To Learn More About
Endpoint Threat Detection, Response and Prevention
Visit: www.bit9.com/etdrp To Download a Free eBook Today
FEATURES

PROFESSIONAL DEVELOPMENT
16 How to Manage Your Online Reputation
Before you tweet, “like” a friend’s vacation pics, or send a LinkedIn request to a speaker you met at a conference—stop! Then ask yourself how it may reflect on you and even your employer. BY COLLEEN FRYE

MANAGEMENT
21 Preventing the Employee Vacuum
Of more than 7,500 IT workers surveyed, 35 percent said they were planning to look for another job in 2014 and 35 percent said they weren’t sure. Are you prepared if an employee moves on? BY DEBORAH JOHNSON

WEB SECURITY
24 Tightening the Web
New domain holders, especially those acting as registries, have an opportunity to demand stronger security controls. BY DAVID DANN

Contents VOLUME 7 • ISSUE 3

DEPARTMENTS
5 EDITOR’S NOTE
Social Acceptance
BY ANNE SAITA

7 EXECUTIVE LETTER
Get Into the GAP
BY JO PORTILLO

9 FIELD NOTES
Spotlight on (ISC)² Eastern Mass. Chapter; CCFP expansions; meet member James McQuiggan

14 MODERATOR’S CORNER
The New Security Professional
BY BRANDON DUNLAP

27 GIVING CORNER
Meet the Scholars
BY JULIE PEELER

29 2020 VISION
What will the future CISSP look like?

5 AD INDEX

InfoSecurity Professional is published by Twirling Tiger Press Incorporated, 7 Jeffrey Road, Franklin, MA 02038. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)² on the issues discussed as of the date of publication. No part of this document—print or digital—may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of (ISC)². (ISC)², the (ISC)² digital logo and all other product, service or certification names are registered marks or trademarks of the International Information Systems Security Certification Consortium, Incorporated, in the United States and/or other countries. The names of actual products and companies mentioned herein may be the trademarks of their respective owners. For subscription information, please visit www.isc2.org. To request advertising information, please email tgaron@isc2.org. ©2014 (ISC)² Incorporated. All rights reserved.
Empower business through security.

Employees busy working. One of them has accidentally opened up an email and downloaded a virus. The whole business could be compromised — and you know it’s your job to get everything back on track, fast.

Kaspersky Security for Business brings together powerful anti-malware and control tools, encryption, mobile and systems management into a single integrated platform.

Empower your colleagues to work the way they want to, without the security risks.

usa.kaspersky.com/business
SOCIAL ACCEPTANCE

I’M BETTING AT some point in your life you’ve wished you could remove some indexed item on the Web. Maybe it’s an inaccurate or incendiary guest post you can’t take down; maybe it’s some inflammatory comments you wrote using an alias (later exposed). More likely, it’s an unflattering photo or critical post on Facebook, Twitter or Instagram put up by a “friend.”

Conversely, it may be you’ve been so quiet or cautious that now there’s little, if any, online evidence of a solid track record or thought leadership for a prospective employer to help determine if you’re the best candidate for a job.

It’s increasingly difficult for most of us to best manage the realm between our public and private selves and the relationships we acquire in the process. Like it or not, you’re now your own best publicist and must decide what image to project in various online forums and offline settings.

In this issue, Colleen Frye talks to several experts in social media to help you, as a security professional, decide what to post online. There's also advice on reputation management in case something negative pops up during a Bing, Yahoo or Google search.

Whether you manage staff or aspire to do so one day, you’ll want to read Deborah Johnson’s piece on hiring and firing, especially as it relates to succession planning for information security professionals.

And, for something different, (ISC)² member David Dann offers a perspective on the potential of ICANN’s new[ish] top-level domain naming system to improve Web security.

We welcome members to contribute to the magazine and its e-newsletter companion, Insights. If you have a great story to tell or an interesting, instructive take on a timely or time-honored security issue, I’d love to hear about it. In addition to being published, you can earn up to five CPEs if your piece makes it into print. Email me your article ideas.

› ANNE SAITA asaita@isc2.org

©Rob Andrew Photography

Editor’s Note

ADVERTISER INDEX

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

<table>
<thead>
<tr>
<th>Bit9</th>
<th>Kaspersky</th>
<th>(ISC)²</th>
<th>Intel Security (McAfee)</th>
<th>(ISC)²</th>
<th>Gartner</th>
<th>(ISC)²</th>
<th>(ISC)²</th>
<th>Black Hat</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>13</td>
<td>15</td>
<td>20</td>
<td>28</td>
<td>30</td>
</tr>
</tbody>
</table>
CSSLP® is the only certification that validates your knowledge and experience in secure software development practices.

Enabling the next generation to

BUILD HACKER RESILIENT SOFTWARE

Get the credential that recognizes your application security expertise. Sign up for our FREE webcast series and find out what you need to know.

education.isc2.org/csslp-webcast
COMING TO A COLLEGE NEAR YOU
GAP bridges the workforce conundrum with more educational opportunities

COLLEGES AND UNIVERSITIES prepare people for the greater professional world by stretching minds through intellectual exercises. (ISC)² is also about educating professionals, in our case to specifically strengthen those aspiring to or already working in the IT security workforce.

So it’s not a stretch for our organization to team up with academic institutions to help fill the current gap in cybersecurity jobs and eligible applicants. That’s why we’ve developed the Global Academic Program, better known as GAP.

This industry-academic cooperation also can bridge the workforce gap between the large demand for qualified cybersecurity professionals and the number of skilled professionals who are prepared for the market.

GAP has three primary focus areas: education, research, and outreach.

Through various academic collaborations, (ISC)² works with a college’s undergraduate and post-graduate academic programs to ensure students learn the skills required for an ever-changing workforce. One way we do this is through classroom materials, from domain-specific modules and practice assessments to faculty handbooks and student textbooks, drawn from our certification CBKs.

GAP also allows (ISC)² to share its thought leadership with new audiences and connect with younger professionals at a critical juncture in their careers. (ISC)² members served as mentors through chapter programs.

One of the first to join (ISC)² GAP was University of Phoenix, which awards full scholarships to select individuals interested in entering or furthering their information security careers. The scholarship also includes an (ISC)² voucher to take the SSCP® or CISSP® within a year of graduation.

“University of Phoenix is committed to providing degree programs and curricula that reflect real industry needs and was one of the first universities to join the (ISC)² Global Academic Program,” said Dr. Tim Welsh, senior vice president for industry strategy at Apollo Education Group, the parent company of University of Phoenix. “There is a clear demand for information security professionals and the University is pleased to collaborate by aligning our education programs with industry talent development priorities.”

Other early adopters include the University of South Florida (U.S.A.). As part of USF’s Cybersecurity Initiative to strengthen information security professionals’ knowledge, the University’s Continuing Education is collaborating with (ISC)² to offer the CISSP and other cybersecurity certification study courses at its Tampa campus.

Additionally, we’ve recently formed partnerships with the University of Alabama at Birmingham and Excelsior College, a private, nonprofit distance-learning institution, home to the National Cybersecurity Institute.

GAP members are accredited academic institutions only to help ensure they meet academic standards. Working together, program participants help instill in students the importance of continuing professional education and industry involvement when they start their academic careers. And, we hope, turn them into lifelong learners. ●
The future of technology is more secure than ever.

We believe that as technology becomes more deeply integrated into life, security must be more deeply integrated into technology. Intel Security combines the expertise of McAfee with the performance and trust of Intel to deliver secure computing to consumers and businesses worldwide. Because when everyone has the confidence to use technology to its full potential they can achieve their full potential. Visit intelsecurity.com. McAfee is now part of Intel Security.
SPOTLIGHT ON (ISC)² EASTERN MASSACHUSETTS CHAPTER

USING TODAY’S HEADLINES TO EDUCATE TOMORROW’S WORKERS

WITH THE INCREASED interest in national and corporate security and consumer privacy following a long list of headlines in the past year, the Eastern Massachusetts (ISC)² Chapter decided to use the public’s interest to launch a series focused on ways to prevent data leaks, breaches and becoming the next big headline.

“Last year’s event involving data leaks exposed a few areas where information security deficiencies contributed to the leak, so we are organizing events to focus on certain parts of that leak,” explains Paul Kozlov, the chapter’s education liaison director.

It’s just one of the ways the Boston-based chapter, formed in 2012 and with 75 current members, is fulfilling its goal to share knowledge among information security professionals and educate the general public on IT security-related issues.

To date there have been two events in the series: one on DLP in October 2013 and another two months later on privileged access. Both drew at least 50 participants who came to hear panels of local and national experts discuss best practices and information security fundamentals—not to discuss newsmakers’ actions or the subsequent fallout.

Education is a major component of chapter activities; so is networking. The chapter leadership last year teamed with a staffing firm, Cyber 360 Solutions, which hosts some of the chapter’s meetings and shares employment opportunities so members know what’s available and what skills are needed in the region’s competitive job market.

Most recently, the placement agency is helping the chapter promote the (ISC)² Foundation’s Safe and Secure Online to area schools. The global program teaches online safety to students and their parents. To date he has taught more than 2,500 students in the greater Orlando region about cyber safety, cybercrime, and more.

James McQuiggan is the Siemens Energy program manager of the NERC (North American Electric Reliability Corporation) Compliance, where he has worked for the past 13 years. He is also the program manager of the Information Security Advisor (ISA) Program, which supports employees throughout the various Energy divisions of the North America region. The ISA program is comprised of 100 members and allows for communication between the business and the North American Energy Corporate Security Office in the area of Information Security.

Within the ISA program, James developed a new workstation audit application and organized the annual ISA Event for the past two years, created yearly training and conducts bi-monthly update awareness sessions for the ISA members. Additionally, he’s done mobile security support and various other information security training.

James, an (ISC)² member since 2008, is also a lead Safe and Secure Online Program volunteer for the (ISC)² Foundation, the lead volunteer for the Southeast U.S. region. To date he has taught more than 2,500 students in the greater Orlando region about cyber safety, cybercrime, and more.
schoolchildren, with presentations tailored to different age groups.

“Promoting Safe and Secure Online is essentially sales work. They are a sales organization and know how to sell stuff; we’re information security and not ‘salesy.’ So they contact local schools and once they make the connection, we take over and arrange for the presentation,” Kozlov said.

In a prepared statement, Cyber 360 Solutions President Mark Aiello said, “We are pleased to formalize this relationship, as it will provide critical cybersecurity education and awareness to children in our local community.”

Kozlov said members are earnest in their interest in improving security and privacy practices throughout the general public but especially schoolchildren. That’s why they are excited by the initial success of Cyber 360’s outreach and each month assign chapter members to speak at schools throughout the northeastern United States.

Chapter members also are working with another foundation to create a SSCP prep course at vocational and technical high schools. At the end of the four-year program, students can take the exam to earn a SSCP credential. The program is currently in its second year.

Additionally, members are working with the (ISC)² Foundation staff to develop a version of Safe and Secure Online for senior citizens.

The challenge is that there’s a difference between the two groups. Kids are very comfortable with technology so you need to be careful that you don’t come through as condescending if they already know a lot,” Kozlov said. “With seniors, it’s different because a lot of them are not as comfortable with technology.”

> **CHAPTER CONTACT:** Christina Mazzone, Membership Director

**Email:** c.m.mazzone@gmail.com  **Website:** www.isc2easternma.org

---

**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 2 Group A CPEs.


---

> **“We are pleased to formalize this relationship, as it will provide critical cybersecurity education and awareness to children in our local community.”**

—MARK AIELLO, President, Cyber 360 Solutions
EXPERT-LEVEL (ISC)² CCFP℠ CERTIFICATION AVAILABLE IN EUROPE

REGISTRATION IS NOW open for (ISC)²’s Certified Cyber Forensics Professional – European Union (CCFP℠-EU) certification. Originally only available for the U.S. and South Korea, the credential has been developed for the European legal environment following a series of exam workshops conducted by a panel of experts from public and private sector organizations in the U.K. and Europe.

“The crime scene is broad and so to be effective, there is a need for collaboration across the cybercrime landscape in a way that bridges all aspects of security…,” explains Lorenz Kuhlee, CCFP-EU, (ISC)² volunteer and lead investigator for the RISK Team at Verizon. “The CCFP credential supports the unique requirements of individual countries, but equips professionals with a best practice-led, uniform and thorough approach to dealing with overall challenges.”

●

(ISC)² LAUNCHES CCFP℠ FOR INDIA

(ISC)² HAS PARTNERED with Data Security Council of India (DSCI) to launch the localized (ISC)² Certified Cyber Forensics Professional (CCFP) for India—CCFP-IN.

Through the agreement signed between (ISC)² and DSCI, DSCI has provided the subject matter experts to localize the existing (ISC)² CCFP content that meets the specific requirements for cyber forensics in India.

“It is critical in India that we have an objective measure of excellence valued by courts and employers alike for indicating the ability to apply forensics to information security discipline,” said Dr. Kamlesh Bajaj, CEO, DSCI. “(ISC)² CCFP is a good fit for this need.”

W. Hord Tipton, CISSP, executive director, (ISC)², concurs: “This is another big leap forward for better serving the information security community in India.”

●

A MEMBER’S TAKE ON THE NOT-TOO-DISTANT FUTURE

“In 2020, clouds will be services like telephony, or the Web. We connect and we go with billing following at the end of the month.

Privacy will not be an issue, given data and software will be secured by strong ciphering with ‘strong’ meaning with no backdoor or expecting a national agency to have a free lunch.

However new issues will show up. If your provider goes bankrupt and all hardware disappears with your data, how will you prevent that? How will you manage those ciphering keys and certificates in order to make sure things are always under control?”

—Pierre Beaulieu, CISSP, Montréal, Canada

●

CCFP℠ CBK GUIDEBOOK NOW ON iTUNES

The Official (ISC)² Guide to the CCFP CBK is now available on iTunes. The textbook has been compiled by leading digital forensics experts throughout the world and brings together a global, thorough perspective of the cyber forensics field.

You can learn more about the book’s release at www.isc2.org.●
DAN WADDELL NAMED NEW (ISC)² DIRECTOR OF U.S. GOVERNMENT AFFAIRS

A FORMER CYBERSECURITY solution lead for Grant Thornton’s Global Public Sector Practice, Dan Waddell has more than 20 years of experience in information technology, information assurance, and cybersecurity and has overseen multi-million-dollar contracts for cabinet-level departments including Defense, State, Commerce, Transportation, Treasury, Health and Human Services, and Homeland Security.

As director of U.S. Government Affairs, Waddell is responsible for advancing the professionalization principles of (ISC)² and increasing the organization’s impact, overall reputation, and prestige throughout the U.S., state, and local government markets. Among the specific duties required are to advocate new programs and initiatives of particular interest to government; promote (ISC)² certification and education programs to government information assurance specialists; serve as a liaison to federal agencies, corporations, Congressional Committee staff members, and other professionalization organizations; and co-chair the (ISC)² U.S. Government Advisory Board.

Waddell looks forward to enhancing (ISC)²’s external partnerships: “In its 25th year of serving the U.S. government information security community, this is an exciting time to be part of the (ISC)² organization that is doing outstanding work in partnership with government, academia, and industry to solve the complex issues facing the government workforce.”

A TASTE OF CONGRESS

(ISC)² Security Congress 2014 promises to offer something for everyone, from general practitioners to those working in healthcare, forensics, and other specialties. Here’s a sampling of some presentation titles:

• “Securing Big Data: Lock It Up or Liberate It?”
• “Malware Analysis 101: N00b to Ninja in 60 Minutes”
• “How to Hack a Bank”
• “Incidents are Against Our Policy: Conflicts Between Good InfoSec and The Forensics/e-Discovery Process”
• “How to Make a Security Awareness Program Fail”
• “Holistic Vendor Risk Assurance: A View from the Trenches”
• “Advanced Red Teaming: Ghosts in Your Building”

For a full list of presentations go to https://congress.isc2.org/.

“The hands-on technical Systems Security Certified Practitioner (SSCP) is open to candidates with only one year of work experience. SSCP professionals can play important roles in an organization: In the world of continuous monitoring, for example, one needs four to five SSCPs for every CISSP.

Yet we still see organizations hiring CISSPs more for the reputation of the credential than the actual skill fit. We estimate about 70% of the security personnel searches we see ask for a CISSP. I know of none requiring the SSCP. But what organizations are really looking for is a practitioner—who has the added benefit of not commanding the same high salary as a CISSP.”

—W. HORD TIPTON, (ISC)² Executive Director, “Luring the Elusive Cyber Security Pro” in the April 14, 2014 issue of Information Week.
Strengthening Cybersecurity Defenders

(ISC)² Security Congress 2014 offers attendees over 80 education sessions, designed to transcend all industry sectors, focus on current and emerging issues, best practices, and challenges facing cybersecurity leaders. As cyber threats and attacks continue to rise, the goal of (ISC)² Security Congress is to strengthen cybersecurity defenders by arming them with the knowledge, tools, and expertise to protect their organizations. Colocated with the ASIS 2014 60th Annual Seminar and Exhibits, (ISC)² and ASIS International have teamed up to bring you the largest security conference in the world.

(ISC)² Member Benefits:

- Earn up to 63 CPEs
- Full Conference Pass Discounts
- (ISC)² Town Hall Meeting
- 25th Anniversary (ISC)² Member Reception
- (ISC)² Safe and Secure Online Program
- Volunteer Orientation

congress.isc2.org
THE NEW SECURITY PROFESSIONAL

In the course of my travels, meeting members of the IT security community from all types of organizations and industries, I can’t help but notice how each of us has incredibly diverse experience and skills that we bring to bear in our daily work. This is especially true as I read through the submissions for the 2014 (ISC)² Security Congress in Atlanta, Ga., U.S.A. Many of us have risen to the challenge of our profession from within the traditional IT silos, often from a networking background. In this issue of InfoSecurity Professional, however, we touch on another kind of networking: the networking of individuals across organizational and geographical boundaries.

The famed science fiction author Robert A. Heinlein (1907-1988), once said, “A human being should be able to change a diaper, plan an invasion, butcher a hog, conn a ship, design a building, write a sonnet, balance accounts, build a wall, set a bone, comfort the dying, take orders, give orders, cooperate, act alone, solve equations, analyze a new problem, pitch manure, program a computer, cook a tasty meal, fight efficiently, die gallantly. Specialization is for insects.”

Unfortunately, for today’s information security professional, specialization has become a necessity. Our field is too broad for a single individual to master all the requisite domains. Instead, we depend on our peers and colleagues to fill gaps in our own knowledge and expertise. We have entered an era of “forced” specialization.

This presents a fantastic opportunity for us to add value to one another, and grow not only the practice of security, but also our own careers. By connecting with one another, strengthening the bonds in our professional networks, and building lasting bridges between one another, we create a network of phenomenal capability. Modern technology makes this even easier, as we drop our fears of social networks and instead leverage them to showcase our individual talents, identify new career paths and cultivate a network of specialists that we can tap into for insights and support.

“Our field is too broad for a single individual to master all the requisite domains.”

By choosing to specialize, becoming experts in the areas that interest us the most, our passion begins to shine through. We become known for what we know and hiring managers, peers, and recruiters start to seek us out for our unique blends of skills and experience.

I hope you take time to think about what keeps you in the profession and what drives you to excel within it. I hope that you learn to develop and extend your personal brand, connecting with others of both similar and divergent interests, and that you begin to stand up for what you believe in.

So seek out your passion and hone your specialized expertise. The value you create in doing so is a currency we can all trade in.

As always, I look forward to continuing the conversation.

Brandon Dunlap is Managing Director of Research for Seattle-based Brightfly. He can be reached at bsdunlap@brightfly.com.
Discover Gartner events dedicated to security & risk management and technical professionals

Security & Risk Management

Today’s IT organizations must weave IT security and risk management into the executive levels of business planning. Gartner security and risk management events offer methods, models and best practices to help create security and risk management programs that are proactive, transparent, risk-based and process-oriented.

**NORTH AMERICA**

Security & Risk Management Summit
National Harbor, MD | June 23 – 26

Identity & Access Management Summit
Las Vegas, NV | December 2 – 4

Save $300 with code GARTISC

**EMEA**

Security & Risk Management Summit
London, U.K. | September 8 – 9

Save €300 with code GARTISC

**AUSTRALIA/NEW ZEALAND**

Security & Risk Management Summit
Sydney, Australia | August 25 – 26

Save $400 with code MPSECE2

Technical Professionals

The premier event for frontline technical professionals and architects tasked with developing and executing IT initiatives, Gartner Catalyst Conference serves multiple roles across the enterprise and aligns to Gartner for Technical Professionals research. Mobility, big data, cloud computing and social collaboration are foundational technologies that are reshaping IT and creating new business models.

**NORTH AMERICA**

Catalyst Conference
San Diego, CA | August 11 – 14

Save $300 with code GARTISC

**EMEA**

Catalyst Conference
London, U.K. | June 17 – 18

Save €300 with code GARTISC

For more information, visit gartner.com/events

© 2014 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. For more information, email info@gartner.com or visit gartner.com.

**EARN CPE CREDITS**

Earn credits toward (ISC)², ISACA and DRII certification programs.
YOU, The Brand

HOW TO MANAGE YOUR ONLINE REPUTATION

BY COLLEEN FRYE

PUT DOWN THAT SMARTPHONE. Before you tweet, “like” a friend’s vacation pics, or send a LinkedIn request to a speaker you met at a conference, stop! Have you considered how those messages might reflect on your online reputation—or that of your employer’s? Today’s professionals are using social media to build their personal brands, but there are pitfalls. Corporate policies are evolving and the lines have blurred between “personal” and “professional.” Yet experts say there are some social media do’s and don’ts that will enable you to make thoughtful contributions to your field, advance your career, and enhance your company’s (and your own) reputation.
Pause Before You Post

First and foremost, “people have to quit thinking of social media as a private room,” says Chris Syme, principal of CKSyme Media Group in Bozeman, Mont., U.S.A., which specializes in helping college athletes and coaches build personal brands on social media. Define your persona and beware of a split personality: “There’s no such thing as an offline reputation that doesn’t jive with an online reputation.”

K.C. Yerrid, a security consultant in the Seattle area, sums it up this way: “Don’t post anything on social media you wouldn’t want your mother reading”—or your boss.

Mel Carson, founder of Delightful Communications, a social media and personal branding consultancy in Seattle, and former digital marketing evangelist at Microsoft Advertising, advises being strict about what you share online. He follows a 60/40 rule: “Sixty percent of what I talk about on social networks is professional, 40 is kind of personal. I think people want to get to know you as a person, not just what you do 9 to 5. It adds some color to your brand.” However, he adds, “Everything you do reflects on your company, even after lights out.”

Yerrid cautions that “opinions can be very dangerous if not handled or shared appropriately. Some security folks have a lot of pent-up frustration, so you need to be careful not to cross the line or bash a company or another professional.”

Also beware of humor, says Mike Lockhart, information security officer at Lancope, Inc., a provider of network visibility and security intelligence in Alpharetta, Ga., U.S.A. “People have a tendency to put a joke out there without realizing it may offend a number of people. This is the digital equivalent of saying a joke loudly in a room full of people they don’t know.”

Always use professional etiquette and common sense, is what it boils down to, says Yerrid. “I don’t say anything that might be hurtful or harmful.”

And, with today’s global workforce, Carson emphasizes the need to be mindful of cultural differences. “I think you should behave as you would if walking the streets of New York, London, Delhi, Dubai, or Sydney.”

Above all, Yerrid says, keep the company’s inner workings out of the banter: “For the most part, everyone I associate with will not disclose company secrets or the organizations they’re representing. They may put [a security] scenario out there but try to generalize enough so they won’t expose a weakness or risk in a security program.”

Know Your Network

Syme draws clear distinctions and strengths among the three social media networks most people use:

- LinkedIn is where you build your resume and promote professional achievements.
- Twitter is like a real-time cocktail party where you can establish a reputation as an expert.
- Facebook “is like your living room.”

From a career perspective, Carson and others put LinkedIn on top. LinkedIn is “your personal branding statement,” says Carson. “It should be written in first person and reflect who you are, your experiences and passions, and where you hope to grow your career.”

It’s often the first thing a recruiter will check, he says, so fill out every field. Talk about your role and successes at each job, he advises.

Syme adds: Get a professional picture, make sure your bio is current, and be succinct. If necessary, she says, hire a copy editor who specializes in resumes.

LinkedIn has its own SEO, she says, so “make sure you ID what sector you work in, and ID a set of keywords that describe your skill areas.” And take advantage of functions that allow you to showcase work projects and post updates for the internal newsfeed.

Carson says that while you can reach out to anyone, “make sure outreach is targeted, personalized, and polite, and don’t take offense if people don’t get back to you.”
Yerrid adds his own rule: no more than 499 connections at any time. “With LinkedIn, at 500 you become a lion. I don’t want to be known as someone who hoards connections with loose relationships.” Carson cautions the same with Twitter: “One faux pas is looking too desperate to have as many fans/followers as you can.”

And as far as Facebook goes, both Carson and Syme advise locking it down. “I would consider having some posts go public so when people do find you through search results, there’s at least something for someone who’s not a friend. You can do that strategically,” Carson says.

Lancope’s Lockhart says 90 percent of his tweets are focused on infosec. “Facebook is a combination of personal and professional; Twitter and LinkedIn are my professional front.” Yerrid does not keep separate personal and professional profiles. “I just choose to be who I am, and treat each social network as a tool to do what it’s designed to do.” To connect with infosec peers on a more specialized path, Yerrid uses IRC (Internet Relay Chat). “The conversations on IRC and Facebook are more natural; Twitter and LinkedIn are for professional use.” He adds, “In other [security] forums, there’s a healthy amount of ribbing. It’s more natural, and you can protect the communication flow and control what it would mean to them in the long term.”

Lockhart says private forums and IRC are “where we get into nitty-gritty tech discussions, and specific problems we’re dealing with. There’s a certain anonymity and freedom you won’t get in other forums.”

Worried about some spring break indiscretion during your college years? Andy Beal, author of Repped: 30 Days to a Better Online Reputation, says you can improve your online reputation by being proactive.

1. **Google yourself.** “It’s by far the most common thing anyone else will do,” Beal says. If you find something you wouldn’t want an employer to see, you need to make some changes.

2. **If you don’t have a LinkedIn profile, create one.** “Highlight your achievements and what you have accomplished.”

3. **Create more positive content.** “Negative things from the past don’t go away but they can be suppressed. Google is agnostic; usually something negative shows up if there’s not enough positive content.” He suggests starting a blog and writing about your industry. Or set up a Flickr profile and post your best photos and vacation snapshots that will push out something negative. “The goal is to build out content that shows up in a search engine. Generally, people only look at the first 10 results; if they don’t see anything that worries them, they won’t go further.”

   —Colleen Frye
Evolving Social Media Policies

Company policies regarding social media are often distinct to each enterprise. In many cases, employees are left on their own or are subject to loose corporate guidelines. When Carson was at Microsoft, the company was in the very early stages of formulating policy. “Microsoft’s response to blogging was simply ‘be smart.’ Since then, there is quite a comprehensive policy in place, quite rightly. I do think it’s important for smaller businesses to think about how they want to be reflected online and how they want employees to reflect.”

Andy Beal, an online reputation management consultant in Raleigh, N.C., U.S.A., cautions businesses against creating a social media rule book that employees will be so afraid of violating that they don’t help build the business’s online reputation. “Explain your goals to employees, explain how they’re a major part of your brand and how their actions represent you, explain what your reputation goal is, and how you want to be portrayed.”

Make no mistake, your online reputation matters. “Companies certainly do use social media to find thought leaders/influencers, and there are tools out there to measure how effective people are,” says Carson. While your influence score or number of followers may not be the most accurate measurement of your online reputation, it is part of the overall picture, Carson says, as is the lack of an online presence.

At Lancope, Lockhart says there are semi-formalized policies for public-facing media. The company does collect Twitter IDs on a voluntary basis, and HR conducts informal social media reviews, but it’s not a requirement for pre-hiring and the company doesn’t ask for passwords. “The big question is, how much say does a company have over your own profile?”

In fact, according the National Conference of State Legislatures, 10 states have enacted legislation prohibiting employers and potential employers from requiring access to personal accounts and 28 additional states have similar legislation pending in 2014.

“We don’t have any federal guidelines yet for how much overstepping employers can do with employees,” Syme says. “The whole idea of using social media on behalf of a brand is all in flux, and will be in a gray area for a long time.”

Security recruiter Wils Bell, based in Oviedo, Fla., U.S.A., says more employers are adding social media to background checks. “Companies are looking for racist/sexual comments, inappropriate pictures. Some also ask for a Klout score.” (Klout is a social media analytics tool for measuring influence.)

Says Yerrid, “A lot of the infosec folks I know have mastered the art of reputation management, at least from a job-seeking perspective. The market will decide the value [of that] for the long term.”

COLLEEN FRYE is a Massachusetts-based freelance writer and regular contributor to InfoSecurity Professional.

“MAKE SURE YOU’RE building your portfolio around your talents and strengths, communicating with the right people, building lasting relationships with people who can both help and teach you (as well as benefit from your help and teaching), and make sure you’re promoting your best talents—the ones you want the world to see. Not everyone will succeed, but you’ll stand a better chance if you’re ready to buckle down, hustle, and do the hard work required to make your ideas come to life. You’ll be more motivated to do those things if you’re working on things you’re passionate about and have a talent for, and you’ll be more sensitive to making the best possible impression without being disingenuous in the process.”

—Lifehacker: “How to Promote Yourself Without Being Sleazy”
Live OnLine Training
Wherever you happen to be...

Life is busy. That’s why we’ve made it easier than ever for you to get certified when you take an official (ISC)²® Live Online Training Seminar – at your convenience wherever you happen to be!

Live OnLine Training includes:
- Training materials that are continually updated
- Official courseware developed by (ISC)²
- Sessions taught by (ISC)²-authorized instructors
- Flexibility to attend at a time and place that is convenient for you
- Access to archived modules for playback anytime, anywhere
- Savings on costly travel expenses

Join today!
education.isc2.org/2014_liveonline
Preventing the Employee Vacuum

Effective succession planning can keep IT security on track

BY DEBORAH JOHNSON

The news that a key IT professional is leaving the company can evoke any number of responses:

“OMG! No one knows what he knows. How will we replace him?”

“Quick, change all the passwords!”

“Know anybody who can do the job right now?”

Sound familiar? Given a recent study by Robert Half Technology, many IT workers may be on the move this year; of more than 7,500 respondents to a telephone survey, 35 percent said they were planning to look for another job in 2014 and 35 percent said they weren’t sure. Only 30 percent said no, they wouldn’t be looking for a new job.

Source: Keeping Their Best on Board. Robert Half Technology. October 17, 2013
If you have a plan and people in place, that moment of panic can pass quickly as you keep the company’s business on track and secure. But technology departments, even companies, can be lulled into a false sense of security, warns Andy Ellis, Chief Security Officer at Akamai, a cloud services provider based in Cambridge, Mass., USA. “The single biggest mistake is thinking that someone is irreplaceable…and so you don’t start planning.”

Replacing the ‘Irreplaceable’
Developing a succession plan takes time and commitment. It’s talent management and it’s serious business, according to Ellis. “This is something you should be doing all the time.”

Ron Sanders, Vice President for Human Capital Learning and Communication at consulting firm Booz Allen Hamilton, based in McLean, Va., U.S.A., concurs. “Organizations typically don’t spend enough time worrying about mission-critical positions. No matter how big an IT staff may be, there are a handful of positions that are critical to its success and the organization may not know which ones they are.”

The process starts with making sure that the skills, projects and activities of the key members of the IT and security teams are chronicled. “Inevitably, people will leave,” observes Jon Oltsik, Senior Principal Analyst at ESG, a global advisory firm specializing in IT, located in Milford, Mass., USA. “The key is to know exactly what role each individual has. Document what they’ve done, how they do the jobs, and how they’ve been reviewed.”

Documentation can be a team project, suggests Ellis. “But if the company is in the position where a single person’s departure is devastating, then there aren’t the resources to document everything.”

Develop Your Bench
In order to assure seamless IT and security management and direction, potential and possible successors must be singled out and prepared.

Oltsik foresees an acute shortage in security staff, especially in the areas of cloud and server security, and mobile device and network security. “Find out what motivates your IT specialists,” he advises, “because they are very hard to replace.”

Perhaps the best place to search for a pool of succession candidates is in-house. Start by reviewing your lower-level staff for growth potential. At Akamai, Ellis says the management goes deep into the junior staff ranks. “Work two levels down. Take people who are not next-generation leaders, but the next level and make sure they get that exposure early and [that] it’s a high-stakes exposure.”

Booz Allen Hamilton’s Sanders advises examining a current staffer’s abilities and qualities: “Does this person have the kind of attributes, technology and otherwise, that should be groomed and polished? Does this person have the potential to move two or three levels up?”

And, he adds, don’t overlook the social network in a company. “If you ask the people in an organization, ‘Who has the technical expertise or influence,’ most of the time there’s no relationship to the company’s organization chart.” There might be a potential rising star you could be missing. And look ahead, Sanders urges—not at next year, but further on. He paraphrases hockey superstar Wayne Gretzky: “You don’t skate where the puck is. You skate where the puck is going to be.’ It’s the same in succession planning. Look five, ten years down the road. And start building a pipeline to fill those jobs.”

More Than Technical Skills
As technology has taken hold in 21st-century business, its practitioners need more than just their technical expertise. The 2013 (ISC)²® Global Information Security Workforce Study prepared by Frost & Sullivan reveals not only an under-staffing in information security workers, but also a need for a high level of manage-
ment skills: “Communication skills, policy formulation and application leadership, business management and project management skills, and legal knowledge are paramount for a successful career in information security.”

Notes Sanders: “[CIO’s must have] the ability to connect the dots. For example, risk. Risk involves physical, personnel and data security, so you need a CIO that has a broad business perspective and understands how data, network and communications come together to support the business.”

Akamai’s Ellis agrees: “Look for people who are conversant with both technology and business. They must be able to articulate the security program to management.”

**Getting and Keeping the Good People**

The competition for quality information security professionals is not in doubt and retaining the best is a constant challenge. An October 2013 Robert Half Technology Survey reported that of the tech workers who said they were planning to look for a new position, 48 percent cited needing a new challenge as the reason, and 47 percent said lack of advancement.

To hire the best and keep them, ESG’s Oltsik recommends finding out what motivates them. “Present a very attractive job opportunity. Allow that person to become a leader in the security field.”

Booz Allen Hamilton’s Sanders advocates investing in those individuals in whom you see a future: “Tell them they’re on the fast track. People appreciate knowing where they stand. Send them to school; put them in charge of juicy projects. … Put your money where your mouth is.”

Not every valued employee is right for advancement, but may still offer a value to the company. Protecting the health of the business may mean some internal movement to maximize talent. Ellis says that you want to keep those people: “The key thing is to encourage people to have other options within the company.”

---

**When Things Go South**

When you’re surprised by a sudden departure, or you have to initiate that departure, the potential for problems is compounded: fear of security breaches and compromised data are part of a worst-case scenario. But the most dangerous reaction, according to Sanders is panic: “Panic and lowering your security standards. Take a deep breath and do the due diligence.” Otherwise, he adds, the rash hiring of an inferior replacement could leave you in a far worse position.

Ellis advises even-handed treatment of the departing individual: “Treat the person with respect. If you’re worried that they were going to do something bad, and they’ve told you they’re leaving, don’t you think they’ve already done something bad?”

What makes IT professionals so challenging, especially those in security, is their unique abilities to solve problems. “Security people are cowboys,” declares Oltsik. They often take shortcuts and don’t always document their actions, which can leave other team members in the lurch, not knowing how a problem was solved. Even more troubling, Oltsik warns, is the potential for manipulating budgets or action items. “Everyone has skeletons, [like] moving funding around to accommodate projects.” He warns managers to make sure you discover all you can before the inevitable departure.

But good succession planning may provide a small crystal ball. Sanders encourages what he calls “attrition assessments” be made of all IT team members. “Are they looking? Are they unhappy? If it’s high risk in key areas, are you ready?”

Akamai’s Ellis sums it up: “Succession should always be on someone’s radar. If you’re not spending that kind of time, you’re likely to be caught flatfooted at some point.”

---

DEBORAH JOHNSON is a managing editor of InfoSecurity Professional magazine.
ICANN announced in June of 2011 that it would open up the Internet domain name space for expansion beyond the existing 22 generic top-level domains (gTLDs). To date, there are more than 3,000 registered gTLDs, according to Kevin Murphy, a journalist who covers the domain name industry for the news blog Domain Incite.

ICANN has listed a number of benefits for this decision, including:

- Internationalizing the domain space by opening it up for non-Latin characters.
- Providing these gTLDs to commercial enterprises for new marketing and branding opportunities.
- Allowing regional, community-based, and cultural affinity groups to publicize and promote their ideas and activities.
For those of us worried about Web security, another potential benefit may be raising the data protection bar for companies and individuals doing business over the Internet.

**KEEPING DATA SAFE**

ICANN believes that some of the new gTLDs could be used to enhance data security. “If your customers want tighter security, make your TLD a high-security zone.” One measure that ICANN is taking to improve security on the Internet is the requirement that all of the new gTLDs must support DNSSEC, the technology that thwarts attackers from hijacking the DNS lookup process and redirecting users to malicious websites.

“*If your customers want tighter security, make your TLD a high-security zone.*”

In response to governments and financial institutions seeking to “identify security, stability, and resiliency requirements for TLDs whose primary purpose is to offer services where users have an expectation of higher security,” formed a high-security zone advisory group (HSTLD) in 2009 to explore the high-security zone possibility. While that group could not reach a consensus on what security controls should be required in a formal HSTLD program, that doesn’t mean that high-security zones can’t be done—nor shouldn’t be done.

These high-security zones could result in more secure websites that further protect sensitive customer data and help reduce phishing attacks. The security benefits of the high-security zone fall into two categories: transparency of ownership and stronger data protection.

1. **Transparency of ownership**
   
   At present, registrars of second-level domains (those domain names immediately to the left of the dot and domain suffix) in the existing gTLD space, such as the ubiquitous .com, only need to know if their customers’ domain names are unique. Domain registrars in the .com space don’t investigate their clients; they also exercise judgment as to whether or not they should accept any given domain name application because that would be in conflict with the free and open nature of that domain. Domains that are discovered to be used by phishers and for bots can be taken down by law enforcement, but this happens only after they have been discovered.

   Under the new gTLD system, entities whose applications are approved by ICANN will have the option of reserving the domain for their exclusive use or to become, in effect, a registrar and allow others to register their second-level domains in it. This is one reason giants like Google and Yahoo were quick to apply for hundreds of domains as soon as the application process opened; there’s a big business—and revenue generation—potential.

   The new gTLD owners will have the prerogative, if they wish, to set criteria as to the second-level domains they will allow.

   For instance, what if a trade group or industry association secures the rights to a new gTLD with the name .securebank or .secureshop and wants to allow only the second-level domains of bona fide banks or retail firms? In this case, those banks and merchants wishing to register their e-business portals in such a domain could be expected to show some proof that they are a legitimate lender or business.

   Their customers, in turn, would have more assurance that they are doing business with legitimate firms and not phishers. We know that criminals frequently register second-level domains that are just slight misspellings of famous legitimate ones in the hopes of snaring users onto malicious websites after they’ve “fat fingered” their keyboards. The control that the new gTLD owner has over what sites can be in the new domain reduces the likelihood of that threat.

2. **Strong data protection**

   This gets to the heart of the high-security zone concept. The new gTLD could also set strict security control standards for the second-level domains to abide by. Those standards might include rigorous system settings and activities, such as secure coding, pen testing, vulnerability scanning, and the requirement
that users authenticate to the site using multi-factor technologies such as secure tokens. The latter is not required under existing frameworks and regulations, such as PCI-DSS and Sarbanes-Oxley.

Membership in these high-security zones would be voluntary; those who firmly believe that their security controls are sufficient can continue to register their domains in the existing .com space. But recent data breaches at big name retail firms Target and Neiman Marcus have alarmed many consumers who have doubts that, at present, their personal data is being adequately safeguarded. Evidence of that concern can be seen in a recent New York Times report of an Associated Press poll conducted in February of 2014, which found that “37 percent of Americans had made an effort to use cash instead of credit or debit cards for purchases as a result of the recent data thefts.”

The high-security zones would function, in effect, as bastion enclaves for e-commerce sites that recognize the public relations and advertising value in assuaging those customer concerns. Having a site in one of these enclaves would bestow on it a better data security seal of approval—a marketing and branding opportunity that the owner could take to the bank.

At its outset, the Web was not envisioned as becoming the critical piece of infrastructure for global commerce that it is now. Communication security that would safeguard sensitive customer data was not baked in during its original design but was added later, such as with the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols that encrypt Web sessions. And these protocols’ use of certificates to digitally sign the public keys also provides some degree of assurance about the identity of a Web host to its client.

The secure enclave could become yet another in a line of such upgrades that will make for more secure websites that can also be better trusted by their users.

DAVID L. DANN, CISSP, CISA, works on information security and audit readiness projects for private and public sector clients in Northern Virginia.
PAYING IT FORWARD  

BY JULIE PEELER

Whether just starting a career or closing in on retirement, we all know people who have shaped us as professionals through their advice, examples, and, maybe, financial contributions. What prompted them to make that investment may vary wildly, but they nonetheless helped us make something of ourselves.

Our members, through the work of the (ISC)² Foundation, are dedicated to assisting qualified individuals with promising futures in the information security profession. This is particularly important as our industry grapples with a widening gap between the number of information security jobs and people qualified to fill them.

Providing scholarships is one way to help fill that skills gap and place more qualified applicants in the pipeline. Here is a list of awards we give throughout the year:

- Women’s Scholarship
- Undergraduate Scholarship
- Graduate Scholarship
- Harold F. Tipton Memorial Scholarship
- U.S.A. Cyber Warrior Scholarship
- University of Phoenix (ISC)² Scholarship
- Faculty Exam Vouchers

And here are updates on some past recipients whose college prospects were enhanced through an (ISC)² Foundation scholarship.

**Victoria Kisekka, Ph.D. candidate**

State University of New York at Buffalo (U.S.A.)

*(ISC)² Foundation Information Security Women’s Scholarship*

“The (ISC)² scholarship allowed me to focus on my research rather than worry about the financial burdens of college. Having this highly prestigious scholarship on my resume has also opened up doors for other opportunities. I have gained confidence in my research work since receipt of the award and I’m now closer to my goal of graduating with my Ph.D.”

**Micah Lippold**

American Military University (U.S.A.)

*(ISC)² Foundation Undergraduate Scholarship*

Because of his 2013 Undergraduate Scholarship award, Micah was able to earn his B.S. in information systems security earlier than expected by using the extra funding to attend classes year round. He now works in the Computer Crimes Division for NASA. Upon receiving the award, he wrote: “I am extremely grateful of receiving the scholarship and thank everybody involved in the process from donations to the selection process. I am extremely excited to get into the workplace and help in defending the nation’s information systems.”

**Sim Li Chien, 3rd Year Student**

Singapore Management University (Singapore)

*(ISC)² Foundation Undergraduate Scholarship*

Li Chien is scheduled this year to receive a Bachelor of Science degree in information management systems. Upon receiving the scholarship, he wrote: “While it not only serves as an affirmation of my relevance in this field, it is primarily a means to alleviate the financial burden on my family—the
cost of education is not low, more so in the case of Singapore. Despite subsidies and assistance from the government, market forces still are at work and we still face rising education costs.”

William Choi, Senior
Bellevue University (U.S.A.)
(ISC)² Foundation Undergraduate Scholarship

William is scheduled to earn a B.S. in both cybersecurity and advanced computer security this spring. He intends to pursue work in the IT security field as a sales engineer or in a security-related field, as well as become a CISSP.

Veronica Valeros
Fasta University (Argentina)
(ISC)² Foundation Graduate Scholarship

Veronica completed her master’s degree in informatics engineering in 2013 and two months later, moved from Argentina to the Czech Republic, where she now works in a Fortune 100 company’s Prague office.

In accepting her award, she said: “I want to say to the people working on the (ISC)² Foundation: Keep going! With these scholarship programs you not only provide economic help, but you also encourage and give hope to us all.”

Well said, Veronica.
THE SHAPE OF THINGS TO COME
A member ponders what the next generation of CISSPs will need

SINCE ITS FOUNDING in 1988, (ISC)² has striven to keep the CISSP relevant. It has continually balanced the needs of the marketplace that demands more and deeper specialization (read: more certifications) and the founding principles that separate the management of security (what CISSPs do) and the implementation of security (what technicians and engineers do).

So, how have we changed in the past 32 years?

The founding members, the grandfathered CISSPs (the giants on whose shoulders we stand), are gone. They helped write the CBK, created whole new bodies of knowledge, and probably could have recited the rainbow books from memory.

The second generation of CISSPs, those certified after 2001, moved the industry forward by leaps and bounds. Under their watch, CISSPs infiltrated the Fortune 1000 and helped define corporate and public policy in the G20 economies.

What skills does a third-generation CISSP need to possess?

Unlike our predecessors, who had it relatively easy, a modern CISSP must not only know the current CBK, and pass a more rigorous test, but she or he must also be a master communicator and manager.

Recognizing that information security touches on digital, physical, financial, psychological, and sociometric factors, and is heavily influenced by local, regional, and global legislative factors, it’s no surprise that more and more of our members are MBAs and/or J.D.s as well.

While we haven’t succeeded in getting Harvard or Stanford to add infosecurity electives to their MBA programs, we’ve made great strides in introducing the concept of cyber risk analysis to their curriculum. Though, to give credit where credit is due, it was the private equity firm KKR that started the ball rolling this year by adding the cyber-risk score to their assessment of the companies in their portfolio.

Insurance and risk analysis became part of the CISSP argot after Lloyd’s of London refused insurance coverage for cyber attacks to the energy sector because their defenses were perceived to be weak.

Top industries for CISSPs in 2020
1. Gaming
2. Energy
3. Private Equity/Mergers & Acquisition
4. Insurance/Underwriting Support
5. Manufacturing

Career Advice
• Get A Mentor/Become A Mentor.
If you’re a new CISSP, seek a mentor in your company or region. If you’re an old hand, pass your knowledge and wisdom to the next generation.
• Become An Effective Communicator.
Whether you attend Toastmasters, writing workshops, improv comedy, or theatrical training, it’s critical that you learn to communicate effectively.
• Network, Network, Network.
Networking is more than handing out business cards or asking for jobs. It’s a critical career boosting skillset. Get to know your peers at conferences, regional events, industry tradeshows. And talk about something other than work-related issues. Network with your peers, vendors, suppliers, and even (gasp!) the competition!

RAJ GOEL, CISSP, is an author, speaker, TV guru, self-described HIPAA and PCI compliance nerd, and cyber civil rights advocate.