Assurance and Security (MS-IAS), aligned to the latest NSA focus areas.

Earn up to three NSA Focus Area Certificates showcasing your mastery of skills in specific cybersecurity areas along the way to your MS-IAS.

Plus, the knowledge you gained for your CISSP®, CEH®, or CNDA® certifications can help you earn credit toward your MS-IAS, saving you time and money.

ANSWER THE CALL. START TODAY. CAPELLA.EDU/ISC2 OR 1.866.933.5836
the audience. They miss the boat [because] they don’t use the terminology, language and perspective of the audience.”

Minella sums it up with this advice, “Demonstrate your mastery of the subject through an ability to describe it succinctly.”

WHEN THE GOING GETS TOUGH

Your success as a presenter (and your ascension to the A-list, if that’s a goal) is also judged on how you handle the unexpected.

Your PowerPoint fails. You spent hours getting the deck just right, and at the last moment, something goes wrong, and the PowerPoint isn’t there. Now you’re on your own.

“Don’t stop,” says Minella. “I’ve done presentations when my slide deck was lost, the audio wasn’t right, the electricity went out. Just work through it.”

Papa agrees, saying that you should be so well prepared that “you should be able to give [your presentation] on a street corner regardless of any A/V needs.”

“I’ve done presentations when my slide deck was lost, the audio wasn’t right, the electricity went out. Just work through it.”

—JENNIFER MINELLA, VP of engineering and consulting CISO, Carolina Advanced Digital

(An aside about the PowerPoint: Professionals agree that your slides should support your presentation. It is not the presentation; therefore, don’t laden slides with overly dense content. “People’s attention spans are short,” Papa says. “They’re distracted by their mobile devices. You’ve got to be really focused on your prioritized messages.”)

Negative comments or criticism from the audience. “Ignore the trolls,” declares Winkler. “Just let the troll be the troll. Good, consistent, hard work will always beat a troll.”

Papa suggests patience in confrontations. He counsels, “Agree to disagree, offer to take it offline, give them your business card, defuse the situation. As the presenter, you should be commanding that room.”

And if you’ve made an error and someone points out you are wrong? “If you’re wrong, you’re wrong,” says Minella, and Winkler agrees. He advises, “If you’re wrong, say you’re wrong.”

Overconfidence. Yes, that can trip up even the most seasoned presenter, says Garon. “They are doing their presentation, they know it inside and out, and they’re almost bored by the topic because they’ve delivered it so many times and they are so close to the subject matter.” It can become obvious to the audience.

Minella recalls a conference where she delivered two presentations: one brand new; the other one that she had given many times before.

“I spent so much time cramming for the first talk, I got overconfident and didn’t put the same effort in my second talk. The result was that I came across as extremely comfortable in the first and not so much with the second, of which I was considered a ‘master.’” And how did she know? “It wasn’t smooth. People actually told me.”

TAKING IT ON

Becoming a security evangelist takes dedication, patience, interest and the ability to communicate. Having a passion, wanting to share your thoughts with an audience, spending the time needed to find your niche and develop your skills can pay off.

As veteran presenter Winkler will say, “You have to grab them by their heart before you grab them by their head.”

DEBORAH JOHNSON is a managing editor for InfoSecurity Professional magazine. She can be reached at djohnson@twirlingtigerpress.com.
VULNERABILITY Central

Start tracking the vulnerabilities keeping you up at night.

Get Started

This exclusive, members-only resource aggregates, categorizes, and prioritizes vulnerabilities affecting tens of thousands of products.

Create a customized feed filtered by the vendors, technologies and keywords that are relevant to your interests.

vulnerability.isc2.org

No new account is required to use Vulnerability Central and it's free to members, just login with your (ISC)² member account.
OPEN WORKSPACES ARE GREAT FOR PRODUCTIVITY,
A ‘NIGHTMARE’ FOR SECURITY  BY ANNE SAITA

Photograph by iStock

HE TEMP WORKER was on the job only 15 minutes before he found
privileged documents in plain view. Next, he found a stack of papers
clearly labeled “confidential”
and stuffed them into a briefcase. Before leaving, he pulled
out his phone and started
taking pictures of even more
data he lifted from copy
machines and computer
screens while employees
worked around him.

In a recent Visual Hacking
Experiment, this happened
more than 40 times, and in
nine out of 10 instances, the
thief got away with it.

“There are organizations at risk because employees are not being mind-
ful of the information accessible in different forms and different locations,”
says Larry Ponemon, Ph.D., CIPP, chairman and founder of the Ponemon
Institute, which conducted the 3M-sponsored Visual Hacking Experiment
on behalf of the non-profit Visual Hacking Advisory Council.
The “temp worker” was really one of several specially trained actors who spied with a business’s permission. Someone in management knew what was happening, but none of the other employees did.

“This study is unique,” Ponemon says. “It was very hard to organize and implement, but it was definitely worth doing. Our fundamental hypothesis is that organizations are sloppy with data, whether it’s electronic as we know it or paper copies. A lot of people aren’t paying attention to the security aspects of what they’re doing.

“And it’s normally not an evil person doing evil things, but it’s more about good people who do stupid things. There are just a lot of mistakes made in the typical office environment.”

According to the study’s findings, released back in February:

• Eighty-eight percent of 43 visual hacking attempts were successful. The five that weren’t took place among R&D centers, defense contractors and other business lines that are generally more security-minded.

• Twenty percent of the data hacked was considered a very valuable information asset.

• Documents on vacant desks and data visible on computer screens are most likely to be hacked.

• In 70 percent of the hacking attempts, employees didn’t confront or report the visual hacker, even after witnessing unusual or suspicious behavior.

Ponemon says companies’ typical cubicle farms that promote open work spaces may be great for camaraderie, creative synergy and productivity, but they are a nightmare for security.

Still, the seasoned privacy professional was startled by the dramatic nature of the results.

“We all do it, Ponemon adds. “We find ourselves in different places—a Starbucks or at an airport, and we’re accessing our information and trying to get work done, and we don’t think about someone behind us taking pictures of what we’re doing.

“It seems like all the innovation has been on how to create more security around data, files and networks, rather than data that might be accessible in paper form or on screens.”

More than 100 U.S. companies were invited to participate in the experiment, and eight in different industries

“A lot of people aren’t paying attention to the security aspects of what they’re doing.”

—LARRY PONEMON, chairman and founder, Ponemon Institute
agreed to allow actors posing as “temp workers” or “consultants” to come into their organization a total of 43 times during a two-month period in the summer of 2014. They were surreptitiously issued badges that allowed them to work casually around the office and observe.

First, they needed to identify sensitive data, which usually took about 15 minutes into the operation and was based on the following criteria:

- Personally identifiable information
- Information about customers or consumers
- Information about employees
- General business correspondence
- Access and login information/credentials
- Confidential or classified documents
- Attorney-client privileged documents
- Financial, accounting and budgeting information
- Design documents, presentations and architectural renderings
- Photos and videos containing business information

Then, researchers decided to make things a little more obvious by leaving a stack of papers clearly labeled “Confidential” or with a similar classification on a vacant table or desk in a public place. The actors placed the bogus documents in their knapsack or briefcase to see if anyone stopped them.

Finally, in the most blatant situation of all, the actors would stand in front of other people and take photographs of screens—in front of other people.

“What we found is that most people didn’t even ask the question, ‘Who are you?’ They just looked the other way and didn’t pay attention to it. They were too busy to say, ‘Gee, this is unusual behavior. Maybe I should talk to someone about it.’”

In only one instance did an employee go to a supervisor and security to complain about the unusual behavior.

After the operations, Ponemon researchers met with company officials to reveal what they found so the company could then incorporate findings into new employee training.

That, by the way, was the big takeaway: Do not forget obvious actions in employee security training.

“Visual privacy is a security issue that is often invisible to senior management, which is why it often goes unaddressed,” attorney Mari Frank, a member of the Visual Privacy Advisory Council, said in a news release upon the study’s release.

“This study helps to emphasize the importance of implementing a visual privacy policy, educating employees and contractors about how to be responsible with sensitive data they are handling, as well as equipping high-risk employees with the proper tools, such as privacy filters, to protect information as it is displayed.”

ANNE SAITA is editor-in-chief of InfoSecurity Professional magazine.
CREATE VALUE FOR YOURSELF AND YOUR ENTERPRISE—START BY REGISTERING FOR AN ISACA CERTIFICATION EXAM TODAY!

“EMPLOYERS SEE MY ISACA CERTIFICATIONS. THEY KNOW I WILL BE A VALUABLE RESOURCE.”

— MARCUS CHAMBERS, CISM, CGEIT
CONSULTANT
LONDON, UNITED KINGDOM
ISACA MEMBER SINCE 2012

Becoming ISACA-certified showcases your knowledge and expertise. Give yourself an edge and gain the recognition you deserve with ISACA certifications—register for an upcoming exam today!

Register at www.isaca.org/2015exams-ISC2

UPCOMING CERTIFICATION EXAM
12 December 2015
Final Registration Deadline: 23 October 2015

Take the first step towards gaining the recognition you deserve—register for a December exam today!

Register online to automatically save US $75! www.isaca.org/2015exams-ISC2
Fostering Goodwill, Education, and Research Initiatives

CORNER

WHY WE NEED MORE WOMEN IN OUR INDUSTRY  BY JULIE FRANZ

Women globally control some U.S. $20 trillion in annual consumer spending. Business experts predict that market will reach US $28 trillion within the next five years.

So you’d think when companies produce computer-related goods, from hardware to apps, that they would always consider women buyers during development. But publications like Harvard Business Review indicate that isn’t the case. Despite their consumer clout, companies continue to underestimate women as they bring products to market that either ignore their needs or segregate their use (think Dell’s ill-fated pink laptop and women-only website).

This, unfortunately, also holds true in information security, where women are grossly underrepresented in the workforce.

According to the 2015 Global Information Security Workforce Study (https://www.isc-2cares.org/IndustryResearch/GISWS/), women comprise a small fraction (about 11 percent) of IT security staffs worldwide.

We explore what can be done to bring more gender parity in a new (ISC)²® Foundation white paper being released this month. We’ll also dive deeper into the subject with a four-session track at (ISC)² Security Congress, which launches Sept. 28 in Anaheim, California.

Why the continued focus on women in the workforce? Because we need to develop consumer goods and services that women will use—systems, applications and tech processes that take into consideration their needs (like easy-to-use mobile apps that can be readily accessed with one hand while the other holds onto a squirming child in the checkout line).

Differing perspectives on an issue provide a more robust solution. And the issues around security only continue to grow as use of technology to run our everyday lives grows.

We need all hands working on these issues.

The information security industry is growing much larger and now requires practitioners to be proficient in more than raw technical skills. Women, in general, have those other skills needed to succeed in the newly defined information security space. They are known for their strong communications and team-building skills and cross-functional management. This makes them ideal for communicating security issues to non-security decision-makers.

These women complement, rather than compete, with their male peers and are positioned to thrive. We just need more of them to choose information security as a career.

It’s not a diversity issue but an economic issue. If we double the number of women working in security, we wipe out the gap in the workforce while building products and services that benefit all of us. The security workers of the future isn’t living under a rock. They are our sisters, daughters, nieces and grandchildren living among us.

Julie Franz  is the (ISC)² Foundation Director. She can be reached at jfranz@isc2.org.

WOMEN IN SECURITY SESSIONS AT (ISC)² SECURITY CONGRESS

Career Advice from Two Old Dinosaur-Ettes (Patricia Myers and Sandra Lambert)
1:45 to 3:30 p.m. • Tuesday, September 29

4:30 to 5:30 p.m. • Tuesday, September 29

Women in Security: Studies on Women in the Security Workforce
11:00 a.m. to 12:00 p.m. • Wednesday, September 30

Women in Security: CSOs/CISOs—How to Work Successfully With These Industry Leaders
3:30 p.m. to 4:30 p.m. • Wednesday, September 30
October 20-22, 2015
Hyatt Regency at Gainey Ranch | Scottsdale, AZ

Big Data, Big Risk, Big Opportunities

From the Keyboard to the Boardroom—A World of Opportunity at your Finger Tips
Suzanne Vautrinot - Major General & Commander, US Air Force (retired) and Board of Director Member, Symantec, Wells Fargo and Ecolab

Denial of Reputation: Sensible Security PR
Opportunities and Innovation in Healthcare Big Data
Data Sovereignty, Global Cybersecurity Policy & Government Control
Voice Privacy Conundrum
Day in the Life of your Customer’s Data
The Data You Want—An Inside Look at Monitoring and Alerting

Women of Influence Awards
Nominate your peers, clients and customers for the Women of Influence Awards. Co-presented by CSO Magazine and Alta Associates, the awards honor four women for their accomplishments and leadership roles in the fields of security, risk management and privacy.

FOR NOMINATION FORM
GO TO: www.ewf-usa.com
Nominations must be submitted by August 15, 2015

For more information on the EWF or to register, please visit: www.ewf-usa.com
EUGENE TAWIAH

Eugene Tawiah, CISSP, is a New York City native who turned an “unhealthy obsession” with 2600 into a successful career in information security and compliance. He’s been a member of (ISC)² since November 2013.

EDITED BY ANNE SAITA

What made you decide to start a security company? And when did you make that decision?

I've been interested in information security since 1992, when a network administrator introduced me to 2600 meetings in the Citicorp building in Manhattan and a book titled TCP/IP. I met the administrator when I volunteered at a local ISP (Dorsai Embassy) and was provided dial-up access to a Solaris shell account. It was the unknown and the desire to know that fueled my drive.

It wasn't until that network administrator disconnected my connection at home over an IRC disagreement that I saw the power of a network administrator. I wasn't given root access, but I made it my mission to figure out how to gain it. 2600 was the door. I was great at my hobby and at one point had developed an unhealthy obsession, but unexpectedly, it turned into a career.

How did you get your first “big break” in information security?

I owe my “break” credit to the media. I co-hosted an online cybersecurity-focused gray hat “radio” show called Parse in 1996 at Pseudo Networks in lower Manhattan. A New York Times reporter named Anthony Lappe said Howard Stern caught the show, and he wanted to see what we were all about. I broke my No. 1 rule at the time, “Don’t talk to the media.” I spoke to the media. A front-page Tech piece led to many more media pieces. The sudden attention from my 15 minutes of fame gave rise to my consulting life and my company, Complex Technologies 1.0.

A lot of members dream of starting a company and are entrepreneurial in spirit. Any tips on what it takes to actually succeed in this business?

I come across a lot of members who perform services on the side but don't feel it's enough to take the plunge. Having been there myself ... I offer a few (non-comprehensive) bits of advice.

First, have at least six months’ to a years’ worth of expenses saved, so you won't be stressed during the early days of no income.

Also, take time to learn the other hats you will be wearing, including:

- How to sell yourself and your services
- How to manage a sales team
- How to manage accounts payable/receivable
- Hire a virtual assistant, so you can manage your time wisely

Consult a corporate tax preparer and attorney and have them review your planned corporate structure and any contracts you intend to have your clients sign.

It wasn't until I started full time that the opportunities and deals started to increase. There's a certain ceiling that you hit when you attempt to run a business on the side while holding another job full time.

How did you become involved in (ISC)²?

I've always known about (ISC)²; however, it wasn't until after I obtained my CISSP that I truly became involved. I now attend local Chapter events and participate in free online events such as the security briefings and various seminars.

How important is your CISSP to your career?

My CISSP is very important to my career, as it is the icing on the cake. I have the experience; however, this well-respected certification adds a layer of validation and credibility that opens doors and starts conversations.

Where do you see yourself in 10 years?

I see myself in a CISO role in a large, well-known enterprise or in a fast-growing startup.

EUGENE TAWIAH reveals more in our upcoming October 2015 e-newsletter, INSIGHTS.
"...70% of people would rather learn about a company via an article than an ad."

—HARVARD BUSINESS REVIEW

You understand the power of content to tell your value story. And at Twirling Tiger Press, so do we.

We are your one-source publishing solution for great writing and design—keeping your audience engaged through original publications, white papers, blog posts and more.

Let us put our editorial, design and marketing expertise to work for you by creating fresh, contemporary content that expresses your thought leadership.

Contact us today at info@twirlingtigerpress.com.
CONGRATULATIONS to the
2015 AMERICAS ISLA FINALISTS

Senior Information Security Professional Category

Jason Pfeiffer
Cyber Fusion Center (CFC)

Lyndon Dubeau
Security Program- Cancer Care Ontario

Bob Cheong
Cybersecurity Program at LAWA

Eric Fromm
Cyber-Ark Privileged Identity Management Suite

Information Security Practitioner Category

Renan Melo Santos
Privileged Account Management Solution at Atacado

Nicholas Sullivan
CloudFare Heartbleed Challenge

Up-and-Coming Information Security Professional Category

Noah Jaehnert
Security Architecture Program

Kenneth Butler
Red Team Testing

Community Awareness Category

Anderson Ramos
Roadsec

James McQuiggan
Program Management & Coordination- NERC CIP Standards

September 30
Anaheim, CA • City National Grove