

Resolving the Cybersecurity Workforce Shortage  
Cyber Workforce Strategy:  
Developing Professionals Internally  
The Role of the Adjunct in Educating  
the Security Practitioner  
Infosec Staffing

  
**ISSA International  
CONFERENCE**  
Conference Guide  
Included

# Resolving the Cybersecurity Workforce Shortage



**CYBERSECURITY  
CAREERS AND GUIDANCE**

When you analyze  
**70 BILLION DNS  
QUERIES A DAY**

you see what other  
security solutions miss.

**Stop by Booth #401**

Pivot through attackers' infrastructure and  
predict where future attacks are staged.

**TAKE IT TO THE CLOUD**  
**SECURITY BEYOND THE FIREWALL**

**OpenDNS**



OpenDNS is  
now part of Cisco.

# Table of Contents

## DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

### Feature

#### 16.....Resolving the Cybersecurity Workforce Shortage

By Kerry Anderson – ISSA member, New England Chapter

The author discusses potential approaches to resolving the cybersecurity talent shortage in the near and long term using collaborations of education, professional associations, and industry and offers ways an organization might solve their staffing issues today.

### Articles

#### 22.....Cyber Workforce Strategy: Developing Professionals Internally

By Jeff Fenton – ISSA Senior Member, Silicon Valley Chapter

This article outlines one organization's approach to developing cybersecurity professionals internally from its existing workforce, creating an internal training program administered by its Security Education and Awareness team.

#### 26.....The Role of the Adjunct in Educating the Security Practitioner

By Karen Quagliata – ISSA member, St. Louis Chapter

The cybersecurity industry faces a shortage of qualified professionals. Part of the solution is to better deliver cybersecurity education in colleges and universities. The purpose of this article is to equip cybersecurity professionals working as adjunct instructors with resources to deliver a more efficient and effective class.

#### 31.....Infosec Staffing

By Steve Riess – ISSA member, Chicago Chapter

This article discusses current employment market conditions for information security professionals.

ISSA International  
**CONFERENCE**

**Conference Guide** inserted after page 18.

### Also in this Issue

4.....[editor@issa.org](mailto:editor@issa.org)

5.....From the President

6.....Herding Cats  
Three Career Guidance Paths

7.....Sabett's Brief  
Who's Ready for a J.D.?

8.....Security in the News

10.....Association News

12.....ISSA's Cyber Security Career Lifecycle®  
Annual Update

14.....The Cyber Profession at Risk: Take Control  
of Your Cybersecurity Career Life Cycle



©2016 Information Systems Security Association, Inc. (ISSA)

The ISSA Journal (1949-0550) is published monthly by  
**Information Systems Security Association**  
12100 Sunset Hills Road, Suite 130, Reston, Virginia 20190  
703-234-4082 (direct) • +1 866 349 5818 (USA toll-free)  
+1 206 388 4584 (International)



## Cybersecurity Careers and Guidance

Thom Barrie – Editor, the ISSA Journal

Again our career-focused issue has garnered a lot of activity, ranging from the shortage of qualified

infosec professionals to getting the right employee and the right job in today's market.

Enterprise Strategy Group (ESG) and ISSA have collaborated on research—"The Cyber Profession at Risk: Take Control of Your Cybersecurity Career Life Cycle"—revealing that "most cybersecurity professionals struggle to define their career paths." ISSA has been working on rectifying this struggle with the Cyber Security Career Lifecycle (CSCL) program, now in its third year, helping infosec pros determine where they are in their careers and what they need to take their careers to the next level. CSCL evangelist and chair Candy Alexander provides an illuminating look at the program in "ISSA's Cyber Security Career Lifecycle Annual Update."

By now we are all familiar with the million-cyberworker shortage looming on the horizon as well as current unfilled needs. The problem? Lack of people with the necessary skills. Thanks, Thom, that's insightful. Okay, seriously.

Kerry Anderson, in "Resolving the Cybersecurity Workforce Shortage," suggests there is a great pool of potential infosec pros in what she calls the under-represented group of folks: women, minorities, veterans, and older workers.

She also emphasizes training and retaining existing cybersecurity teams—keep who you got and help them improve their skills.

Picking up on retaining and promoting existing employees, Jeff Fenton describes how a major enterprise looks to its own motivated staff in "Cyber Workforce Strategy: Developing Professionals Internally." While it takes effort to build out an excellent program, keeping and improving your existing workforce "strengthens the culture and benefits the corporation and the employee." Sounds pretty good.

And what about those still in school? Karen Quagliata looks at the state of qualified cybersec instructors in colleges and universities in "The Role of the Adjunct in Educating the Security Practitioner." It may be news to you, but nearly three-quarters of instructors are not tenured professors, but adjunct instructors who are often professionals working in their fields. That being the case, she offers up steps for adjuncts to improve their skills as well as ways for professional organizations like ISSA to help.

Finally, Steve Riess rounds us out with "Infosec Staffing," sharing insights from 25 years of helping organizations and workers find each other. Concerning the workforce shortage—more positions, less candidates—it's a seller's market for job seekers. If you are not finding the folks you need, perhaps you are just not going about it in the right manner.

*See you in Dallas, Thom*

## ISSA JOURNAL

Editor: Thom Barrie  
[editor@issa.org](mailto:editor@issa.org)

Advertising: [vendor@issa.org](mailto:vendor@issa.org)  
866 349 5818 +1 206 388 4584

### Editorial Advisory Board

- Phillip Griffin, Fellow
- Michael Grimaila, Fellow
- John Jordan, Senior Member
- Mollie Krehnke, Fellow
- Joe Malec, Fellow
- Donn Parker, Distinguished Fellow
- Kris Tanaka
- Joel Weise – Chairman, Distinguished Fellow
- Branden Williams, Distinguished Fellow

### Services Directory

#### Website

[webmaster@issa.org](mailto:webmaster@issa.org)  
866 349 5818 +1 206 388 4584

### Chapter Relations

[chapter@issa.org](mailto:chapter@issa.org)  
866 349 5818 +1 206 388 4584

### Member Relations

[member@issa.org](mailto:member@issa.org)  
866 349 5818 +1 206 388 4584

### Executive Director

[execdir@issa.org](mailto:execdir@issa.org)  
866 349 5818 +1 206 388 4584

### Advertising and Sponsorships

[vendor@issa.org](mailto:vendor@issa.org)  
866 349 5818 +1 206 388 4584

The information and articles in this magazine have not been subjected to any formal testing by Information Systems Security Association, Inc. The implementation, use and/or selection of software, hardware, or procedures presented within this publication and the results obtained from such selection or implementation, is the responsibility of the reader.

Articles and information will be presented as technically correct as possible, to

the best knowledge of the author and editors. If the reader intends to make use of any of the information presented in this publication, please verify and test any and all procedures selected. Technical inaccuracies may arise from printing errors, new developments in the industry, and/or changes/enhancements to hardware or software components.

The opinions expressed by the authors who contribute to the ISSA Journal are their own and do not necessarily reflect

the official policy of ISSA. Articles may be submitted by members of ISSA. The articles should be within the scope of information systems security, and should be a subject of interest to the members and based on the author's experience. Please call or write for more information. Upon publication, all letters, stories, and articles become the property of ISSA and may be distributed to, and used by, all of its members.

ISSA is a not-for-profit, independent cor-

poration and is not owned in whole or in part by any manufacturer of software or hardware. All corporate information security professionals are welcome to join ISSA. For information on joining ISSA and for membership rates, see [www.issa.org](http://www.issa.org).

All product names and visual representations published in this magazine are the trademarks/registered trademarks of their respective manufacturers.



## International Board Officers

### President

Andrea C. Hoy, CISM, CISSP, MBA,  
Distinguished Fellow

### Vice President

Justin White

### Secretary/Director of Operations

Anne M. Rogers  
CISSP, Fellow

### Treasurer/Chief Financial Officer

Pamela Fusco  
Distinguished Fellow

### Board of Directors

Debbie Christofferson, CISM, CISSP,  
CIPP/IT, Distinguished Fellow

Mary Ann Davidson  
Distinguished Fellow

Rhonda Farrell, Fellow

Geoff Harris, CISSP, ITPC, BSc, DipEE,  
CEng, CLAS, Fellow

DJ McArthur, CISSP, HiTrust CCSFP,  
EnCE, GCIH, CEH, CPT

Shawn Murray, C|CISO, CISSP, CRISC,  
FITSP-A, C|EI, Senior Member

Alex Wood, Senior Member

Keyaan Williams, Fellow

Stefano Zanero, PhD, Fellow

The Information Systems Security Association, Inc. (ISSA)<sup>®</sup> is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

With active participation from individuals and chapters all over the world, the ISSA is the largest international, not-for-profit association specifically for security professionals. Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial, and government.

The ISSA international board consists of some of the most influential people in the security industry. With an international communications network developed throughout the industry, the ISSA is focused on maintaining its position as the preeminent trusted global information security community.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

## Greetings ISSA Members

Andrea Hoy, International President



**T**his year our ISSA International Conference will be held in Dallas, Texas! And it is not too late to sign up.

—Are you with a security vendor, bringing new and emerging technology to the forefront? We want to see you.

—Were you part of the cybersecurity workforce, perhaps retired, and want to stay involved in our ISSA community? Come network and share your expertise.

—Are you new to cybersecurity, just getting your feet wet and not sure about next steps? We have members who want to meet with you and help.

—Perhaps you are not yet a member and picked up this *Journal* off a co-worker's desk? We want you to attend and take advantage of the membership discount by joining our global association.

—Thinking about volunteering to attend? Let us know. We'd love your help.

Our second annual "Party in the Sky" will be held at the Reunion Tower—listed in Trip Advisor's "Top 12 Thing to Do in Dallas." And for those of you wanting to hone your skills, there will be a Capture the Flag competition during the party.

**Chapter Leaders**—we know many of you are concerned about growing your chapter membership, dealing with fund-raising issues, getting compelling speakers, and dealing with tax filings. There will be a one-day session the day before the conference where you can meet with other chapter leaders to share strategies and lessons learned.

**CISOs** and those holding equivalent qualified roles—Our CISO Executive Forum was made just for you. The theme is "Big": big data, big network, bigger environment. But isn't everything bigger in Texas?!

**SIGs**—Are you interested in finding out more about Security Education and

Awareness, Women in Security, Health Care, or the Financial Industry? These SIGs are growing quickly and will be hosting a breakfast wednesday morning: come start your day with your special interest group.

ISSA's Board and staff have been working hard on establishing relationships that will provide value to our members. We have formed a strategic partnership with The Security Awareness Company (TSAC), founded by industry luminary and author Winn Schwartau. TSAC provides free on-demand resources such as modules for security concept training, interactive learning, downloadable security posters, a repository of searchable, indexed documents, and indexed security education materials, games, videos, and much more. We thank TSAC for creating the ISSA International Conference video that can be viewed on the [conference home page](#).

And we have some great news for those studying for their CISSP! We have successfully negotiated a 50-percent discount for members to obtain the *Official Handbook*. Contact your local chapter leader or ISSA HQ if interested.

I would like to close with some wonderful news from Egypt. The ISSA Egypt Chapter is now an accepted member of the United Nations Department of Economic and Social Affairs, participating with consultative status at UN conferences and events and spreading the word about ISSA activities at the global scale, furthering our international presence. Thank you, Mohamed El-Guindy, for sharing this latest accomplishment. See the story on page 11.

Moving forward,  
See ya'll in Texas!



## Three Career Guidance Paths

By Branden R. Williams – ISSA Distinguished Fellow, North Texas Chapter

Sometimes I get asked for career advice, based on my twenty years in the tech workforce, and it's a question that I think many of us in my age group struggle to answer. How did I end up here? Well, frankly, it's a combination of being in the right place at the right time, saying yes to new challenges outside of my comfort zone, and investing heavily in my education. For this month, I thought I would tell three stories to support each of those items so that readers can understand ways they can further plan their careers. For those wondering, my next career move will either go down the CISO/CIO route or the GM route. I've got a few things I need to accomplish first, but that's where I'd like to see myself in three to five years!

### Right place, right time

Job seekers require an element of luck to land their next great position. It could start with a chance meeting with a new executive, seeing and responding to a LinkedIn job posting, or a talking with a friend who casually mentions an opening in his company. Then it's up to you to take an active role in pursuing the lead.

In 2009 I was connected with several executives in conjunction with the sale of a business at which I was currently employed. After the sale of the company went in a direction I was not comfortable with, I reached out to one of those executives and suggested we try to work something out. A few meetings and presentations later, I essentially landed my current boss's job at a security company and was able to spend almost three and a half years at a storied information security company.

---

**Through good mentorship and strong leadership, I was able to lead the team to a place where we exceeded our goals...**

---

First, I was lucky to be involved in the negotiations of the sale, which allowed me to meet powerful people. Had I not taken an active role in reaching out to the company I wanted to go work for, I would not have had those great opportunities. It resulted in one of the most memorable jobs I've ever had. I even got to spend a day discussing security challenges with various luminaries on a show that was broadcast from the famed WQED in Pittsburgh—the very studio where Fred Rogers had his neighborhood.

### Saying yes to new challenges

There was a point in my career where I had to run a sales team. I've never been a quota-carrying member of the profession. As a GM in previous roles, I relied on a shared sales force combined with my army of consultants to ensure that we met or exceeded our bookings and revenue goals. What made me even remotely qualified to run a sales team?

The short answer, not much—but I knew I could take a risk by using the same principles I learned previously to lead that sales team. Through good mentorship and strong leadership, I was able to lead the team to a place where we exceeded our goals and demonstrated 200 percent year-over-year growth in twelve months.

### Investing in education

For a guy who was a mediocre high school student and couldn't wait to

finish my undergrad so I could fully commit my time to the workforce, I sure did keep punishing myself through two more schools and the same number of degrees. I didn't even wait two full years from the time I graduated with my bachelor's to the time I was enrolling in a master's program. After that, I at least waited a full six years before doing it all over again and eventually earning a doctorate. After I walked across that stage, my wife looked me square in the eyes and said, "OK, that's enough. No more. I've seen you walk three times. ENOUGH."

So, what did I do? Within a month I enrolled in a bunch of classes on Coursera so I could learn more applied data science techniques, which helped me conduct two studies in payments security and do extremely critical work at my job. She glared at me for a full five minutes, but she knew what she was getting into when she said "I do."

The point is that you have to invest both time and money to continue to make yourself marketable. You have to be willing to take on new challenges and risks, knowing that you will be out of your comfort zone for a period of time. And you must absolutely give yourself every opportunity to be in the right place at the right time.

### About the Author

*Branden R. Williams, DBA, CISSP, CISM is a seasoned infosec and payments executive, ISSA Distinguished Fellow, and regularly assists top global firms with their information security and technology initiatives. Read his blog, buy his books, or reach him directly at <http://www.brandenwilliams.com/>.*

## Who's Ready for a J.D.?

By Randy V. Sabett – ISSA Senior Member, Northern Virginia Chapter



My son entered his junior year of high school this year, so now we've begun the college selection and admission process. He really has taken a liking to aerospace and mechanical engineering (despite his summer job of writing C# data-filtering routines for a major online company). Given his penchant for spirited debate, though, I frequently tell him to consider being an attorney. He politely (okay, not really—more like vehemently) tells me “no way.” Despite his non-endorsement, I would highly recommend that any of you who have an interest in policy, law, or compliance to consider a legal career. As I frequently tell my technical audiences, the legal profession does not have enough people with your kind of skills. Let's explore this a little bit more.

Lawyers, by their very nature and training, tend to be conservative, risk averse, and opinionated. On that last point, one my best friends and colleagues who spent 42 years at the same firm used to say that “lawyers are often wrong but never in doubt.” While that may be true, law schools generally teach very little about cybersecurity. While more and more schools are developing cybersecurity courses, they don't necessarily (and, really, cannot) teach the core principles and subtleties that come into play when practicing cybersecurity law.

I had the fortunate experience of beginning my career on the technical side as a crypto engineer and, years later, continuing on to become an attorney. What was most fascinating to me was the different style of thinking necessary for learning and practicing the law. Unlike technical disciplines that are very precise, the law is malleable and over the course of time can change fairly signifi-

cantly. Such change, however, happens at a very slow pace.

Whereas Moore's Law has relatively accurately predicted continuous increases in compute power for a number of years, we don't have any type of analog in the law (and if the current Congress is any indication, it's no surprise why changes in the law are so slow). Such slow change often leads to laws that are outdated and subject to tortured interpretations. Two prime examples of this are the Electronic Communications Privacy Act (ECPA) (enacted in 1986 and amended several times since then) and the Computer Fraud and Abuse Act (CFAA) (also enacted in 1986 and also amended several times). Despite those amendments, many criticize the laws as being woefully out of date and subject to much misinterpretation. It takes lawyers with an excellent appreciation of how security really works to make arguments under these laws.

For those of you potentially considering a legal career, I like to describe the profession in terms of three “buckets.” First (and probably the way that many lawyers today entered cybersecurity law as a profession), the adversarial side of the practice involves disputes of varying types, often culminating in litigation. These can range from corporate claims of companies engaging in questionable online activities to individuals being charged with computer crime. The second bucket, at the other end of the spectrum, involves advising and counseling on numerous different aspects of cybersecurity. This involves providing legal advice to companies on their policies, practices, and liabilities associated with their approach to cybersecurity. It can also involve advocating or even lobbying before government officials.

The third bucket, that in some ways straddles the other two, is incident response. This can involve something as innocuous as a temporarily lost but then found physical notebook of employee information all the way through to a massive, five-year-long APT incursion into a network of a financial services company that was brought to the attention of my client by federal law enforcement. Both of these are situations I've had to handle, along with numerous others.

So in closing, I would strongly encourage anyone in the cybersecurity industry that has an interest in the law to consider a legal career. I am having such a great time—and you could too. If you have any questions, please feel free to shoot me an email...or if you want to be talked out of it, I will give you my son's email address.

### About the Author

Randy V. Sabett, J.D., CISSP, is Special Counsel at Cooley LLP ([www.cooley.com](http://www.cooley.com)), and a member of the Boards of Directors of ISSA NOVA and the Georgetown Cybersecurity Law Institute. He was a member of the Commission on Cybersecurity for the 44<sup>th</sup> Presidency, was named the ISSA Professional of the Year for 2013, and can be reached at [rsabett@cooley.com](mailto:rsabett@cooley.com). The views expressed herein are those of the author and do not necessarily reflect the positions of any current or former clients of Cooley or Mr. Sabett.

## News That You Can Use...

Compiled by Joel Weise – ISSA Distinguished Fellow, Vancouver, BC, Chapter and  
Kris Tanaka – ISSA member, Portland Chapter

### IoT and Your Digital Supply Chain

<http://www.csoonline.com/article/3120846/security/iot-and-your-digital-supply-chain.html>

The Internet of Things is really a mess with a great deal of code being released before it's tested and no means to update it. The author points out that we've been down this road before with the evolution of the Internet. Sadly, it looks like we are repeating the same mistakes with the development of IoT.

### New Report: 12 Hot Markets for Cybersecurity Jobs

<http://www.darkreading.com/risk/new-report-12-hot-markets-for-cybersecurity-jobs/d/d-id/1326927>

It's no surprise that the demand for cybersecurity professionals is growing and that companies are scrambling to attract and retain highly qualified candidates. Although the challenge to increase the talent pool is predicted to get worse before it gets better, what is encouraging is that more and more decision-makers are placing an emphasis on security management and its ability to help organizations reach their performance targets.

### HP Detonates Its Timebomb: Printers Stop Accepting Third-Party Ink En Masse

<http://boingboing.net/2016/09/19/hp-detonates-its-timebomb-pri.html>

Apparently some HP printers will stop working if they use OEM printer cartridges. I don't see how the company will be able to avoid dealing with a restraint of trade issue, especially if people were not given any forewarning. Imagine the wave of frustration that will be generated when what was thought to be a perfectly good printer cartridge suddenly stops working.

### The NSA Is Hoarding Vulnerabilities

<https://www.schneier.com/crypto-gram/>

For those who subscribe to Bruce Schneier's Cryptogram (and if you call yourself a security practitioner you should), the lead article is probably not a big shock. Yikes, the National Security Agency is hoarding security vulnerabilities! Surprised? Not really. The larger debate is the basic trade-off. Should the US government hoard vulnerabilities for offensive purposes, or would we all be safer if these were shared and patched? My feeling is that if the NSA found a vulnerability, more than likely someone else has found the same one as well. So why not get it patched? I'm sure the NSA can find other ways to differentiate themselves.

### Top Colleges for Cybersecurity

<http://www.securityweek.com/hunting-snark-machine-learning-artificial-intelligence-and-cognitive-computing>

I find it a bit strange that there is only one university on the list from the west coast, especially considering the number of top-tier universities there. I would be remiss if I did not mention the joint NSA and DHS sponsorship of the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program. This is a great way for someone in college to enter the information security field. General information on the program can be found here: <https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/>

And here is the current list of institutions: <https://www.iad.gov/nietp/reports/current-cae-designated-institutions.cfm>

### Law Enforcement Hacking Declared Search under Fourth Amendment

<http://searchsecurity.techtarget.com/news/450304323/Law-enforcement-hacking-declared-search-under-Fourth-Amendment>

The United States District Court for the Western District of Texas has ruled that law enforcement's use of malware to attack and access one's computer is by definition considered to be search. This will obviously need some clarification as other courts have ruled that hacking does not violate the Fourth Amendment. As an aside, those interested in this issue may wish to follow the proposed updates to Rule 41 of the Federal Rules of Criminal Procedure: <https://www.eff.org/deeplinks/2016/04/rule-41-little-known-committee-proposes-grant-new-hacking-powers-government>

### Photos on Dark Web Reveal Geo-locations of 229 Drug Dealers – Here's How

<http://thehackernews.com/2016/09/dark-web-drug-weapon.html>

This should be an obvious one, but clearly not all criminals are as computer savvy as they think they are. It appears that some criminals take pictures of contraband and include the EXIF (Exchangeable Image File Format) data, which often contains image information including GPS coordinates of the location where the photo was taken.

### Yahoo Says 500 Million Accounts Stolen

<http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/>

Ouch. The breach reportedly took place in 2014. Then, two years later, information surfaces that a hacker, going by the name of "Peace," is selling user data from over 200 million Yahoo accounts. As the investigation continues to uncover new details, we can't help but wonder what other "surprises" are waiting for us.

### Here's What Trump and Clinton Had to Say about Cybersecurity and Cyberwarfare in the Debate

<http://venturebeat.com/2016/09/27/heres-what-trump-and-clinton-had-to-say-about-cybersecurity-and-cyberwarfare-in-the-debate/>

Did Donald Trump and Hillary Clinton take advantage of the opportunity to showcase their cybersecurity knowledge during the first of three presidential debates? Not really. However, there was one positive takeaway from the televised encounter—it is clear that cybersecurity is now at the forefront of the US national security conversation. Hallelujah—it's about time.





# Reduce cyber risk and simplify compliance

Coalfire is the single source for your cybersecurity and compliance needs. We deliver the expert advice, assessments, testing, and tools that help you identify risks, close gaps, and meet your industry's regulatory requirements.

Partner with the cybersecurity experts and protect your business today and in the years to come.

Cloud | Payments | Healthcare | Financial Services | Education  
State and Local Governments | Critical Infrastructure

[Coalfire.com](https://www.coalfire.com) | 877.224.8077

## ISSAEF Annual Fund-Raiser Set to Kick Off in Dallas



The ISSA Education Foundation (ISSAEF) is pleased to announce its fifth annual fund-raiser in conjunction with ISSA's annual conference to be held November 2 and 3 in Dallas, Texas. Please stop by our booth at the conference EXPO to learn about our scholarship program and make a tax-deductible (USA) donation for a chance to win great prizes at the drawing, such as a SANS course donated by SANS in memory of Dr. Gene Schultz, a former SANS instructor and also one of the Foundation's named memorial scholarships.

We're looking for volunteers to staff our booth this year. Please contact Deb Peinert at [dpeinert@yahoo.com](mailto:dpeinert@yahoo.com) if you can help.

Chapters, members, and corporations wishing to support the work of the foundation can make a tax-deductible donation at our website: [www.issaef.org](http://www.issaef.org). For donating tax-deductible prizes for the upcoming annual fund-raiser, please contact Angela Spease for more information at [aspease@issa-foundation.com](mailto:aspease@issa-foundation.com).

The 2016 scholarship winners will soon be announced. Many thanks to Dr. Javier Torner, Scholarship Selection Committee chair, and his dedicated committee for their work in granering and vetting this year's candidates. If you want to help the Foundation next year by serving on this committee, please contact Dr. Torner at [jtorner@csusb.edu](mailto:jtorner@csusb.edu).

### ISSA SPECIAL INTEREST GROUPS

#### Special Interest Group Webinars

Want to hear more from ISSA's Special Interest Groups? [Join free here](#).

ISSA.org => Learn => Special Interest Groups

##### Women in Security SIG

November 14: 4:00 pm - 5:00 pm EST. [Promoting Creativity](#).

##### Healthcare SIG

December 15: 12:00 pm - 1:00 pm EST. [Auditing and Access to Electronic Health Records](#).

##### Financial SIG

December 9: 1:00 pm - 3:00 pm EST. [Financial Security Incidents: Forecast for 2017](#).

## The Open Forum

The Open Forum is a vehicle for individuals to provide opinions or commentaries on infosec ideas, technologies, strategies, legislation, standards, and other topics of interest to the ISSA community. Please submit to [editor@issa.org](mailto:editor@issa.org).

### ISSA Fellow PROGRAM

## Congratulations 2016 Fellows

#### Distinguished Fellow

Randall Frieztzsche  
Gordon Mitchell  
David Reed

#### Fellow

Michael Brown  
Patrick Geborys  
George Grachis  
Patrick Laverty  
Colleen Murphy  
William Smith Jr.  
Timothy Stanley  
Keyaan Williams

### ISSA CISO FORUM

The CISO Executive Forum is a peer-to-peer event. The unique strength of this event is that members can feel free to share concerns, successes, and feedback in a peer-only environment. Membership is by invitation only and subject to approval. Membership criteria will act as a guideline for approval.

**Dallas, TX: November 3-4, 2016** – Theme: **Big!**

For information on sponsorship opportunities, click [here](#) or go to [ISSA.org](http://ISSA.org) => Learn => CISO Executive Forum.

## ISSA CISO Virtual Mentoring Series

ISSA.org => Learn => Web Events => CISO Mentoring Webinar Series

**LEARN FROM THE EXPERTS!** If you're seeking a career in cybersecurity and are on the path to becoming a CISO, check out the [schedule of upcoming presentations](#).

## ISSA Chapter Events

ISSA.org => Learn => Event Calendar

- **October 12-13: Honolulu, HI.** "Hawaii's 23rd Annual Discover Security Conference 2016." For details and registration, click [HERE](#).
- **October 13: Long Beach, CA.** "From the Basement to the Boardroom" - 31st Annual ISSA SoCal Symposium." For details and registration, click [HERE](#).

Get your events published in the *ISSA Journal* and E-News. You will build chapter activities, and your sponsors will appreciate the extra publicity. Send your events with the following information in this exact format: Date, Chapter Name, Time, Location, Title, Speaker, Sponsor, and a hyperlink to Details and Registration. Email to [mdelacruz@issa.org](mailto:mdelacruz@issa.org).

For more ISSA and industry events, visit the [ISSA Calendar](#).



## ISSA Journal Scholastic Writing Award for Best Student Article Extension

ISSA.org => Learn => Journal

The ISSA Journal Editorial Advisory Board is inaugurating an annual \$1,000 ISSA Journal Scholastic Writing Award for the best article submitted by a current college/university student.

The submission period is now open and the Board will accept articles until November 1, 2016. We encourage students to follow the published [editorial calendar](#) but will consider any submission that is focused on information security.

The Board will select the best article that meets our professional standards for publication and will feature it in the Jan-

uary 2017 “Best of 2016” issue of the *ISSA Journal*. Recipient must be attending an accredited college or university full time and actively pursuing a degree. Submit your article and proof of enrollment to [editor@issa.org](mailto:editor@issa.org) by November 1, 2016.

Please review our [editorial guidelines](#) and the [2016 editorial calendar](#). Questions may be directed to [editor@issa.org](mailto:editor@issa.org).

## CSCL Pre-Professional Virtual Meet-Ups

ISSA.org => Learn => Web Events => CSCL Meet-Ups

So, you think you want to work in Cybersecurity? Not sure which way to go? Not sure if you're doing all you need to do to be successful? Check out Pre-Professional Virtual Meet-Ups to help guide you through the maze of cybersecurity.



October 13: 11:00 am - 12:30 pm EST. [Addressing the Cyber Security Skills Gap](#).

## ISSA Egypt Chapter's International Involvement

ISSA Egypt Chapter is keen to cooperate with international organizations to spread the word under the ISSA name. This year, ISSA Egypt partnered with the Institute for Global Security and Defense Affairs (IGSDA), an online think tank based in Abu Dhabi and formed by defense and security experts from different disciplines including NATO experts. Partnering with international organizations helps promote ISSA in different ways, such as online presence and participation in activities and international conferences.

ISSA Egypt chapter president Mohamed El-Guindy cooperates with international entities under ISSA Egypt to help promote ISSA's vision and mission in the cybersecurity field. In September, the Institute for Global Security and Defense Affairs (IGSDA) organized a National Security Conference in Taiwan in cooperation with Taiwan Think Tank (TTT). TTT invited an elite group of international experts in the fields of global, international, and national security from Taiwan, Italy, Greece, the United Kingdom, Belgium, France, Jordan, Egypt, and Japan, as well as academic experts from NATO, to participate at this conference.

As a partner with IGSDA, ISSA Egypt was invited to present at the conference. During the September 12-13 conference, ISSA Egypt chapter delivered a presentation on terrorism activities in cyberspace that was appreciated by all experts participating in the conference. The conference was wonderful opportunity for networking and collaboration with experts



ISSA Egypt chapter president Mohamed El-Guindy, right, at the National Security Conference in Taiwan.

and senior officials from the ministries of Foreign Affairs and Defense and the National Security Council.

Recently, ISSA Egypt Chapter was accepted as a member of UN Department of Economic and Social Affairs (DESA) NGO branch. UN DESA is the focal point within the UN Secretariat for non-governmental organizations in consultative status with the Economic and Social Council (ECOSOC) and for NGOs seeking status. Membership with the UN DESA will open doors for ISSA Egypt Chapter to get support from the UN, participate in international UN events and conferences, and gain intergovernmental support.

We encourage all ISSA chapters to partner with international organizations and participate in international activities to help spread the word.

—ISSA Egypt chapter president Mohamed El-Guindy



## ISSA's Cyber Security Career Lifecycle® Annual Update

This month will mark the third anniversary of ISSA's launching the Cyber Security Career Lifecycle (CSCL). This past year, the CSCL has accomplished some major milestones and gained visibility beyond our membership. The Cyber Security Career Lifecycle has been awarded a trademark by the US Federal Trademark Office, so it is now official!

ISSA also gained visibility with our message on how to use the CSCL "get in and stay in" the profession, being invited to present at both the 2016 RSA Conference and the 2016 Blackhat Conference. The message behind these presentations speaks to the necessity of applying the Cumulative Knowledge Model through the Cyber Security Career Lifecycle. Let's take a look.

The Cyber Security Career Lifecycle is a methodology:

- A means to look at where individuals are in their career and understand what is needed by way of knowledge, skills, and aptitude (KSAs) in order to be successful.
- A means to identify options in regards to a career path based on where the individual currently is, and if choosing a certain path, what additional KSAs are needed to get to that next level.

The CSCL enables us to apply the cumulative knowledge model that many of us have used through ISSA service offerings without even realizing it.

The concept of the cumulative knowledge model starts with establishing a foundational knowledge base, which many of us have established with the CISSP certification; others have university degrees to form that knowledge base. The key is that it provides the basis for building your knowledge. It is mastering the basic principles of information security. We can consider this part of the Pre-Professional or Entry Level phase of one's career. However, our need for additional knowledge and skills doesn't stop there.

As information or cybersecurity professionals—technologists—it is crucial that we stay on top of new technologies. Technology seems to change at the speed of light, and we need to learn quickly how it works and go beyond that to understand its vulnerabilities and risks. Unfortunately, traditional training programs can't offer this "cutting edge" knowledge, so we must look to other means. This is where ISSA adds so

### Cumulative Knowledge

- "Increasing by successive addition"
- Progressive through the CyberSecurity Career Lifecycle
- Building on the knowledge of those that came before you

### Traditional programs to baseline knowledge;

- Universities and colleges
- Industry Certifications



### "Just in Time" Learning

- Responsive to new technologies and/or threats
- New, innovative and scalable training with quick delivery mechanisms
- Trusted sources from quality providers
- Security Users Groups and/or Meet-ups
- YouTube Security Channels

much value. As members, we are able to obtain this "just in time" learning from various services such as presentations at chapter meetings, ISSA's virtual mentoring, web conferences, and even online videos found on YouTube and other video apps.

However, technology is only one part of KSAs. Another critical component is building out the "soft skills" through professional development. We have identified in the CSCL KSAs that in addition to having sharp technical skills one should include effective communications and knowledge of business operations and project management, which are just as important. Often times when we look at our professional development plans, these KSAs are overlooked and are only identified through on-the-job challenges and experiences. It is during times such as these that our personal network or mentoring through ISSA helps us identify the need to develop skills in this area and where we can get help.

So, it is when we combine foundational knowledge with technical "just in time" learning and professional development based on experiences that we come to the point of cumulative knowledge, which is unique to each individual and is progressive throughout an individual's cybersecurity career.

By being a member of ISSA, you are provided a unique opportunity to obtain all of these in a "one stop shopping experience" from a vendor- and certification-agnostic organization. The "just in time" technical learning, professional development, and guidance from other ISSA members will provide you with *your* cumulative learning, leading to a successful career.



Candy Alexander, CISSP, CISM; Chair, Cyber Security Career Lifecycle Program

SEE US AT BOOTH #201

# CloudPassage

## SOLVING KEY SECURITY CHALLENGES

On-demand, automated server & cloud workload security that works anywhere, at any scale.



**WORKLOAD PROTECTION**  
Protect Servers and Cloud-based Workloads From Attack



**MICROSEGMENTATION**  
The Fastest, Easiest Way to Control East-West Traffic



**COMPROMISE DETECTION**  
Your Servers Have Been Compromised. How Can You Tell?



**AUTOMATED COMPLIANCE**  
Don't Let Manual Processes Hold Up Compliance



**SECURITY AT DEVOPS SPEED**  
Don't Let Security Put the Brakes on DevOps



**AWS EC2 SECURITY**  
Enhanced Security and Compliance for AWS EC2

## VISIT OUR SESSION ON THE EIGHT IMPERATIVES FOR AGILE AND SCALABLE CLOUD SECURITY

Wednesday, November 2 at 1:45 pm in the Cumberland A/B Room.  
Presented by Sami Laine, Principal Technologist, CloudPassage

To learn more, visit [cloudpassage.com](https://cloudpassage.com) or call 800-215-7404

## New findings from “The Voice of Cybersecurity Professionals (Part I): A Cooperative Research Project by ESG and ISSA”

# The Cyber Profession at Risk: Take Control of Your Cybersecurity Career Life Cycle

According to research being released this month, most cybersecurity professionals struggle to define their career paths.

This new finding comes at a time when there are more data breaches, net new malicious IP addresses created per day, zero-day vulnerabilities as well as more credential theft and phishing attempts than ever before. Organizations are willingly bolstering their defenses and making cybersecurity a top business and IT priority in response. Yet 46 percent of organizations still claim to have a problematic shortage of cybersecurity skills, according to ESG research.

This picture paints an escalating and dangerous game of cybersecurity “cat and mouse.” Today’s cybersecurity professionals reside on the front line of this perpetual battle, tasked with applying limited resources to out-think would be cyber attackers and defend their organizations. Alarming, cybersecurity professionals often accept this challenge knowing they are undermanned for the fight.

How well are cybersecurity professionals holding up? Do they have the skills necessary for their jobs as cyber adversaries develop new exploits? Are they able to coordinate on cybersecurity strategies and tactics with their business and IT peers? Are they overwhelmed and burned out?

To answer questions like these, the Enterprise Strategy Group (ESG) and ISSA teamed up and initiated a primary research project in mid-2016 with the goal of capturing the voice and thoughts of cybersecurity professionals on the state of their profession and gaining a perspective on situational analysis from those closest to the fight. In pursuit of this goal, ESG/ISSA surveyed 437 cybersecurity security professionals (and ISSA members). Survey respondents represented organizations of all sizes and include professionals located in all parts of the world.

Those participating in this project were asked a series of questions on a variety of cybersecurity topics. Part I of the research is focused on the life cycle of cybersecurity professional careers. **Based upon the data collected as part of this project, this report concludes: Nearly two-thirds (65 percent) of respondents do not have a clearly-defined career path or plan to take their careers to the next level.**

This is likely due to the diversity of cybersecurity focus areas, the lack of a well-defined professional career development standard and map, and the rapid changes in the field itself. Business, IT, managers, academics, and public policy leaders

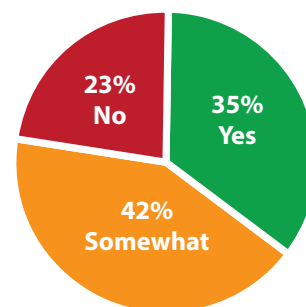
should take note of today’s cybersecurity career morass and develop and promote more formal guidelines and frameworks that can guide professionals in their career development in the future. Independent organizations such as ISSA with its Cybersecurity Career Lifecycle® are taking the lead on such initiatives.

Other conclusions include:

- **Cybersecurity certifications are a mixed bag.** Over half (56 percent) of survey respondents had received a CISSP and felt it was a valuable certification for getting a job and gaining useful cybersecurity knowledge. Other than the CISSP certification, however, they appear lukewarm on other types of industry certifications.
- **34 percent of survey respondents said that achieving additional security certifications was an effective method for improving one’s knowledge, skills, and abilities (KSA).** Only a third of respondents agreed with what has been a common belief in the cybersecurity world, especially among inexperienced professionals looking to move ahead.
- **Continuing cybersecurity training is lacking.** When asked if their current employer provides the cybersecurity team with the right level of training in order for them to keep up with business and IT risk, more than half (56 percent) answered “no,” suggesting that their organizations needed to provide more or significantly more training for the cybersecurity staff.
- **There is a moral imperative that attracts people into the cybersecurity profession.** When asked why they became cybersecurity professionals, 27 percent said it gave them the chance to use their technical skills to help protect valuable business and IT assets, while 22 percent claim they were attracted to the morality of the profession. In the mind of many cybersecurity professionals, their jobs equate to a battle between right and wrong.
- **Yet...cybersecurity professionals are only relatively satisfied with their jobs.** While 41 percent of respondents claim to be very satisfied with their jobs, 44 percent are

### Cybersecurity Career Path Preparation

Do you believe you have a well-defined career path and plan to get to the next level? (Percent of respondents, N=437)



only somewhat satisfied, and 15 percent are not very satisfied or not at all satisfied. Respondents point to things like financial compensation (32 percent), organizational culture that includes cybersecurity (24 percent), business management's commitment to cybersecurity (23 percent), and the ability to work with a highly-skilled and talented cybersecurity team (22 percent).

- **And...Cybersecurity professionals are in extremely high demand.** This is another critical data point and “red flag” exposed in this research project as 46 percent of cybersecurity professionals are solicited to consider other cybersecurity jobs (i.e., at other organizations) at least once per week. In other words, cybersecurity skills are a “sellers’ market” where experienced professionals can easily find lucrative offers to leave one employer for another. Turnover in the cybersecurity ranks could represent an existential risk to organizations in lower paying industries like academia, health care, public sector, and retail. Organizations that don't provide continuous training to cybersecurity staff will fall farther behind cyber adversaries while increasing business and IT risk. This should be an unacceptable situation for all business and technology managers.

When it comes to the role of the CISO, the report also concludes that many CISOs are not getting enough face time in the boardroom; internal relationships need work between cybersecurity, business, and IT teams to be “good”; and there is high CISO turnover due to business and economic roots.

Given these new insights, how can you take control of your cybersecurity career? The report provides this direction for you:

- **Cybersecurity professionals starting their career should seek out help.** Junior security professionals should dedicate ample time to explore career opportunities, determine career choice options, and create a personal strategy to achieve their goals over time.
- **Cybersecurity managers should support staff members with mentorship and guidance.** CISOs and VP-level cybersecurity professionals (as well as HR managers and business executives) should reach out to staff members and provide counseling, training, and coaching to help them understand career choices and what steps are necessary to get them where they want to go.
- **Cybersecurity training, education, and professional organizations should dedicate further resources toward career development.** These institutions must evolve beyond networking groups and specific training programs and adopt programs and services to help cybersecurity professionals with career development. It would also be helpful to establish global standards with regards to job titles, descriptions, KSAs, and career mappings—a standardization that is developed by the profession for the pro-

## Most Effective Methods for Increasing KSAs

Which of the following would you consider the most effective methods for increasing your knowledge, skills, and abilities as a cybersecurity professional?  
(Percent of respondents, N=437, five responses accepted)



profession that remains agnostic to any training/certification/government.

Cybersecurity professionals can use the research presented in this report as a guideline for career planning by reading the “Top 5 Research Implications for Cybersecurity Professionals.” The research also offers the “Top 5 Research Implications for Employers.”

A cybersecurity career can be fraught with challenges as individuals struggle to keep up with skills, work at low cybersecurity IQ organizations, and try to cope with the stress of their jobs. In spite of these issues, however, it is encouraging that 79 percent of survey respondents strongly agree or agree with the statement: “Overall, I am happy as a cybersecurity professional.” This data point speaks volumes about professionals who are willing to passionately fight the good fight regardless of their personal situations.

Visit the ISSA website to learn more details about the report, responses and recommendations – [ISSA.org/esgsurvey](https://www.issa.org/esgsurvey).

**Note to readers:** This article is excerpted from “The Voice of Cybersecurity Professionals (Part I): A Cooperative Research Project by ESG and ISSA.” Stay tuned for a subsequent report, Part II in the series, to be published in November of this year that will concentrate on cybersecurity professionals’ opinions about their organizations’ cybersecurity practices as well as the overall state of cyber security today.

—Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group (ESG) and Candy Alexander, CISO, ISSA Cyber Security Career Lifecycle Chair

# Resolving the Cybersecurity Workforce Shortage



By Kerry Anderson – ISSA member, New England Chapter



**The author discusses potential approaches to resolving the cybersecurity talent shortage in the near and long term using collaborations of education, professional associations, and industry and offers ways an organization might solve their staffing issues today.**

## Abstract

The cybersecurity field is currently experiencing a growing shortage of practitioners with over a quarter-million positions remaining unfilled in the US alone and a predicted shortfall of 1.5 million cybersecurity professionals by 2019. This article discusses potential approaches to resolving this talent shortage in the near and long term using collaborations of education, professional associations, and industry. Also, the article offers ways an organization might solve their staffing issues today.

There is little debate that there exists a need to expand the cybersecurity workforce to satisfy the increasing demand for practitioners to secure private and public organizations. According to the US Bureau of Labor Statistics, in 2016 more than two hundred thousand positions in cybersecurity jobs went unfilled in US alone with a 74 percent increase in job posting over the past five years.<sup>1</sup> Industry experts put the global number at over a million

vacant cybersecurity positions.<sup>2</sup> Mike Brown, the CEO of Symantec, predicts a shortfall of 1.5 million cybersecurity professionals by 2019.<sup>3</sup>

Several strategic collaborations between industry, education, and certification organizations are pursuing ways to recruit and train new practitioners. These initiatives include introducing security and technology knowledge at the K-12 levels, such as (ISC)<sup>2</sup>'s Center for Cybersecurity and Education.<sup>4</sup> However, these initiatives have lengthy start-up times before yielding a significant increase in the cybersecurity workforce. As a profession, we need to generate both near-term as well as long-term solutions to growing the cybersecurity workforce.

The approach involves simultaneously pursuing a number of tactics to increase the overall size of the available cybersecurity workforce, including:

<sup>1</sup> Morgan, S. (2016) "One Million Cybersecurity Job Openings in 2016," - <http://www.forbes.com/sites/stevenmorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#89a09d7d274>.

<sup>2</sup> Cisco, "Mitigating the Cybersecurity Skills Shortage," Cisco Security Advisory Services (2016) - <http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf>.

<sup>3</sup> Frank, Hope (2016) "Q1 Cybersecurity Snapshot," LinkedIn - <https://www.linkedin.com/pulse/cyber-security-snapshot-hope-frank>.

<sup>4</sup> Center for Center for Cyber Security and Education (2016) - <https://www.isc2cares.org/Default.aspx>.



- Establishing collaborations between businesses, professional organizations, and education to develop current and future practitioners
- Recruiting under-represented groups such as minorities, women, and veterans
- Thinking outside the box when recruiting for cybersecurity positions, such as practitioners from other professions
- Creating recruitment and development channels for individuals looking to transition into cybersecurity
- Actively courting and developing Gen Y and Gen Z

## Near-term approaches

### Increase participation from under-participation workforce segments

Cybersecurity workforce studies, such as (ISC)<sup>2</sup> Global Information Security Workforce Study,<sup>5</sup> have repeatedly shown that some segments of the workforce are under-represented in the cybersecurity field: female practitioners make up only ten percent of the cybersecurity workforce despite the escalating growth in the field, and this situation has not changed over the last two years.<sup>6</sup> The participation of female practitioners has declined by three percent since an IDC study reported 13 percent in the field in 2006.<sup>7</sup> There is a similar situation with some minority groups. African Americans compose about seven percent, and Hispanic account for five percent of cyber-

security practitioners.<sup>8</sup> This participation is low when compared with the overall workforce or even IT labor pool.<sup>9</sup> These under-represented groups offer an opportunity to increase<sup>10</sup> the cybersecurity workforce in the near and long term. This is important because both Gen Y and Gen Z have significant numbers of minorities, especially individuals of Latino and mixed-race heritage.<sup>11</sup>

### Applying a previously successful strategy

Another professional field took a proactive approach when faced with a similar situation. According to the *Journal of Accountancy*, in 1951 there were only 500 female certified public accountants. Currently, female accounting practitioners make up approximately sixty percent of accountants and auditors in the US, with an estimated 843,000 women in the accounting workforce.<sup>12</sup> This statistic reflects the forecasts from a 1984 AICPA Future Issues committee report, which said that female accounting practitioners would comprise at least half of the accounting workforce within two decades.

This outcome did not take place without an action plan. It resulted from the collaboration between professional associations, such as the American Institute of CPAs (AICPA), and educational institutions to recruit women into the accountancy and auditing fields. This situation is a dramatic change

5 ISC2 Global Information Security Workforce Study (2015), available at [https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-\(ISC\)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf](https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf)

6 "Women in Security: Wisely Positioned for the Future of InfoSec," a Frost & Sullivan White Paper (2015) – <https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/2015-Women-In-Security-Study.pdf>.

7 Bagchi-Sen, S.; Rao, H.; Upadhyaya, S.; Chai, S. (2009) Women in Cybersecurity: A Study of Career Advancement, IT Pro.

8 Chabrow, E. (2011) Minorities Scarce in IT Security Field – <http://www.bankinfosecurity.com/women-minorities-scarce-in-security-field-a-4143>.

9 Ibid.

10 "Number of Female Accountants Increasing," AccountingWeb (2006) – <http://www.accountingweb.com/topic/education-careers/number-female-accountants-increasing>.

11 Williams, A. (2015) "Move Over, Millennials, Here Comes Generation Z," *The New York Times* – [http://www.nytimes.com/2015/09/20/fashion/move-over-millennials-here-comes-generation-z.html?\\_r=0](http://www.nytimes.com/2015/09/20/fashion/move-over-millennials-here-comes-generation-z.html?_r=0).

12 Wootton, C.; Spruill, W. (1994) "The Role of Women in Major Public Accounting Firms in the United States during World War II," *Business and Economic History*.

When it comes to cybersecurity, being out of the loop is a dangerous place.

Shared Knowledge.  
Shared Security.



Your Membership Will Provide You With:

- Peer-to-Peer Networking
- Continued Education & Training
- Career Development, Growth and Opportunities

Developing and Connecting Cybersecurity Leaders Globally



# ISSA

Information Systems Security Association



[www.issa.org](http://www.issa.org)

from decades ago when female students were discouraged from majoring in accounting.<sup>13</sup>

A similar strategy between cybersecurity professional organizations and higher education might result in an increase in the supply of entry-level cybersecurity practitioners over the next five to ten years. In addition to creating strategic collaborations between professional associations and higher education, colleges and universities need to demonstrate a commitment to creating a diverse cybersecurity workforce for today and the future through their actions, including:

1. Recruiting a diverse faculty
2. Establishing mentor programs with industry
3. Providing increased opportunities for visibility for female, minority, and other non-traditional students, such as older students or veterans
4. Using female and minority alumni as “ambassadors” in outreach efforts
5. Offering course electives aimed at female and minority students, such as leadership classes for these student segments

One professional organization is specifically seeking to promote cybersecurity careers among under-represented groups including women, minorities, and veterans. The International Consortium of Minority Cybersecurity Professionals (ICMCP) launched in 2014 with a mission to bridge this “great cyber divide” in the cybersecurity profession.<sup>14</sup> ICMCP offers programs and services to these groups to assist them in gaining skills and visibility to promote their careers, including:

- Mentoring opportunities for entry and mid-career cybersecurity practitioners
- Networking opportunities
- Skills workshops

The vision is ICMCP is building a pipeline of cybersecurity practitioners at all levels and supporting them throughout their careers. Their efforts have the potential to broaden the pool of available experienced cybersecurity practitioners.

### Calling all transitioning cybersecurity workers

Not all practitioners set out with a career in cybersecurity as the final destination. At a recent SecureWorld conference in Boston, a session speaker mentioned that many current practitioners were not specifically trained for the cybersecurity field or planned a career in the profession. Some individuals may look to transition in the cybersecurity field from another discipline. These people may possess strong competencies from their prior career experiences, but may require the acquisition of some security-specific proficiencies. The advantage of developing transitioning practitioners is a possibly shorter start-up period and perhaps lower development costs.

These transitioning practitioners may need accelerated and targeted training versus the more traditional competency acquisition programs. They also may be able to assume higher-level positions because of their years of experience and knowledge in other fields. Colleges and universities may consider developing accelerated programs aimed at career changers such as similar programs that allow individuals with prior college degrees to earn degrees in medical and technical fields, such as nursing. This strategy would provide a way of increasing the cybersecurity labor pool in the near-term, as well as offering the advantage of providing teams with diverse proficiencies and experiences.

In the 1980s, a Massachusetts-based technology corporation re-trained unemployed teachers as technologists to fill a shortage of employees. A similar approach might produce cybersecurity practitioners in a year to 18 months, depending on the specialization.

### Look outside the box for position candidates

Cybersecurity organizations need to broaden their pool of potential candidates to recruit competent, bright, and innovative individuals. Overly specific job descriptions narrow the pool of potential applicants. Job descriptions for cybersecurity positions often appear remarkably similar regardless of the actual job duties and level regarding required certifications, proficiencies, and experience. For example, an entry-level cybersecurity analyst requiring a master’s degree and professional certification (CISSP, CISA, or CISM) is identical to position requirements for many Chief Information Security Officer (CISO) positions.

This situation is confusing for potential applicants and may lead the wrong candidates to apply. By documenting position descriptions more precisely, the pool of potential candidates for vacant positions may widen, especially in regards to entry-level and mid-level jobs. It is important to delineate the required core competencies necessary for the job and other proficiencies possible to acquire on the job, such as vendor applications. Instead of using the traditional skills-based position postings, consider employing a functional strategy that reflects the specific job tasks,<sup>15</sup> such as analyzing data or correlating multiple data sources to identify the root cause of an issue. This tactic may generate more candidates from diverse related fields to apply rather than limiting applicants to individuals that can meet very specific and perhaps limiting requirements.

Siobhan Gorman, director at the Brunswick Group, recommends looking for mid-career professionals with limited specific cybersecurity experience, but a significant applicable background in a related discipline such as project management. While organizations would prefer fully trained and experienced practitioners, even if a quarter of all US college students enrolled and completed cybersecurity programs and entered the workforce, the shortage would not be complete-

<sup>13</sup> Ibid.

<sup>14</sup> International Consortium of Minority Cybersecurity Professionals – <https://icmcp.org/>.

<sup>15</sup> Anderson, K. (2014.) *The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture*, CRC Press.

# 2016

 **ISSA** International  
**CONFERENCE**

## **SURVIVAL STRATEGIES IN A CYBER WORLD**

Hyatt Regency | **NOVEMBER 2-3** | Dallas, Texas

**PREDICT**

**PREPARE**

**PROTECT**

## **2nd Annual Party in the Sky**

**REUNION  
TOWER**

Blue Diamond Sponsor



**WEDNESDAY NIGHT  
6:00-9:00PM**

**CEH Live Exam Prep – Q & A and Testing • ISSA SIGs Sponsored Breakfast • Exhibit Hall Exhibitors' Gala Reception • Breakout Sessions • Prize Drawings in the Exhibit Hall Cyber Defense Center • ISSA Career Central: Secure Your Future • Awards Luncheon**

**REGISTRATION | INFORMATION | [WWW.ISSACONFERENCE.ORG](http://WWW.ISSACONFERENCE.ORG)**

# SURVIVAL STRATEGIES IN A CYBER WORLD

## SURVIVAL STRATEGIES IN A CYBER WORLD

Hyatt Regency | **NOVEMBER 2-3** | Dallas, Texas

**PREDICT**

**PREPARE**

**PROTECT**

## Welcome Cybersecurity Professionals!

**Fellow members and leaders of ISSA and cybersecurity professionals, it is our pleasure to welcome you to the 2016 ISSA International Conference.**

You have all heard the phrase, "Everything Is Bigger in Texas!" At this year's ISSA International Conference, we will prove to you that everything is also BETTER in Texas.

You will enjoy our **2nd Annual Party in the Sky** at Dallas's iconic Reunion Tower, snap a pic at our themed **Selfie Station**, play **Capture the Flag** with fellow attendees, and – new this year – focus on your professional development at **ISSA Career Central: Secure Your Future**.

When planning this year's conference, we reflected back on cybersecurity's biggest obstacles, from high-profile breaches to increasingly sophisticated malware. We must remember that our industry is set in an ever-changing backdrop of technology; we cannot become the cybersecurity leaders of tomorrow using outdated policies, practices, and processes. This is why our interactive educational sessions are specifically designed to arm you with **Survival Strategies in a Cyber World**.

Let's navigate this digital landscape together, and we can tackle even Texas-sized challenges.

Many thanks to the dozens of volunteers and staff who worked tirelessly to present you with an outstanding educational program. Thanks to our passionate speakers for contributing expertise through their thought-provoking sessions. Thanks to our generous sponsors and exhibitors for their support. Last but certainly not least, THANK YOU for joining us at the **2016 ISSA International Conference**.

Dr. Stefano Zanero

Chair, ISSA International Conference

### Keynote Speakers



Wednesday, November 2  
8:15 am – 9:45 am

**Mark Weatherford**

Senior Vice President and  
Chief Cybersecurity Strategist,  
vArmour



Thursday, November 3  
9:00 am – 10:00 am

**Michael Coates**

Chief Information  
Security Officer, Twitter

### Featured Speakers

11/2/2016, 11:45 am - 12:30 pm

**Joel Scambray**

Principal, Cigital

11/2/2016, 1:45 pm - 2:30 pm

**Malcolm Harkins**

Chief Security and Trust Officer, Cylance,  
@ProtectToEnable

11/2/2016, 2:45 pm - 3:30 pm

**Michael Angelo**

Chief Security Architect, Micro Focus |  
NetIQ Corporation

11/2/2016, 4:00 pm - 4:45 pm

**Eric Evenchick**

Director, Linklayer Labs

11/3/2016, 2:30 pm - 3:15 pm

**Deidre Diamond**

Founder and CEO, CyberSN

### ISSA Host Chapters

**Alamo**  
**Capitol of Texas**  
**Fort Worth**  
**North Texas**  
**Oklahoma**  
**South Texas**

## Conference Agenda at a Glance

### Tuesday, November 1, 2016

- 8:00 am – 5:00 pm:** Chapter Leaders Summit\*
- 5:00 pm – 8:00 pm:** Conference Registration Open
- CEH Live Exam Prep -- Q and A and Testing

### Wednesday, November 2, 2016

- 7:00 am – 4:00 pm:** Conference Registration Open
- 7:30 am – 8:15 am:** ISSA SIGs Sponsored Breakfast
- 8:15 am – 9:45 am:** Welcome Remarks and Keynote Address – Mark Weatherford, Senior Vice President and Chief Cybersecurity Strategist, vArmour
- 9:45 am – 4:00 pm:** Exhibit Hall Open (Grand Opening at 9:45am)
- 9:45 am – 4:00 pm:** ISSA Career Central: Secure Your Future
- 11:15 am – 11:45 am:** Coffee Break in the Exhibit Hall
- 12:30 pm – 1:30 pm:** Lunch in Exhibit Hall
- 2:30 pm – 2:45 pm:** Coffee Break in the Exhibit Hall
- 3:30 pm – 4:00 pm:** Coffee Break in the Exhibit Hall
- 4:45 pm – 5:00 pm:** Prize Drawings in the Exhibit Hall
- 5:00 pm – 6:00 pm:** Cyber Defense Center: Diamond Sessions
- 6:00 pm – 9:00 pm:** Party in the Sky and Capture the Flag at Reunion Tower – Blue Diamond Sponsor Armor

### Thursday, November 3, 2016

- 8:00 am – 3:00 pm:** Conference Registration Open
- 8:00 am – 7:00 pm:** Exhibit Hall Open
- 8:00 am – 4:00 pm:** ISSA Career Central: Secure Your Future
- 8:00 am – 9:00 am:** Breakfast in Exhibit Hall
- 9:00 am – 10:00 am:** Keynote Address – Michael Coates, CISO, Twitter
- 11:00 am – 11:30 am:** Coffee Break in the Exhibit Hall
- 12:15 pm – 2:00 pm:** Awards Luncheon
- 3:15 pm – 3:30 pm:** Coffee Break in the Exhibit Hall
- 4:30 pm – 5:30 pm:** Cyber Defense Center: Diamond Sessions
- 5:30 pm – 7:00 pm:** Exhibitors' Gala Reception
- 7:30 pm – 8:30 pm:** CISO Forum Opening Dinner\*\*

### Friday, November 4, 2016

- 8:00 am – 5:00 pm:** CISO Executive Forum\*\*

### Saturday, November 5, 2016

- CEH Live Exam Prep -- Q & A and Testing

\*The [Chapter Leaders Summit](#) is open to all chapter officers and board members of record at the time of registration. Please RSVP online. If you have questions please contact [chapter@issa.org](mailto:chapter@issa.org). Requires separate registration.

\*\*[CISO Forum](#) is open to members of the CISO Executive Program and qualified first-time guests. Requires separate registration.

## #ISSAConf - Let's Get Social!

### Social Media Fast Tips

- On Facebook, "Like" the ISSA International page, post photo to page, and tag it using #ISSAConf
- On Twitter, tag @ISSAINTL and include #ISSAConf
- On Instagram, tag @ISSAINTL and include the hashtag #ISSAConf
- Any photos tagged using #ISSAConf may be shared in the moment of repurposed in the future by ISSA International

### Social Media messages to adapt and share!

- Having a great time in Dallas at #ISSAConf! Off to [speaker name]'s session on [session topic]
- #ISSAConf is going BIG in Dallas this year! I met some cool sponsors including [sponsor name] at the exhibit hall [make sure to include a pic!]
- Howdy, fellow #ISSAConf attendees! Happy to connect with each other social media - send me a tweet @[insert Twitter handle]

#### Use #ISSAConf on Facebook

- "Like" the ISSA International page, if you haven't done so already
- Use #ISSAConf

#### Share #ISSAConf on Twitter

- To insert a photo, click the camera icon in the composition screen
- Compose your 140-character tweet, and include #ISSAConf and @ISSAINTL

#### Share #ISSAConf on Instagram

- Take a picture or short video
- Write a post and be sure to include #ISSAConf and @ISSAINTL
- Auto-share to Facebook and Twitter, if all three accounts are connected

#### Share on LinkedIn

- Join our discussion group: [www.linkedin.com/groups/48091](http://www.linkedin.com/groups/48091)
- Share an update with your contacts to let them know you're at the ISSA International Conference

**Each social media post using the hashtag #ISSAConf will give you one entry into our prize drawing!**

## Interested in Writing for the ISSA Journal?

Thom Barrie, Journal Editor, will be at the Journal booth and wandering the halls...Stop by and he'll set you up with what you need.

 ISSA JOURNAL

Thom Barrie,  
ISSA Journal Editor



## Special Events

**Tuesday, November 1**

### Chapter Leaders Summit: 8:00 am – 3:00 pm, Cumberland B/C

Whether you are a new or long-time chapter board member, this one-day summit is a must. The Chapter Leaders Summit is designed to provide you with leadership tactics to support, strengthen, and further develop your chapter and enhance member value. How can you make it easy for members to get the most out of their membership?

\*\*The [Chapter Leaders Summit](#) is open to all chapter officers and board members of record at the time of registration. Requires separate registration.

**Wednesday, November 2**

### ISSA SIGs Sponsored Breakfast: 7:30 am – 8:15 am

Network with ISSA International members, recognize star SIG leaders from 2016, and participate in interactive sessions to help us better understand what each of you needs to thrive in your chosen SIG communities. Tell us how to increase value in our four SIGs: Finance, Health Care, Security Awareness, and Women in Security. We will also gather your ideas and share what the SIGs are planning for 2017 and beyond. Join us to have your voice heard and your perspective valued.

### Party in the Sky at the Reunion Tower, Dallas BLUE DIAMOND SPONSOR

**6:00 pm – 9:00 pm**

Iconic, futuristic, and colorful, Reunion Tower is easily the most recognizable building in the Dallas skyline. At 561 feet, this landmark brightens the Dallas horizon and offers its guests spectacular 360-degree views of the city. Join ISSA at our International Conference November 2-3 to be a part of our incredible event.

**Thursday, November 3**

### International Awards Luncheon: 12:15 pm – 2:00 pm

The International Awards Luncheon will be held in Landmark B/C is open to all attendees. Join the Who's Who of the information security community and toast the influential leaders who have demonstrated a superior level of expertise, effectiveness, and dedication to the advancement of the profession.

#### 2015 Award Winners:

##### Hall of Fame

Gerald Combs  
Jim Reavis

##### Honor Roll

Richard Greenberg  
Joel Weise

##### Volunteer of the Year

Constance Matthews  
Colleen Murphy

##### Chapter of the Year

Small: Minnesota Chapter  
Large: Capitol of Texas Chapter

##### Security Professional of the Year

Albert Marcella

##### President's Award for Public Service

Howard Schmidt

##### Organization of the Year

OWASP

### ISSA Exhibitors' Gala Reception: 5:00 pm – 7:30 pm

All attendees are welcome to join us in the Exhibit Hall at this informal networking reception in Marsalis Hall A.

**Thursday, November 3 (Evening – Dinner) & Friday, November 4 (All-day workshops)**

### CISO Forum Opening Dinner: Thursday 7:30 pm – 8:30 pm

### CISO Forum Program: Friday 8:00 am – 5:00 pm

[CISO Forum](#) is open to members of the CISO Executive Program and qualified first-time guests. Requires separate registration.

## ISSA Career Central: Secure Your Future

For years, ISSA has been the go-to resource for information security professionals looking to advance their career. For years, ISSA has provided its members with webinars, networking events, educational programs, and a career center with over 1,000 job postings. For years, members have called us their cybersecurity "home."

ISSA is always looking for ways to demonstrate its dedication to YOU, the information security professional looking for career advance-

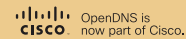
ment. So at this year's International Conference in Dallas, we would like to present to you ISSA Career Central: Secure Your Future.

**Attendees, you can:** Meet recruiters and speak with them in a private setting; receive feedback on your resumes; and complete mock interviews.

**Employers:** Are you currently recruiting? Stop by and let us know about your job openings!

## Cyber Defense Center

From 5:00 pm to 6:00 pm Wednesday and 4:30 pm to 5:30 pm Thursday, attend special product demonstrations, receptions, prize drawings and more in the ISSA Cyber Defense Center.



When you analyze  
**70 BILLION DNS  
QUERIES A DAY**

you see what other  
security solutions miss.

**Stop by Booth #401**

Pivot through attackers' infrastructure and  
predict where future attacks are staged.

**TAKE IT TO THE CLOUD**  
**SECURITY BEYOND THE FIREWALL**

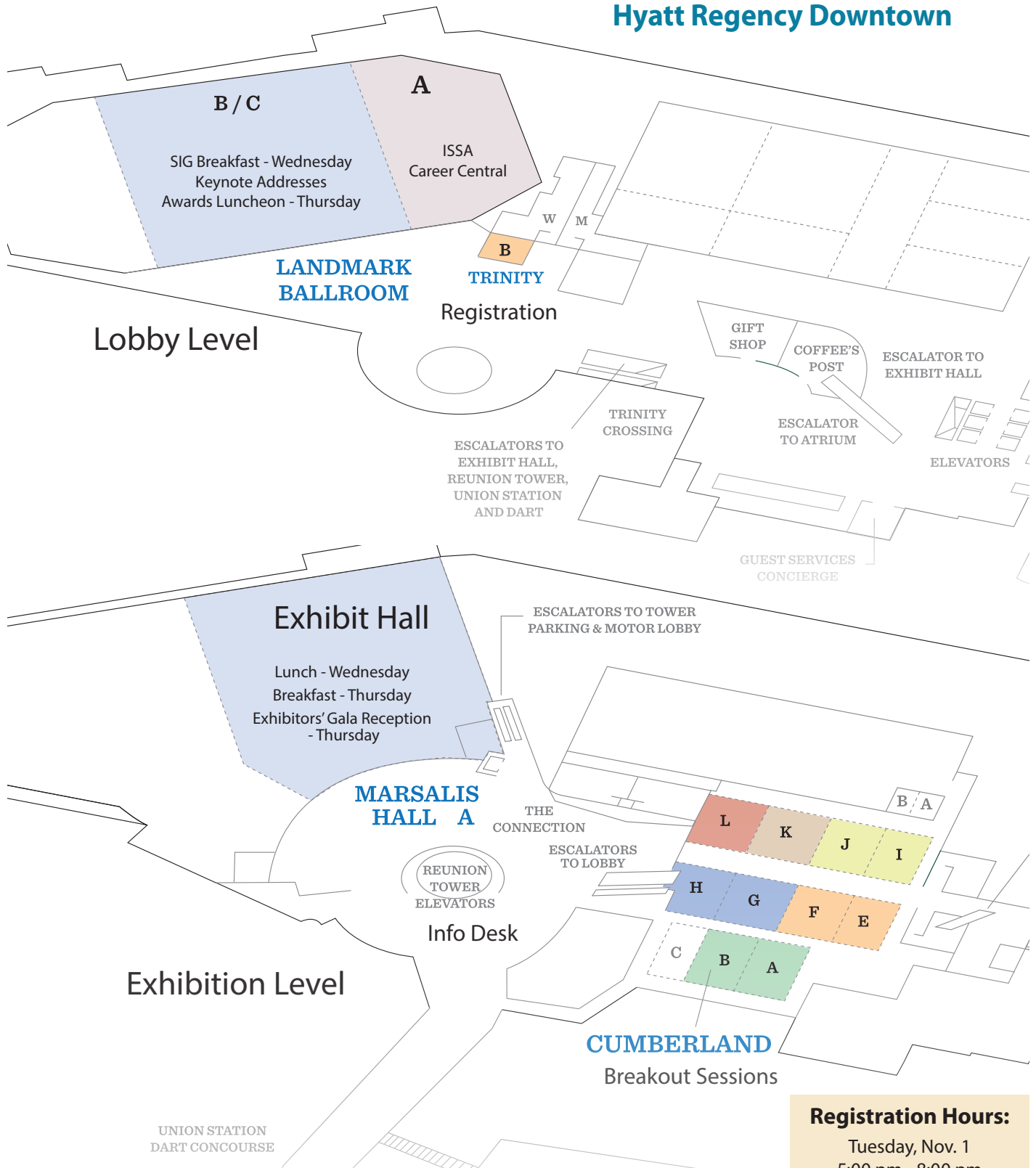
**OpenDNS**



OpenDNS is  
now part of Cisco.

# SURVIVAL STRATEGIES IN A CYBER WORLD

## Hyatt Regency Downtown



### Registration Hours:

Tuesday, Nov. 1  
5:00 pm - 8:00 pm  
Wednesday, Nov. 2  
7:00 am - 4:00 pm  
Thursday, Nov. 3  
8:00 am - 3:00 pm

### Photo & Video Disclaimer

By attending the ISSA International Conference, you will be entering an area where photography, video, and audio recording may occur. By attending, you consent to photography, audio recording, video recording, and its/their release, publication, exhibition, or reproduction to be used for news, webcasts, promotional purposes, telecasts, advertising, inclusion on websites, or any other purpose by ISSA and its affiliates and representatives. You release ISSA, its officers and employees, and each and all persons involved from any liability connected with the taking, recording, digitizing, or publication of interviews, photographs, computer images, video and/or sound recording.



# Be Sure to Visit All Our Solution Providers in the Exhibit Hall

Wednesday, November 2: 9:45 am – 4:00 pm  
 Thursday, November 3: 8:00 am – 7:00 pm

109	209	309	409	509	609	709
108	208	308	408	508	608	708
107	207	307	407	507	607	707
106	206	306	406	506	606	706
105						
104	204	304	404	504	604	704
103	203	303	403	503	603	703
102	202	302	402	502	602	702
101	201	301	401	501	601	701

Sponsors/Exhibitors	Booth #
Armor [Blue Diamond].....	404/504
Carbon Black & Vectra Networks [Diamond].....	204/304
OpenDNS, now part of CISCO [Diamond].....	401/501
Tanium [Diamond]	
Centrify Corporation [Platinum].....	606/706
CloudPassage [Platinum].....	201/301
Darktrace [Platinum].....	206/306
MediaPro [Platinum].....	601/701
Vormetric – A Thales Company [Platinum].....	506
Bomgar [Gold].....	406
Coalfire [Gold].....	105
CyberArk Software, Inc. [Gold].....	703
Cylance [Gold].....	502
NRI SecureTechnologies Ltd. [Gold].....	508
Zscaler, Inc. [Gold].....	302
AccessData [Silver].....	503
Anitian Corporation [Silver].....	403
BeyondTrust GCA Technology Services [Silver].....	603
Clearswift [Silver].....	607
CYBERBIT [Silver].....	303
Forum Systems [Silver].....	101
NCC Group Security Services, Inc. [Silver].....	507
Qualys, Inc. [Silver].....	402
Swivel Secure, Inc. [Silver].....	602
Tremolo Security, Inc. [Silver].....	707
Above Security – A Hitachi Group Company [Exhibitor].....	207
BluVector [Exhibitor].....	TBD
Checkmarx [Exhibitor].....	202
Department of Homeland Security [Exhibitor].....	TBD
Future Com, Ltd. [Exhibitor].....	407
Gigamon, Inc. [Exhibitor].....	308
HPE Security – Data Security [Exhibitor].....	608
InfoArmor [Exhibitor].....	708
LightCyber [Exhibitor].....	203
Minerva Labs [Exhibitor].....	408
Nyotron [Exhibitor].....	208
OPSWAT [Exhibitor].....	TBD
SANS [Exhibitor].....	TBD
Seclore [Exhibitor].....	307
The Security Awareness Company [Exhibitor].....	TBD
Synack [Exhibitor].....	TBD
SpiderOak [Exhibitor].....	TBD
VERODIN [Exhibitor].....	TBD
Workplace Answers [Exhibitor].....	TBD

## Blue Diamond Sponsor



## Diamond Sponsors



## Platinum Sponsors



## Gold Sponsors



## Silver Sponsors



# SURVIVAL STRATEGIES IN A CYBER WORLD

## ISSA Conference Tracks:

- Application Security:** Application Security, Security Development Life Cycle
- Business Skills for the Information Security Professional:** The business case for Information Security, Career Paths for Infosec Professionals, Privacy
- Incident Response**
- Securing the End User:** Security Awareness Training, Social Media, Access Control
- Infrastructure:** Endpoint Security, Network Security, Data Loss Prevention, Pen/Vulnerability Testing, Security Intelligence, Data Protection, Architecture
- Laws and Regulations:** Legal Updates, GRC, Standards

## Wednesday, November 2

**International Conference Registration Open:** 11/2/2016, 7:00 am – 4:00 pm, Trinity B

**ISSA SIGs Sponsored Breakfast:** 11/2/2016, 7:30 am – 8:15 am, Landmark B/C

### Opening Keynote Address – Mark Weatherford To the Cloud: Ready or Not!

11/2/16, 8:15 am - 9:45 am, Landmark B/C

**Exhibit Hall Grand Opening:** 11/2/2016, 9:45 am – 10:30 am, Marsalis Hall A

**Book Signing with Peter McLaughlin:** 11/2/16, 9:45 am – 10:30 am, Landmark A

**ISSA Career Central – Secure Your Future:** 11/2/2016, 9:45 am – 4:00 pm, Landmark A

### Breakout Session One: 11/2/2016, 10:30 am - 11:15 am

Application Security	Business Skills	Incident Response	Infrastructure	Laws & Regulations	Securing the End User
<b>Cyber Security and the Need for a Root of Trust</b> Cumberland G/H	<b>“Architecting” Your Cybersecurity Organization for Big Data, Mobile, Cloud, and Digital Innovation</b> Cumberland I/J	<i>Sponsored Session</i> <b>Self-Learning Defense – Identifying Early-Stage Threats with an Enterprise Immune System</b> Cumberland A/B  <b>Cyber Fraud Hunt Operations-Case Study Analysis</b> Cumberland K	<b>Champagne Protection on a Beer Budget</b> Cumberland L	<b>Business Email Compromise – Your Company’s Greatest Uninsured Financial Risk</b> Cumberland E/F	

**Break in the Exhibit Hall:** 11/2/2016, 11:15 am – 11:45 am, Marsalis Hall A

### Breakout Session Two: 11/2/2016, 11:45 am - 12:30 pm

Application Security	Business Skills	Incident Response	Infrastructure	Laws & Regulations	Securing the End User
<i>Featured Speaker</i> <b>App Sec: Start, Scale, Sustain</b> Landmark B/C  <b>Game of Hacks – Play, Hack, and Track</b> Cumberland G/H	<b>Privacy Attitude of Security Leaders Who Survive the Cyber World</b> Cumberland I/J	<i>Sponsored Session</i> <b>Tracking Down the Cyber Criminals: Revealing Malicious Infrastructure</b> Cumberland A/B  <b>Improving Incident Response Plan with Advanced Exercises</b> Cumberland K			<b>Forging Your Identity: Credibility Beyond Words</b> Cumberland L



### DOWNLOAD THE MOBILE APP

**Search:**  
ISSA International Conference

Accessible through smart phone, tablet, or computer




### WELCOME TO THE 2016 ISSA INTERNATIONAL CONFERENCE APP:

*Use this app to enhance your conference experience:*

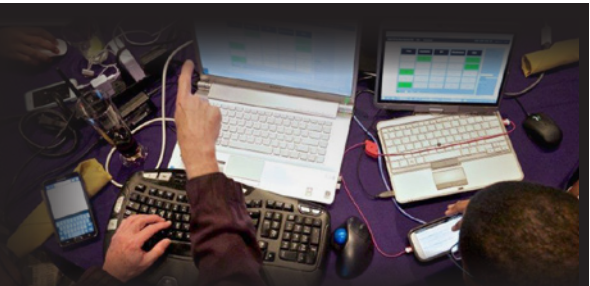
- Meet and network with other conference participants
- Build your personal schedule
- Schedule meetings with attendees, exhibitors, and career counselors
- View speaker abstracts
- Take notes on sessions, speakers, sponsors, and exhibitors
- Stay informed with the latest event happenings
- And more!

Session Information Follows the Session Grids

# Play Capture the Flag at the Party in the Sky

Capture the Flag helps to spread security techniques, measure security skill, and strengthen technical and management skills in a fun and competitive atmosphere!

Sign up here: [www.issa.org/page/CTF2016](http://www.issa.org/page/CTF2016)



Capturing the flag at the 2014 International Conference.

**Lunch in the Exhibit Hall:** 11/2/2016, 12:30 pm – 1:30 pm, Marsalis Hall A

**Book Signing with Malcolm Harkins:** 11/2/16, 12:30 pm – 1:30 pm, Cylance Booth

## Breakout Session Three: 11/2/2016, 1:45 pm - 2:30 pm

Application Security	Business Skills	Incident Response	Infrastructure	Laws & Regulations	Securing the End User
<b>Sponsored Session</b> <b>The Eight Imperatives for Agile and Scalable Cloud Security</b> Cumberland A/B  <b>A Practitioner's Guide to a Secure Agile Transition</b> Cumberland G/H	<b>Featured Speakers</b> <b>Protect to Enable</b> Landmark B/C	<b>The CISO's Guide to Incident Response</b> Cumberland K	<b>The Architecture of a Secure IoT Gateway: A Technical Deep Dive</b> Cumberland L	<b>Cyber Law Update</b> Cumberland E/F	

## Breakout Session Four: 2:45 pm – 3:30 pm

Application Security	Business Skills	Incident Response	Infrastructure	Laws & Regulations	Securing the End User
<b>Sponsored Session</b> <b>Protecting Sensitive Data in the Cloud</b> Cumberland A/B	<b>CISO Success Strategies: On Becoming a Security Business Leader</b> Cumberland L  <b>Propel Your Career with Personal Strategic Planning</b> Cumberland I/J	<b>Featured Speaker</b> <b>Posture Makes Perfect – Cyber Residual Risk Scoring</b> Landmark B/C		<b>Digital Investigations: Leveraging the Multitude of Records</b> Cumberland K	<b>ISSA Healthcare SIG Sponsored Session</b> <b>Ransomware &amp; Health Information Exchanges - Is Your Data Safe?</b> Cumberland E/F  <b>The Man Behind the Curtain: Revealing the Truth of Overhyped Security Solutions</b> Cumberland G/H

**Break in the Exhibit Hall:** 11/2/2016, 3:30 pm – 4:00 pm, Marsalis Hall A

## Breakout Session Five: 11/2/2016, 4:00 pm - 4:45 pm

Application Security	Business Skills	Incident Response	Infrastructure	Laws & Regulations	Securing the End User
<b>Featured Speaker</b> <b>Automotive Security: Challenges and Perspectives</b> Landmark B/C  <b>Prevent Ransomware with the Right Architecture</b> Cumberland K  <b>Modernize Your Security for Critical Applications</b> Cumberland G/H	<b>Building a Mature Cyber Intelligence Program</b> Cumberland I/J	<b>Sponsored Panel</b> <b>How Effective are Incident Response Plans?</b> Cumberland A/B		<b>Integrating Business Case Skills into GRC Regulatory Compliance Initiatives</b> Cumberland L	<b>Protecting Data Everywhere it is Used, Shared, and Stored</b> Cumberland E/F

**Prize Drawings in the Exhibit Hall:** 11/2/2016, 4:45 pm – 5:00 pm, Marsalis Hall A

**Cyber Defense Center – Diamond Sessions:** 11/2/2016, 5-6 pm



**Party in the Sky at Reunion Tower:** 11/2/2016: 6:00 pm – 9:00 pm



# SURVIVAL STRATEGIES IN A CYBER WORLD

## Thursday, November 3

**International Conference Registration Open:** 11/3/2016, 8:00 am – 3:00 pm, Trinity B

**Breakfast in the Exhibit Hall:** 11/3/2016, 8:00 am – 9:00 am, Marsalis Hall A

**Booking Signing with Peter McLaughlin:** 11/3/16, 8:00 am – 9:00 am, Landmark A

**ISSA Career Central – Secure Your Future:** 11/3/2016, 8:00 am – 4:00 pm, Landmark A

**Exhibit Hall Open:** 11/3/2016, 8:00 am – 7:00 pm, Marsalis Hall A

**Keynote Address – Michael Coates**  
**Building a Security Program that Succeeds – Scale, Efficacy and Executive Support**  
 11/3/2016, 9:00 am – 10:00 am, Landmark B/C

### Breakout Session Six: 11/3/2016, 10:15 am - 11:00 am

Application Security	Business Skills	Incident Response	Infrastructure	Laws & Regulations	Securing the End User
<b>Artificial Intelligence: The Foundation for a Secure Cyber Future</b> Cumberland G/H	<b>Advances in Security Risk Assessment</b> Cumberland I/J  <b>Cyber Security Professional Career Study Findings</b> Cumberland E/F	<b>The Visible Attack Surface – What It Is and Why It Matters</b> Cumberland K			<b>Sponsored Sessions</b> <b>Best Practices from the World's Top Security Awareness Programs</b> Cumberland A/B  <b>Balancing Mobile Security with Privacy: A Prescription for Closing the Trust Gap</b> Cumberland L

**Break in the Exhibit Hall:** 11/3/2016, 11:00 am – 11:30 am, Marsalis Hall A

### Breakout Session Seven: 11/3/2016, 11:30 am - 12:15 pm

Application Security	Business Skills	Incident Response	Infrastructure	Laws & Regulations	Securing the End User
	<b>Sponsored Panel</b> <b>Culture Changes, Communicating Cyber Risk in Business Terms</b> Cumberland A/B  <b>Scraping Together a Security Program</b> Cumberland I/J	<b>Digital Forensics – First Responders &amp; Incident Management</b> Cumberland K	<b>Transform from Surviving to Thriving by Preparing for the Next Wave of Cyber-Attacks and Information Borne Threats</b> Cumberland L		<b>Secure User Application Access in a Hurry</b> Cumberland G/H




**ISSA International Awards Luncheon:** 11/3/2016, 12:15 pm – 2:00 pm, Landmark B/C

### Breakout Session Eight: 11/3/2016, 2:30 pm - 3:15 pm

Application Security	Business Skills	Incident Response	Infrastructure	Laws & Regulations	Securing the End User
<b>Sponsored Session</b> <b>What Happens in the Cloud Stays in the Cloud: Data Protection of Public Cloud Storage</b> Cumberland G/H	<b>Featured Speaker</b> <b>Weaponizing Your Words For Talent Retention</b> Landmark B/C  <b>The 100-Minute MBA for Information Security Professionals [2-part workshop]</b> Cumberland I/J  <b>ISSA WIS SIG Sponsored Session</b> <b>Get the Right People in the Right Places to Maximize Your Cyber Team Performance [2-part workshop]</b> Cumberland E/F	<b>Best Practices for Responding to a Cyberattack and Working with Law Enforcement in the Aftermath</b> Cumberland K	<b>Is Your Vulnerability Management Program Evolving? Introducing the Vulnerability Management Maturity Model – VM3</b> Cumberland L		<b>Sponsored Session</b> <b>Stepwise Security – A Planned Path to Reducing Risk</b> Cumberland A/B

**Book Signing with Malcolm Harkins:** 11/3/16, 2:30 pm -3:30 pm, Landmark A

**Breakout Session Nine: 11/3/2016, 3:30 pm - 4:15 pm**

Application Security	Business Skills	Incident Response	Infrastructure	Laws & Regulations	Securing the End User
	<b>Featured Speaker</b> <b>Mr. Robot – Can it Really Happen?</b> Landmark B/C	<b>Business Continuity and Cyber Security – Partners in Crime (Cyber)</b> Cumberland K	<b>Compliance in the Cloud</b> Cumberland L		
<b>Cyber Defense Center – Diamond Sessions: 11/3/2016, 4:30 pm – 5:30 pm</b>			   		
<b>Exhibitor's Gala Reception: 11/3/2016: 5:30 pm – 7:00 pm, Marsalis Hall A</b>					

## Session Descriptions

### Wednesday, November 2

#### Wednesday Keynote Address: 8:15 am - 9:45 am



#### To the Cloud: Ready or not!

*Mark Weatherford: Senior Vice President and Chief Cybersecurity Strategist, vArmour*  
**Landmark B/C**

As the global cyber threat environment continues to evolve, organizations need to begin thinking differently about information security and the protection of their infrastructure. The evolution from perimeter-centric, hardware-based environments to virtualized data centers and the

cloud is underway and many organizations are late to the game. As CIOs and CISOs are driven to transition their CapEx investments to OpEx spending, the economic efficiencies of the cloud provide a rational path to those goals. From a security perspective, however, security models that don't sufficiently address workload and application-aware segmentation, lateral traffic visibility, and network-based threat detection of on-premises data center and public cloud-based

environments leave a huge gap in the overall security posture. This talk will provide CIOs and CISOs struggling with decisions about migration to the cloud with some thoughts about how the cloud can be the catalyst that improves security while also reducing costs and technology footprint.

#### Breakout Session One: 10:30 am - 11:15 am

##### Sponsored Session

#### Self-Learning Defense – Identifying Early-Stage Threats with an Enterprise Immune System



*Molly Slocum: Cybersecurity Account Executive, Darktrace*

##### Incident Response

11/2/2016, 10:30 am – 11:15 am

**Cumberland A/B**



Unsupervised Machine Learning: A New Approach to Cyber Defense


From insiders to sophisticated external attackers, the reality of cybersecurity today is that the threat is already inside. Legacy approaches to cybersecurity, which rely on knowledge of past attacks, are simply not sufficient to combat new, evolving attacks, and no human cyber analyst can watch so much or react quickly enough. A fundamentally new approach to cyber defense is needed to detect and investigate these threats that are already inside the network—before they turn into a full-blown crisis. Self-learning systems represent a fundamental step-change in automated cyber defense, are relied upon by organizations around the world, and can cover up to millions of devices. Based on unsupervised machine learning and probabilistic mathematics, these new approaches to security can establish a highly accurate understanding of normal behavior by learning an organization's "pattern of life." They can therefore spot abnormal activity as it emerges and even take precise, measured actions to automatically curb the threat. Discover why unsupervised machine learning is the future of defense and how the "immune system" approach to cybersecurity provides complete network visibility and the ability to prioritize threats in order to better allocate time and resources.


In this session, learn:


- How new machine learning and mathematics are automating advanced cyber defense
- Why full network visibility allows you to detect threats as or before they emerge
- How smart prioritization and visualization of threats allows for better resource allocation and lower risk
- Real-world examples of unknown threats detected by "immune system" technology


### Cyber Security Career Lifecycle® Levels

*Note: if the session fits multiple levels, the lower and higher levels will be displayed.*

 **PRE-PROFESSIONAL:** any individual who has not yet obtained a position working in the cybersecurity field. This may include anyone who has interest in working in this area with or without formal training and education in the field. Examples of who may be part of this phase are those who are switching careers (former military, IT, retail, law enforcement, etc.), and students (high school or university).

 **ENTRY LEVEL:** An individual who has yet to master general cybersecurity methodologies/principles. Individuals in this phase of the life cycle may have job titles such as associate cybersecurity analyst, associate network security analyst, or cybersecurity risk analyst, for example.

 **MID-CAREER:** An individual who has mastered general security methodologies/principles and has determined area of focus or specialty. Individuals in this phase of the life cycle may have job titles such as network security analyst, cybersecurity forensics analyst, application security engineer, and network security engineer. Individuals who are nearing the "senior level" may begin to hold job titles such as senior network security engineer or senior cybersecurity analyst, for example.

 **SENIOR LEVEL:** An individual who has extensive experience in cybersecurity and has been in the profession for 10+ years. These individuals have job titles such as senior cybersecurity risk analysis, principal application security engineer, or director of cybersecurity, etc.

 **SECURITY LEADER:** An individual who has extensive security experience, ability to direct and integrate security into an organization. These individuals have job titles such as Chief Information Security Officer, Chief Cybersecurity Architect, etc. After extensive periods of leadership, some become recognized industry leaders.

# SURVIVAL STRATEGIES IN A CYBER WORLD

## **Cybersecurity and the Need for a Root of Trust**



*Juan Asenjo: Director of Cryptographic Integrations for Partner Solutions, Thales e-Security, Inc., @asenjoJuan*

### **Application Security**

11/2/2016, 10:30 am - 11:15 am  
**Cumberland G/H**

Cybersecurity strategies increasingly use cryptographic applications to ensure the protection of critical data and other sensitive resources. As organizations deploy more devices and sensors connected to enterprise networks and to the Internet, their identification, authentication, and the integrity of the code they run become critically important. Counterfeit devices and devices running malware can pose significant cybersecurity risks with potentially catastrophic consequences. Since cryptography is only as good as the level of protection afforded to the cryptographic keys, a robust root of trust using an isolated hardware security modules (HSMs) is recommended to safeguard and manage underpinning application keys, including those used for device identity management and code signing.

## **"Architecting" Your Cybersecurity Organization for Big Data, Mobile, Cloud, and Digital Innovation**



*David Foote: Chief Analyst and Chief Research Officer, Foote Partners, LLC*

### **Business Skills**

11/2/2016, 10:30 am - 11:15 am  
**Cumberland I/J**

The role technology as an engine of enterprise, innovation, and competitiveness has caught many IT leaders unprepared: for years they've been slow to address persistent human capital problems such as tech skill deficits, hiring/retention issues, pay inequalities, and murky career paths. This is hitting cyber/info security organizations particularly hard as cybersecurity threats continue to stun the industry regularly and as Big Data, Cloud, Mobile, and Digital Innovation popularity explodes. Bottom line is the pressure to fix longstanding "people problems" associated with securing the enterprise has never been greater. Coming to the rescue: applying traditional architecture practices to cyber/info security human capital and workforce management. Known as "People Architecture," it is proving to be the most effective solution for executing mission-critical IT-business initiatives such as cyber/info security effectively and predictably. In this session, industry analyst David Foote will define the pillars of people architecture for security, describe people architecture components, and reveal who's doing it and how they're doing it.

## **Business Email Compromise – Your Company's Greatest Uninsured Financial Risk**



*Dr. Christopher Pierson: CSO and General Counsel, Viewpost, @DrChrisPierson*

*James T. Shreve: Attorney, BuckleySandler, LLP*

### **Laws and Regulations**

11/2/2016, 10:30 am - 11:15 am  
**Cumberland E/F**



Every day business finance or HR professionals are duped into sending money or spreadsheets containing SSNs and other PII to cyber thieves. Fraudsters bypass all the security devices, firewalls, perimeter defenses, and even APT defenses and merely ask the people with

the keys to the kingdom to hand over the goods . . . and they do so. Employees miss the fact the email is not from the CEO or CFO and the display name says the right name, but the email address does not! This presentation will focus on the social hack of BEC (Business Email Compromise/CEO Fraud) Fraud focusing on several areas: (1) how this attack happens, (2) controls to implement to reduce the effectiveness of these attacks, (3) how to train your employees, and (4) the legal aspects of whether or not you are protected and can get your money back.

We will spend time discussing the case law on BEC cases, the role that insurance does or does not play, tactics to mitigate this harm, controls you can request from your bank, and how to shift some of this burden to others. BEC Fraud is on the rise and you will not want to miss this security and legal talk!

## **Cyber Fraud Hunt Operations-Case Study Analysis**



*Jarrett W. Kolthoff: President & CEO, SpearTip LLC, @SpearTipCyberCI*

### **Incident Response**

11/2/2016, 10:30 am - 11:15 am  
**Cumberland K**

The audience will be exposed to host-based and network incident response/digital forensics tactics utilized during several cases outlined during the presentation. The presentation will discuss the process of collecting and analyzing several disparate evidentiary elements within a Fusion Cell methodology that the audience can utilize at their own corporation. Leveraging these critical lessons learned from real-world case studies can be the key element that helps build a more successful defensive strategy.

## **Champagne Protection on a Beer Budget**



*Justin Bumpus: Information Security Manager, Ozburn-Hessey Logistics, @justinbumpus*

### **Infrastructure**

11/2/2016, 10:30 am - 11:15 am  
**Cumberland L**

Are you getting the most out of your information security dollar? Find out how to protect an enterprise while dealing with budget constraints with a little out-of-the-box thinking, charm, and FUD. If all else fails this talk finishes with best practices for career development and temper tantrum throwing in today's business environment.

## **Breakout Session Two: 11:45 am - 12:30 pm**

### **Featured Speaker**

## **App Sec: Start, Scale, Sustain**



*Joel Scambray: Principal, Cigital, @joelscam*

### **Application Security**

11/2/2016, 11:45 am - 12:30 pm  
**Landmark B/C**

New research into application security practices at over 75 companies will be discussed, covering software security strategies and tactics as they are practiced "in the wild." Statistics will be balanced with case studies from the field to illustrate foundational principles of starting, scaling, and sustaining programs, as well as "what not to do" gotchas that can kill an initiative in its tracks.

### **Sponsored Session**

## **Tracking Down the Cyber Criminals: Revealing Malicious Infrastructure**



*Mark Stanford: Systems Engineering Manager, OpenDNS, now part of Cisco*

### **Incident Response**

11/2/2016, 11:45am - 12:30pm  
**Cumberland A/B**



Cyber Criminals are increasingly exploiting the Internet to build agile and resilient infrastructures, and consequently to protect themselves from being exposed and taken over. The Internet is an open system, meaning that the information to expose those infrastructures is available somewhere. The challenge is that fragments of data broken up and spread across the web are not immediately visible. Connecting the dots, being able to analyze a diverse set of information made of billions of pieces of discrete data allows one to build the maps that



# 15-Second Visibility & Control Over Every Endpoint. Even Across the Largest Networks.

Impossible? Think again.

**ASK**

your question in plain English.



**KNOW**

what is happening right now across all of your endpoints  
(even the ones you didn't know about).



**ACT**

Change all impacted endpoints as needed.



Learn more at [www.tanium.com](http://www.tanium.com)

# SURVIVAL STRATEGIES IN A CYBER WORLD

reveal where the malicious infrastructure is hidden and where the attacks are staged. This turns the table of traditional security with a new approach where the defender takes the upper hand on the attacker, being able to pivot through the criminal infrastructure.

## **Game of Hacks – Play, Hack, and Track**



*Itai Heller: Senior Sales Engineer, Checkmarx*

### **Application Security**

11/2/2016, 11:45 am - 12:30 pm

**Cumberland G/H**

We created “Game of Hacks”—a viral web app marketed as a tool to train developers on secure coding—with the intention of building a honeypot. Game of Hacks, built using the node.js framework, displays a range of vulnerable code snippets, challenging the player to locate the vulnerability. A multiplayer option makes the challenge even more attractive and the leaderboard spices up things when players compete for a seat on the iron throne. Within 24 hours we had 35K players test their hacking skills...we weren’t surprised when users started breaking the rules. Join us to:

- Play GoH against the audience in real time and get your claim to fame.
- Understand how vulnerabilities were planted within Game of Hacks.
- See real attack techniques (some caught us off guard) and how we handled them.
- Learn how to avoid vulnerabilities in your code and how to go about designing a secure application.
- Hear what to watch out for on the ultra-popular node.js framework.

## **Privacy Attitude of Security Leaders Who Survive the Cyber World**



*Grace Buckler: Global Privacy Consultant, The Privacy Advocate, LLC, @grace4privacy*

### **Business Skills**

11/2/2016, 11:45 am - 12:30 pm

**Cumberland I/J**

Since there is no industry certification for a positive, well-informed survival attitude, nobody demands, requires, or regulates it. But attitude has an effect on how well you are able to put a successful privacy program in place and survive the cyber world.

Is your attitude fit? The right attitude with sound strategies will propel you through today’s less structured and non-traditional data protection measures. Having the wrong attitude can get you much closer to experiencing a devastating data breach today than you were before.

Consumer data is the new critical asset that you must preserve with all you’ve got or can get. You need privacy in your cybersecurity strategies. And it takes the right attitude and diligence to do it successfully. Security and privacy require distinct tools and attitudes to accomplish a corporate mandate of data protection. Studies show the average cost of data breach on a global scale is \$3.6 million. Consider your stakes, such as \$500+ in incident expenses per record exposed, negative news media attention, public mistrust, loss of customers, liabilities, hours in court, and more. A data breach is inevitable. But how fast can your attitude help you fight back and bounce back with little financial damage? And save face? Master the attitude that will make the difference between a successful privacy implementation and a helpless scramble to survive a major attack.

## **Improving Incident Response Plan with Advanced Exercises**



*Stephanie Ewing-Ottmers: Cyber Exercise Consultant, Delta Risk LLC*

*Chris Evans: Vice President for Advanced Cyber Defense, Delta Risk LLC*

### **Incident Response**

11/2/2016, 11:45 am - 12:30 pm

**Cumberland K**



How mature is your cybersecurity exercise program? Are you evolving or checking the box? Cybersecurity exercises present a plausible, relevant, and high-impact scenario and offer opportunities to drill processes,

evaluate personnel effectiveness, and observe gaps in people, processes, and technology in response to that scenario. This session discusses how cyber exercises can be matured into integrated, multi-year strategic programs, leveraging different types of cybersecurity exercises, as evolved from the HSEEP (Homeland Security Exercise and Evaluation Program) framework. Advanced concepts, addressing evolving threats and topics of scenario design, planning, execution, and the differences that make cybersecurity exercises relevant will be highlighted. Leveraging the latest techniques based on proven frameworks, a strategic cybersecurity exercise program can provide realistic opportunities to train the way we need to defend and allow people, processes, and technology to train together and be evaluated jointly rather than individually. Participants will discuss how to create an organic exercise program capability through capacity building, with emphasis on exercise capability as a central component of a broader cybersecurity preparedness program. Several case studies from both government and the commercial sector highlighting the benefits and key observations from cyber exercises are provided, adding a tangible outcome dimension to the session.

## **Forging Your Identity: Credibility Beyond Words**



*Tim Roberts: Security Consultant, Solutionary, Inc., @ZanshinH4X*

*Brent White: Security Consultant, Solutionary, Inc., @brentwdesign*

### **Securing the End User**

11/2/2016, 11:45 am - 12:30 pm

**Cumberland L**



Pretending to be an employee is one thing, but owning layers of identities is what has led to owning the data centers, PBX rooms, Security Control Centers, and more. If a discerning employee is not buying into your

backstory, your credibility can sometimes make or break an assessment. In this presentation, we will discuss how to help add that credibility through document and badge forgery, setting up and forwarding local phone numbers, fake employee web search results, and other tactics. You will listen to real-world scenarios that led to an armed security guard handing over the building keys, facilities opening two-factor authentication restricted areas, and more!

## **ISSA Career Central: Secure Your Future**

**ISSA is always looking for ways to demonstrate its dedication to YOU, the information security professional looking for career advancement. So at this year’s International Conference in Dallas, we would like to present to you ISSA Career Central: Secure Your Future.**

**Attendees, you can:** Meet recruiters and speak with them in a private setting; receive feedback on your resumes; and complete mock interviews.

**Employers:** Are you currently recruiting? Stop by and let us know about your job openings!



Armor | Anywhere

# Confident security for your cloud.

So confident that we're offering special pricing on Armor Anywhere for a limited time only.

50% OFF

100% SECURE



Consistently defend your valuable data and applications, no matter where they're located. Extend and scale Armor's battle-proven cloud security and threat intelligence capabilities to public clouds or even your own internal IT environments.

Armor | Anywhere

DEFEND YOUR DATA. ANYWHERE.

ARMOR™

BETWEEN YOU AND THE THREAT

armor.com | 1 877 262 3473

## Breakout Session Three: 1:45 pm - 2:30 pm

### Featured Speaker

#### Protect to Enable



Malcolm Harkins: Chief Security and Trust Officer, Cylance, @ProtectToEnable

#### Business Skills

11/2/2016, 1:45 pm - 2:30 pm

Landmark B/C

Why does the information security team exist? How should we frame the context for computing to connect and enrich lives while also ensuring the obligations to do it right are appropriately addressed?


### Sponsored Session

#### The Eight Imperatives for Agile and Scalable Cloud Security



Sami Laine: Principal Technologist, CloudPassage

#### Application Security

11/2/2016, 1:45 pm - 2:30 pm 

Cumberland A/B

The momentum of cloud computing is continuing to build, but security of workloads in the cloud continues to be a key concern. There are many myths as well as real challenges. This presentation will explore the reasons why traditional security tools do not work well in cloud environments. Then we will discuss eight key imperatives for securing cloud-based infrastructure and application delivery, based on real-world results at large enterprise environments.

#### The CISO's Guide to Incident Response



Andrew Hay: CISO, DataGravity, @andrewsmhay

#### Incident Response

11/2/2016, 1:45 pm - 2:30 pm

Cumberland K

Security and IT practitioners often find themselves in an uphill battle to convince C-suite executives of the importance of a formal incident response (IR) program. One of the most common rebuttals from the business is the age old "It hasn't happened to us" or "Nobody cares about attacking our organization." This is simply not the case. We, as a security industry, finally have ample data from which to draw—without having to resort to fear, uncertainty, and doubt (FUD)—to justify the investment in tools, processes, and training to protect our respective organizations. This session aims to teach in-the-trenches practitioners how to communicate the need for a formal IR program in a way that resonates with your senior leadership team. Learn tips and tools for justifying the expense of training, personnel, and equipment in the face of common business objections.

#### A Practitioner's Guide to a Secure Agile Transition



Cuneyt Karul: Chief Security Architect, BlueCat Networks

#### Application Security

11/2/2016, 1:45pm - 2:30pm

Cumberland G/H

Agile SDLC methodologies have a bad reputation when it comes to security because the fast pace of development cycles often leaves little room for extensive security validation; and frequent changes in requirements makes it harder to foresee potential security issues. Although the dynamic nature of agile is indeed a challenge, agility does not necessarily mean insecure software. This session will overview the lessons we, as a mid-size network appliance and software vendor, learned during our transition from a traditional top-down SDLC methodology to a fast-paced agile/scrum environment. There are many challenges in transitioning to an agile methodology even when security is not a major concern. From the viewpoint of a security practitioner, the challenges are bigger as it is not always easy to convince product

owners that security is not an impediment but a vital part of the business. Short development cycles combined with frequent changes in requirements make the software even harder to secure against threats. There is no silver bullet, but with a lot of experimentation and research we were able to create a process where security is an integral part of our entire agile SDLC process with great results. This presentation will go over practical aspects of what we have tried to ensure that our agile process is secure; what worked well and what did not. We will present a list of actionable items, both managerial and technical, along with how we exactly implemented them, so that they can be used as guidelines. Some of the process changes we made include raising the awareness and skills of the entire team about security, integrating automated vulnerability scanning at every stage of development, involving dedicated security experts in projects as SMEs, and using misuse cases along with use cases in our agile story generation, to name a few. Another important lesson we've learned was that security is an ongoing process that requires constant refinement over time, and active participation in the security community is essential.

#### Cyber Law Update



Monique Ferraro: Counsel, Cyber Practice, Munich Re US

#### Laws and Regulations

11/2/2016, 1:45 pm - 2:30 pm

Cumberland E/F

Data breach, cybersecurity, and Internet of Things, including drone legislation and litigation, will be the focus of this session. Topics will include pending federal legislative proposals, implementation of the CISA, the recent (at the time of proposal pending) SCOTUS decision in *Spoeko, Inc vs Robins* and pending legislative proposals regarding drones.

#### The Architecture of a Secure IoT Gateway: A Technical Deep Dive



David Dufour: Head of Security Architecture, IoT, Webroot, Inc., @davidmdufour

#### Infrastructure

11/2/2016, 1:45pm - 2:30pm

Cumberland L

The pervasive spread of Internet-connected devices into Operational Technology Ecosystems has spurred the growth of purpose-built IoT Gateways that aggregate data from disparate IoT devices in an attempt to secure this data for transport via the Internet. Manufacturers are now forced to not only work in the confines of their specific technology but to also become experts in cybersecurity to ensure their devices meet the security needs of their clients. These teams must quickly become familiar with cybersecurity technologies found in traditional network appliances such as Deep Packet Inspection (DPI), SSL Decryption, Threat Intelligence, and others and then best determine how to implement these technologies in their gateways. The purpose of this presentation will be to walk through, in detail, the varying technologies available to device and appliance manufacturers and explain how these technologies interrelate to one another. The session will begin with an overview of a basic IoT Gateway and the components required to build such an appliance. It will then lead into a description of how SSL Decryption works, why it is relevant for traffic monitoring, and considerations for the analysis of traffic encrypted using proprietary techniques. This will lead into a deeper discussion around the need for Deep Packet Inspection, how to effectively implement and build open source packet inspection tools for prototyping, and considerations needed for moving from a prototype phase to production. The discussion around IoT Gateway functionality, packet inspection, and decryption techniques will set the stage for implementing security technologies on the Gateway itself.

*There are three principal means of developing intelligence... observation of our environment, reflection, and structured analysis. Observation collects facts; reflection combines them; structured analysis verifies the result of that combination.*



The need for accurate intelligence and predictive analysis has never been greater. We must improve our intelligence tradecraft and analytic intelligence methods to protect our critical assets. Treadstone 71—Intelligence Analysis, Training, Services, and Strategic Intelligence Program Development. Contact Treadstone 71 at [osint@treadstone71.com](mailto:osint@treadstone71.com), 888.714.0071, [www.treadstone71.com](http://www.treadstone71.com) We See What Others Cannot



# SURVIVAL STRATEGIES IN A CYBER WORLD

## Breakout Session Four: 2:45 pm - 3:30 pm

### Featured Speakers

#### Posture Makes Perfect – Cyber Residual Risk Scoring



*Michael Angelo: Chief Security Architect, Micro Focus | NetIQ Corporation, @mfa0007*

#### Incident Response

11/2/2016, 2:45 pm - 3:30 pm  
Landmark B/C

Survival in today's cyber world requires an answer to the question: "Why, with all the compliance mandates, certifications, tools, and training are hackers so successful?" The answer, "Our cyber-risk posture is too fluid to define, measure, and adapt; thus we are never as protected as we think we are" is a cop out. We should be able to describe our cyber-risk posture today, even if it will be totally different tomorrow. In other words, cyber-risk processes must adapt as we move forward. This session provides a strategy for re-evaluation and assessment using adaptive cyber-risk analysis and cyber residual risk scoring.

### Sponsored Session

#### Protecting Sensitive Data in the Cloud



*Eric Wolff: Senior Product Marketing Manager, Vormetric - A Thales company*

#### Application Security

11/2/2016, 2:45pm - 3:30pm  
Cumberland A/B



As mentioned in the keynote, you're moving to the cloud, ready or not. Both business unit agility requirements and shadow IT are driving your organization to public and private cloud service providers for business-critical workloads. Meanwhile, nearly every business function in your organization leverages a software-as-a-service solution, be it Salesforce.com, Marketo, or Workday, among many others. You have an imperative to ensure your sensitive data remains protected and secure across cloud providers. How do you get the most out of your cloud environments while maintaining control and protection of your sensitive data?

In this breakout session, learn:

- What your peers are thinking about regarding cloud security and what they are doing about it.
- Questions to ask your cloud service provider regarding data security.
- What IaaS and SaaS providers are doing, and should be doing, about securing your data.

### ISSA Healthcare SIG Sponsored Session

#### Ransomware & Health Information Exchanges - Is Your Data Safe?



*Chris Apgar: CISSP, CEO, President, Apgar & Associates, LLC, @apgarandassoc*

*Panelists: Kyle Miller: CISSP, Senior Consultant, CSG Government Solutions. @CSGGovSolutions; Marty Edwards: MS, CHC, CHPC, HCLS Compliance Officer, Dell Services Healthcare and Life Sciences; Stephen Fitton: GSLC, Information Security Officer, Clinicient*

#### Securing the End User

11/2/2016, 2:45 - 3:30 pm  
Cumberland E/F

The moderated panel will inform participants about the latest in ransomware attacks and how healthcare organizations who use health information exchanges (HIE) may be vulnerable to attack by other HIE participating organizations not implementing needed security controls.

The panel will also focus on steps HIE participating organizations can prevent ransomware attacks and how to respond in the event of a ransomware attack.

The panel will discuss:

- The current risks associated with ransomware
- The risks to healthcare organizations who participate in a HIE
- Steps participants can take in their own organizations to protect against a ransomware infection
- Steps participants can take to mitigate risk in the event of a ransomware attack
- Current views on whether or not to pay the ransom

#### CISO Success Strategies: On Becoming a Security Business Leader



*Frank Kim: CISO, SANS Institute*

#### Business Skills

11/2/2016, 2:45 pm - 3:30 pm  
Cumberland L

Learn three things that CISOs and security professionals can do to go beyond technical skills and make information security relevant and understandable to key stakeholders across your organization. The increased importance and visibility of cybersecurity as a vital component of business growth make it critical that security leaders understand how to connect with senior executives and business leaders. This session is a unique opportunity to hear from Frank Kim, seasoned security leader and CISO, as he explains three things that will make you a more effective security business leader.

#### Propel Your Career with Personal Strategic Planning



*Christa Pusateri: Team Lead at CISO Coalition, @cmpusateri*

*Bobby Dominguez: Chief Security & Strategy, CISSP, PMP, CPP, CRISC, GSLC, ITIL, C|CISO, Lynx Technology Partners, @Moonraker069*

#### Business Skills

11/2/2016, 2:45 pm - 3:30 pm  
Cumberland I/J



Your success as a professional in the cybersecurity, audit, and risk profession depends on your ability to communicate effectively and influence people who may not report to you. You also have to stay up to speed with

the latest regulations, threats, and technology. The challenge to inspire busy colleagues to cooperate and participate in the process to secure the organization is difficult. In fact, you are often accused of slowing down business workflows or holding up critical projects. The challenge is compounded with the outdated stereotypes and preconceptions that come with your technical title. Solution: When you invest in yourself and utilize a practical, personal strategic planning framework, you can develop your leadership, influence, and communication skills to find more success in your current position and future career. Attendees will leave with:

- Understanding of the 7 Pillars of Personal Strategic Planning Framework
- Examples of the rewards of investing in personal development

## You Can Help the Next Generation of Cybersecurity Professionals!

### Partner with the ISSA Educational Foundation

Stop by our booth and learn how. Our annual fund-raiser kicks off at the conference.



EDUCATION FOUNDATION

[www.issaef.org](http://www.issaef.org)

- Real-life success stories
- Interactive discussion and self-discovery
- Practical template for personal planning
- Resource suggestions for continued study

Christa Pusateri is on a mission to help cybersecurity professionals overcome stereotypes and take a proactive approach to personal strategic planning. She has been known as a dynamic, confident, and interesting speaker with a passion for bringing her sales and marketing experience to cybersecurity professionals to provide a diverse perspective in thriving in the cybersecurity field. Christa currently serves as president of ISSA Tampa Bay Chapter and is helping to build the exclusive CISO Coalition, a confidential and collaborative environment for information security executives from enterprises to create shared resources, collaborate and vet, validate, and verify their approaches to the most pressing security challenges.

### Digital Investigations: Leveraging the Multitude of Records



*Benjamin Wright: Attorney and Senior Instructor, SANS Institute, @benjaminwright*

#### **Laws and Regulations**

11/2/2016, 2:45 pm - 3:30 pm  
**Cumberland K**

Owing to advancing technologies like cloud, smartphones, and the Internet of Things the quantity of records relevant to any official investigation is expanding beyond imagination. There are SO MANY records in SO MANY places . . . email, text, photos, metadata, backups, social media, travel histories, deleted stuff . . . that traditional assumptions on how to advance an investigation or resolve a dispute have become obsolete. Today smart investigation teams are able to

leverage the massive volume of records in new and surprising ways. The team does not necessarily need access to records in order to take advantage of their existence. This presentation teaches tips and strategies and tells war stories that simply were not applicable 10 years ago. These lessons help investigators and their employers reach more favorable outcomes in HR disputes, potential lawsuits, forensic audits, regulatory inquiries, criminal proceedings and corporate espionage cases.

### The Man Behind the Curtain: Revealing the Truth of Overhyped Security Solutions



*Simon Crosby: Co-founder and CTO, Bromium, @simoncrosby*

#### **Securing the End User**

11/2/2016, 2:45 pm - 3:30 pm  
**Cumberland G/H**

With all of the hype around the potential of artificial intelligence (AI), machine learning (ML), and deep learning, it's not surprising that security companies have gotten their feet wet, declaring each new hype the fuel to their "next-gen" solution. It certainly sounds useful to leverage new math and machines to detect new threats, but what does all of this really mean? AI and ML unfortunately leave us with two challenges: vast amounts of data of unknown value that we don't know when to discard, and nagging worries that the security team might have missed a needle in the haystack. Deep learning, on the other hand, is just a new term for an old technique, already proven unsuccessful. In this session, Bromium CTO and co-founder Simon Crosby will debunk the myth of "next-gen," deep learning, and the AI/ML security solutions and discuss the benefits of investing in security experts, as well as tools that offer security by design, instead of banking on unproven and uncontextualized techniques.



## Half protected is half not.

### Full identity security for the enterprise

Centrify provides a unified solution for securing and managing privileged users' identities. Centrify leverages an organization's existing identity infrastructure to enable identity consolidation, privilege management and auditing for security and compliance, and a simplified identity infrastructure for IT.



[www.centrify.com](http://www.centrify.com)

Free trial: [www.centrify.com/free-trial](http://www.centrify.com/free-trial)  
Learn more: [www.centrify.com/resources](http://www.centrify.com/resources)

# SURVIVAL STRATEGIES IN A CYBER WORLD

## Breakout Session Five: 4:00 pm - 4:45 pm

### Featured Speaker

#### **Automotive Security: Challenges & Perspectives**



*Eric Evenchick: Director, Linklayer Labs, @ericevenchick*

#### **Application Security**

11/2/2016, 4:00 pm - 4:45 pm

#### **Landmark B/C**

In recent years, there has been a sharp increase in the discussion of automotive security. Vehicle systems, which were once static and air-gapped, are now becoming connected devices. At the same time, automotive systems are becoming more automated, with computers in control of many aspects of vehicle operations. In this talk, we will discuss the current state of automotive security and look at some of the recent attacks that have been performed. We will then talk about the systems in vehicles and why they are vulnerable, and the challenges of securing these systems. An overview of how you can get your feet wet with car hacking will be presented, and finally we will provide some insights into how the industry is moving forward, and how they can improve.

### Sponsored Panel

#### **How Effective are Incident Response Plans?**



*Moderator: Jim Robison, Director of Sales and Marketing, Anitian*

*Panelists: Andy Thompson: Strategic Advisor, Southwest Region, CyberArk, @r41nm4kr; Bil Harmer: CISSP, CISM, CIPP – Strategist, Office of the CISO, Zscaler, @wilharm3*

#### **Incident Response**

11/2/2016, 4:00 pm - 4:45 pm

#### **Cumberland A/B**

Every day we see a new story about a sophisticated new attack or big breach. The attackers are no longer just stealing data; they are holding it for ransom. In 2015 an Experian study said 81 percent of organizations had an incident response plan, which was an eight percent increase from 2014. All these breaches point to an inevitable fact: we all need an effective Incident Response Plan. It has been said that the ultimate measure of a security team's capabilities is their ability to respond to a breach. As such, let's explore what makes up an effective IRP and how we can optimize it to go beyond reaction to truly build a sustainable defense against attack.

#### **Prevent Ransomware with the Right Architecture**



*Scott Simkin: Senior Manager, Threat Intelligence, Palo Alto Networks, @scottsimkin*

#### **Application Security**

11/2/2016, 4:00 pm - 4:45 pm

#### **Cumberland K**

Thanks to advances in attack distribution, anonymous payments, and the ability to reliably encrypt and decrypt data, ransomware is on a tear. To protect your organization from having to pay attackers to free your data, you need to evolve beyond a layered security approach to a prevention-oriented architecture—or face threats of Jurassic proportions.

Key takeaways include:

- Common ransomware attack vectors and how they get into the network, endpoint, or through SaaS applications
- How to disrupt the attack life cycle by reducing the attack surface,

preventing known threats, and blocking unknown threats

- Architectural requirements for providing the visibility, intelligence, and enforcement to prevent sophisticated threats, like ransomware

#### **Modernize Your Security for Critical Applications**



*Russell Rice: Senior Director of Product Management, Skyport Systems*

*Pete Fox: VP Cybersecurity, Ascent Solutions*

#### **Application Security**

11/2/2016, 4:00 pm - 4:45 pm

#### **Cumberland G/H**



A handful of critical applications power the IT infrastructure and control access to everything—applications, data, computers, storage, and the network. That's why 70-90 percent of breaches involve compromising these applications, all too easy to do with

current tools and techniques. To regain control of your environment, you need a modern approach that keeps malware out, valid administrators and trusted systems in, provides micro-segmentation per application, doesn't require instant patching of new vulnerabilities, and provides a reliable forensic trail. This session will arm you with:

- Why the bad guys win so easily
- Recommended guidelines to secure critical applications
- A method to assess your current approach to application security
- Five key steps to follow for a secure environment

#### **Building a Mature Cyber Intelligence Program**



*Jeff Bardin: Chief Intelligence Officer, Treadstone 71, @treadstone71lc*

#### **Business Skills**

11/2/2016, 4:00 pm - 4:45 pm

#### **Cumberland I/J**

Many organizations claim to be creating intelligence for their corporate stakeholders. Most believe technology solutions provide the same. Tools, techniques, and protocols/procedures of adversaries is nothing more than data and information unless properly collected, produced, organized, analyzed, and disseminated. This discussion covers how to establish the proper strategy using proven intelligence tradecraft methods. We will cover areas of vision, mission, goals, and initiative. The discussion guides attendees through the process of development methods of collection and outlines areas for producing intelligence using structured analytic techniques while extracting the required issues from leadership for focused delivery.

#### **Protecting Data Everywhere it is Used, Shared, and Stored**



*Joe Sturonas: Chief Technology Officer, PKWARE, @jsturonas*

#### **Securing the End User**

11/2/2016, 4:00 pm - 4:45 pm

#### **Cumberland E/F**

Too many CEOs and IT leaders address data security in broad strokes, as if everything inside the company—every email, every document, every system—must be protected with the same level of tenacity. While that is a noble effort, the defend-everything-at-all-costs approach can be as costly as it is ineffective. When it comes to data security, the uncomfortable truth is that security professionals will never prevent every breach. That's why leaders need to take inventory and assess where their company is most vulnerable. In this presentation, Joe Sturonas, CTO of PKWARE, will bring attendees up to speed about how to develop a holistic data security strategy to protect information everywhere it is used, shared, and stored. Joe will help attendees answer: Where is your data located? Who has access to it? What protects it?

**Integrating Business Case Skills into GRC Regulatory Compliance Initiatives**



*Ken Lobenstein: Cyber Risk Specialist, Deloitte*  
*Neethu Thomas: Senior Consultant, Deloitte*

**Laws and Regulations**

11/2/2016, 4:00 pm - 4:45 pm  
**Cumberland L**



This session uses examples of laws and regulations as they relate to business planning and business case decision-making to demonstrate the importance of holistic GRC program and a strong enterprise approach to use of GRC tools to survive in the face of cyber challenges.

**Cyber Defense Center - Diamond Sessions: 11/2/2016, 5:00 pm - 6:00 pm**



**How to Block 2hreats Before, During, and After an Attack**



*Mark Stanford: Systems Engineering Manager, OpenDNS, now part of Cisco*

**Incident Response**

11/2/2016, 5:00 pm – 6:00 pm  
**Cumberland E/F**

With cyber attacks growing at a rapid pace, organizations of all sizes must adopt a layered security strategy to provide maximum threat protection. In this informative session, you will learn about defense-in-depth strategies and the “multiplier” benefit of combining OpenDNS Umbrella with Advanced Malware Protection (AMP) and cloud-based security services, delivered at the DNS layer. OpenDNS Umbrella delivers security at the DNS layer, creating a first layer of defense in your security stack. In seconds, this cloud platform displays your global activity from all locations. Instantly, you can identify targeted attacks by comparing your activity—over any port, protocol, or app to the rest of the world. Cisco AMP provides global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches. But because you can’t rely on prevention alone, AMP continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

**Tool Time with Tanium: With All the IT Tools Available Today, Which One Is Best for the Job?**

*Santino Salyards: Tanium*

11/2/2016, 5:00 pm - 6:00 pm  
**Cumberland G/H**



Today’s organizations are being flooded with endpoint tools for security, operations, and other various IT needs. Many of these tools claim to provide next-gen security, incident response, forensics, patching, compliance, and other general operations features. All of them have their own console, management infrastructure, and yet another agent. How do you prioritize endpoint real estate and budget? During this demonstration, we will discuss the problems that everyone is trying to solve with these tools, the overlap in functionality, the challenges they present, and why everyone should have a simple toolkit that is fast, easy to use, effective and gives you the flexibility to switch out parts so that you can adapt to tomorrow’s problems.

**Thursday, November 3**

**Thursday Keynote Address: 9:00 am - 10:00 am**



**Building a Security Program That Succeeds – Scale, Efficacy and Executive Support**

*Michael Coates, CISO, Twitter, @\_mwc*

**Landmark B/C**

How does an organization build a security program that is effective, elevates security to business-level decisions but also doesn’t slow down productivity? It seems there is a never-ending list of adversaries including organized crime, hackers, adversarial governments, rampant malware, and more. An insecure business won’t succeed; a business crippled by security overhead won’t succeed either. We’ll discuss strategies for building security programs, mitigating top risks, and building an internal structure that elevates security visibility and decision-making across the business.

**Breakout Session Six: 10:15 am - 11:00 am**

**Sponsored Session**

**Best Practices from the World’s Top Security Awareness Programs**



*Steven Conrad: Managing Director, MediaPro*

*Tom Pendergast: Chief Strategist, MediaPro, @tommediapro*

**Securing the End User**

11/3/2016, 10:15 am - 11:00 am

**Cumberland A/B**

The world’s most risk-aware companies know that enlisting their employees in the fight against cyberthreats takes a continuous program of training, reinforcement, communication, and analysis. Steve and Tom have worked with hundreds of companies to create award-winning programs, and they’ll share the best practices from these companies—and ask you to brainstorm new ideas to improve your program.



**Cybersecurity Professional Career Study Findings**



*Jon Oltsik: Senior Principal Analyst, ESG, @JOltsik*

*Candy Alexander: Chair, Cyber Security Career Lifecycle, ISSA, @NH\_Candy*

**Business Skills**

11/3/2016, 10:15 am - 11:00 am

**Cumberland E/F**

This session will provide an open collaborative discussion about the inaugural ESG/ISSA research detailing cybersecurity professional development, training, career management, and opinions.

**Artificial Intelligence: The Foundation for a Secure Cyber Future**



*Keith Moore: Senior Product Manager, SparkCognition*

**Application Security**

11/3/2016, 10:15 am - 11:00 am

**Cumberland G/H**

Artificial Intelligence can identify emerging attacks the same way a human would by using a suite of machine-learning algorithms. These algorithms look at log data, such as firewall, proxy, or web logs, and aggregate threat intelligence from the web, view

# SURVIVAL STRATEGIES IN A CYBER WORLD

the DNA of downloaded files, and analyze user behaviors to find compromise within a system. This session will cover how to combine this intelligence with a massive, machine-generated, curated database of security events to provide context, experience, and constant learning in your security ecosystem.

## **Advances in Security Risk Assessment**



*Doug Landoll: CEO, Lantego LLC, @douglanoll*

### **Business Skills**

11/3/2016, 10:15 am - 11:00 am

**Cumberland I/J**

Security risk assessments are required under most information security regulations (e.g., HIPAA, PCI, FISMA), yet few information security professionals are comfortable performing them. Mr. Landoll will guide attendees through tried and true methods for performing risk assessments and recent advances in the industry, based on decades of experience and lessons learned as documented in the best selling risk assessment book, *The Security Risk Assessment Handbook*.

## **The Visible Attack Surface – What It Is and Why It Matters**



*Gidi Cohen: CEO, Skybox Security, @gidicohen*

### **Incident Response**

11/3/2016, 10:15 am - 11:00 am

**Cumberland K**

What are Indicators of Exposure and why pairing them with Indicators of Compromise makes for a more holistic and effective security strategy. For 20 years, security leaders have struggled to gain a satisfactory level of visibility over their attack surface, all the ways in which their IT systems are vulnerable to threats including potential attack vectors. Conventional security approaches—such as vulnerability scanners, endpoint protection products, patch management solutions, and network security configuration analysis—often fall short because they only give fleeting glimpses into an enterprise's current state of security. When operational teams have partial, sporadic, and inconsistent information, they cannot analyze data in context, limiting their ability to make timely and effective decisions. To build a mature, proactive security management program, security leaders need a more holistic and continuous view of the attack surface with a consistent taxonomy of its various weaknesses and vulnerabilities. This includes Indicators of Exposures (IOEs), such as exploitable attack vectors, hot spots of vulnerabilities, network security misconfigurations, and non-compliant firewalls. While Indicators of Compromise (IOCs) provide incident response teams with important traces of an incident, Indicators of Exposure (IOEs) give insight into potential exploitable attack vectors before the incident happens. Indicators of Exposure are also useful in the event of an ongoing attack, as they reveal potential hot spots so security teams can prioritize operational activities for quick and effective containment. By combining IOEs and IOCs, security leaders gain greater visibility over the attack surface, which gives them the insight they need to develop a more effective strategy for shrinking it and detecting and containing security breaches.

## **Balancing Mobile Security with Privacy: A Prescription for Closing the Trust Gap**



*James Plouffe: Lead Security Architect, MobileIron*

### **Securing the End User**

11/3/2016, 10:15 am - 11:00 am

**Cumberland L**

In a 2015 survey of 3,500 employees conducted by Harris Poll, MobileIron found that a whopping 30 percent would leave their jobs if their employer could see personal information on their mobile devices. And while most CIOs really do not want access to employees' personal content, those surveyed still worry about

the privacy of personal emails, texts, or photos, browsing history, etc., on smartphones and tablets they use for both business and personal tasks. Part of the problem is a lack of clearly defined policies. Another part is that employees are confused about what employers can and cannot see, the actions employers can take on their mobile devices, and the reasons employers may have for viewing or taking action on the information they can access. The speaker will discuss establishing privacy-centric mobile device policies for preventing the loss or compromise of corporate information, best practices for communicating with employees, and leveraging new mobile OS-level controls. Every device today is a mixed-use device, which means IT must remember to protect employee privacy as fiercely as it protects corporate data.

## **Breakout Session Seven: 11:30 am - 12:15 pm**

### **Gold Sponsored Panel**

## **Culture Changes, Communicating Cyber Risk in Business Terms**



*Moderator: Dr. Shawn Murray: Principal Scientist, United States Missile Defense Agency*

*Panelists: Chris Lietz: Principal, Cyber Risk Advisory, Coalfire Systems, Inc.; Sam Elliott: Culture Changes, Communicating Cyber Risk in Business Terms, Bomgar, @samelliott; Zach Scott: Vice President of Business Development, NRI SecureTechnologies*

### **Business Skills**

11/3/2016, 11:30 am - 12:15 pm

**Cumberland A/B**

Cybersecurity is gaining the required attention of business executives worldwide. One of the ongoing challenges is communicating what cybersecurity initiatives take precedence over other business unit priorities. From a business perspective, cybersecurity projects should align with the overall business strategy and allow the business to run more efficiently while reducing risk to the organization overall. Cybersecurity and risk management should be part of the business culture. The CIO and CISO should have a strong relationship with other business units to identify key processes, personnel, and IT resource requirements so risk can be properly assessed and cyber-related solutions can be planned, funded, and implemented. It is vital that the CIO and CISO be able to communicate justification in business terms, how they address risk, and bring value to the organization. This panel will discuss the requirement for CIOs, CISOs, and IT leaders to have the ability to confidently justify and articulate risk related to IT and cybersecurity projects in a language that is understood by everyone. We will also discuss strategies on how to ensure executives back these initiatives as part of the organizational culture as well.

## **Digital Forensics – First Responders & Incident Management**

*Prof John Walker: Visiting Professor School of Science and technology NTU; Assessor Society for Forensic Sciences, Hexforensics LTD, @hexforensics*

### **Incident Response**

11/3/2016, 11:30 am - 12:15 pm

**Cumberland K**

The digital forensics market is anticipated to grow by 125 percent before the year 2020—and this, associated with the mass of successful digital and cyber attacks becoming more frequent, drives the need to evolve skills and associated capabilities into both public and private





organizations with a coordinated life cycle that will support them to operationally Engage > Contain > Respond > Acquire > Mitigate > Report. Based on five years of delivering digital forensics, first responder capabilities, CSIRT frameworks, and expert witness engagements in the UK High Courts supporting International cases, this session will present pragmatic solutions which may be exploited to engage any internal miscreant user or external cyber attack, and seek to expand on the future role of digital investigations across private laboratories, government agencies, commercials, and international police forces.

The session will focus on how organizations can build in their own internal robust capabilities, and will introduce the importance of processes, security artifacts [both physically and logically], intentional legislations ranging from the implications of the Patriot Act, State Bills such as 1386 through the UK and EU Data Protection Acts and the ITA 2000 [Indian technology Act 2000], and the associated implications when engaging as a First responder. We will also examine the complexities of dealing with child abuse images, the COPINE and SAP scale, and qualify how such incidents should be legally dealt with. We will also investigate the value of virtualized flow—the sun CSIRT Incident Management Teams, and the value of coordinated capabilities driven by Run-Books to support the operational, in-flight incident engagement life cycle. This session will share a number of supporting resources with the delegates in the form of Run-Books, which have been developed to support child abuse image Investigations, DDoS, and malware attacks, to the Incident threat engagement. The session will conclude by offering a case example as to how OSINT, and CTI [Cyber Threat Intel] act as pre-crime, event assessment methodologies that may be used to assess the future potentials of cyber attacks [called minority reporting].

  **Scraping Together a Security Program**



*Robert Rudloff: Partner, Cybersecurity Advisory Services, RubinBrown LLP, @hfhudloff*

*David Hendrickson: Senior Cybersecurity Specialist, RubinBrown LLP*

**Business Skills**

11/3/2016, 11:30 am - 12:15 pm

**Cumberland I/J**



Building a security program looks pretty easy on a one-page graphic, but is a little more challenging to implement in reality. Join us as we describe building a security program from the ground up—going from a seemingly random set of individual activities to an integrated approach. The presentation is based on our experience doing this at a local higher education institution. Rob will describe how we pulled together governance, frameworks, policy, and requirements. David will describe how he was able to implement operational security activities designed to meet the requirements (and how to manage the unreasonable requirements). Politics, managing across organizational boundaries, influencing people who were uninterested and under engaged, and of course balancing people, process, and technology in a resource-limited environment all played a part in the effort. More important than our story, we put together a structured approach you can use in your organization to start with whatever you have and build towards a functioning security program. While every environment is unique, we believe anyone faced with starting a security program from scratch can use our approach to accelerate their progress towards a functioning security program.

**CloudPassage**

SEE US AT BOOTH #201

**SOLVING KEY SECURITY CHALLENGES**

On-demand, automated server & cloud workload security that works anywhere, at any scale.



**WORKLOAD PROTECTION**

Protect Servers and Cloud-based Workloads From Attack



**MICROSEGMENTATION**

The Fastest, Easiest Way to Control East-West Traffic



**COMPROMISE DETECTION**

Your Servers Have Been Compromised. How Can You Tell?



**AUTOMATED COMPLIANCE**

Don't Let Manual Processes Hold Up Compliance



**SECURITY AT DEVOPS SPEED**

Don't Let Security Put the Brakes on DevOps



**AWS EC2 SECURITY**

Enhanced Security and Compliance for AWS EC2

**VISIT OUR SESSION ON THE EIGHT IMPERATIVES FOR AGILE AND SCALABLE CLOUD SECURITY**

Wednesday, November 2 at 1:45 pm in the Cumberland A/B Room.  
Presented by Sami Laine, Principal Technologist, CloudPassage

To learn more, visit [cloudpassage.com](http://cloudpassage.com) or call 800-215-7404

# SURVIVAL STRATEGIES IN A CYBER WORLD

## **Transform from Surviving to Thriving by Preparing for the Next Wave of Cyber Attacks and Information-Borne Threats**



*Dr. Guy Bunker: SVP, Products, Clearswift, @guybunker*

**Infrastructure**

11/3/2016, 11:30 am - 12:15 pm

**Cumberland L**

Cyber security leaders that play vital a role in protecting their organization's critical resources and enabling new business outcomes in this accelerating cyber world need to rethink how they can pro-actively defend against the next wave of cyber attacks and information-borne threats, two of today's most pressing and employee-centered security challenges. Dr. Bunker will analyze the latest attack techniques and information risks while discussing how new adaptive detection technology and non-disruptive protection methods influence employee collaboration and take the organization's security culture from surviving to thriving.



## **Secure User Application Access in a Hurry**



*Scott Scheurich: Program Manager, Ashburn Consulting, LLC*

*Marc Boorshtein: CTO, Tremolo Security, Inc.*

*Michael Dent: Chief Information Security Officer, Fairfax County, VA*

**Securing the End User**

11/3/2016, 11:30 am - 12:15 pm

**Cumberland G/H**

Too often there are information technology applications stood up to support first responders only to require those first responders to create and remember yet another username and password to use the application. The problem continues as more applications are activated. Furthermore, each application has to keep track of these users and provision users with the right permissions within the application. Leveraging grant funds, and on behalf of the National Capital Region, Fairfax County sponsored and manages a service called the Identity and Access Management Service (IAMS) that has successfully overcome these challenges. IAMS is a self-contained authentication service that enables personnel to use his or her locality credential to access regional applications when properly authorized. It does this by communicating, via the NCRNet, with properly authorized end-user directories within each participating locality. IAMS merely works to query those directories to validate the user for the purpose of accessing the application. IAMS can also perform certain provisioning and workflow functions to easily and properly authorize access for the end user (including those who do not possess a locality identity) to applications and application entitlements.

## **Breakout Session Eight: 2:30 pm - 3:15 pm**

### **Featured Speaker**



## **Weaponizing Your Words for Talent Retention**



*Deidre Diamond: Founder and CEO, CyberSN,*

*@deidrediamond*

**Business Skills**

11/3/2016, 2:30 pm - 3:15 pm

**Landmark B/C**

Our words are powerful. With CISO attrition at an all-time high and practitioners leaving technical careers more than any other field, it's clear our industry is experiencing breakdown. People are leaving

information security, especially women. Talent retention is more than competitive salaries; it's about having an empowered vocabulary and eliminating limiting words. Positive communication weaponizes our words, creating measurable agreements and clear responsibilities. Communication skills can be tactical or destructive, and it's up to us to choose and use them wisely. Let's discuss our talent retention challenge and learn the five words that must be eliminated from our vernacular.

### **Sponsored Session**



## **Stepwise Security – A Planned Path to Reducing Risk**



*Wade Tongen: Western Area System Engineering Director, Centrifly, @Centrifly*

**Securing the End User**

11/3/2016, 2:30pm – 3:15pm

**Cumberland A/B**



Attackers are making major headway into our businesses with simple tactics that exploit our weakest points. It's clear that we need to bolster our defenses, but prioritization can seem daunting. Join Wade Tongen, Western Area System Engineering Director from Centrifly, as he walks through some proven practices for prioritizing a risk mitigation strategy, starting with the easy gaps that most often lead to data breach, and moving to sophisticated and comprehensive control.

### **ISSA WIS SIG Sponsored Session**



## **Get the Right People in the Right Places to Maximize Your Cyber Team Performance [2-part workshop]**



*DeeDee Smartt Lynch: President/ Chief Resource Investigator, Smartt Strategies LLC, @ddsmarttlynch*

**Business Skills**

11/3/2016, 2:30 pm - 4:15 pm

**Cumberland E/F**

Understanding the significance of team roles and incorporating that into your cyber portfolio allows your team to more quickly and efficiently respond to any cyber-related incident or organizational inquiry. This session clarifies the necessity for a balanced approach and explains how the different team-role behaviors impact and provide greater value to the overall team. A FREE personal Team Role Assessment (a strong people-oriented tool that helps increase your cyber team effectiveness) with analysis is included. Exercises prepare you for application of the principles learned. This workshop will make a huge difference in how your team operates, interacts, and performs!



## **Best Practices for Responding to a Cyber Attack and Working with Law Enforcement in the Aftermath**



*Edward McAndrew: Assistant United States Attorney, Cybercrime Coordinator, US Attorney's Office*

*Patrick Dennis: President, CEO, Guidance Software, @Patrick\_Dennis*

**Incident Response**

11/3/2016, 2:30 pm - 3:15 pm

**Cumberland K**

Organizations are increasingly operating under the assumption that their network has already been compromised or will be. Cybercriminals are constantly looking for new ways to bypass security measures. As a result, no organization is immune from attack. Forty-three percent of organizations surveyed by the Ponemon Institute in 2014 said they had suffered a data breach. Yet, 27 percent of companies didn't have a data breach response plan or team in place. The human instinct is to try to find those responsible for an attack. However, companies should resist this course of action. Any attempt to access, damage, or impair another system that appears to be involved in an attack without law enforcement involvement is most likely illegal and can result in civil and/or criminal liability. Government agencies have repeatedly

stressed the value of working closely with the government to mitigate the damage from attacks and to protect consumers. This year, the FTC stated that it is more likely to view companies that have worked with the agency involved in a cybersecurity investigation favorably than those who have not. In this session, Assistant US Attorney Edward McAndrew and Guidance Software President and CEO Patrick Dennis will discuss best practices for preparing and responding to a cyber attack and working effectively with law enforcement.

**The 100-Minute MBA for Information Security Professionals [2-part workshop]**



*James K. Adamson: Principal Consultant, Urbane Security, @jameskadamson*

*Branden R. Williams: VP, Head of Strategy, FirstData, @brandenwilliams*

**Business Skills**

11/3/2016, 2:30 pm - 4:15 pm

**Cumberland I/J**

Many security professionals (even most information technology workers) did not go to college to pursue a business degree. Most don't have an MBA. This isn't all bad, because we don't place ourselves in the box of business history. But MBAs do tend to come with some negative connotations (they're just suits that think they know everything, right?) The reality is that the degree aims to prepare students to manage the details of a business, from finance to ethics, strategy to operations. As a member of the security team, you are a business inside of your business. You are a service to the end goal of the company. You are a cost center. You have an important offering, but it will only be accepted if it meets the needs of the business. Whether you work at a small startup or a large enterprise, learn the skills that will help you make security important to your entire organization.

**Is Your Vulnerability Management Program Evolving? Introducing the Vulnerability Management Maturity Model – VM3**



*Gordon Mackay: Executive Vice President, Chief Technology Officer, Digital Defense Inc., @gord\_mackay*

**Infrastructure**

11/3/2016, 2:30 pm - 3:15 pm

**Cumberland L**

The information security landscape has evolved significantly during the last five years with the emergence and wider use of new technologies such as Cloud, BYOD, Mobile, and the Internet of Things. Alongside this landscape, corporate organization key defense leaders—CIOs, CSOs, and CISOs—have evolved in their information security defense strategies, as well as in how they think and approach information security. This different and evolved landscape, combined with defense leaders' new mind-set, has influenced key information security processes and in particular has resulted in a greater understanding of the process of vulnerability management. This session presents a Vulnerability Management Maturity Model, referred to as VM3 and which identifies six different levels of vulnerability management maturity within which different organizations operate. The session covers the six high-level activities, as well as a surrounding business environment that characterize an organization's execution of the vulnerability management process. Key challenges present within each of the six high-level activities of vulnerability management, as well as challenges imposed by the organization's surrounding business environment, are identified and described. Attendees will learn and appreciate how these key challenges impede one's ability to achieve higher levels of maturity, as well as strategies on overcoming these identified challenges. .

**THALES | Vormetric**  
A Thales company

**Data Protection**  
With Management, Speed and Trust

- APPLICATION ENCRYPTION**  
Format Preserving and Field-Level
- TRANSPARENT ENCRYPTION**  
Database and Files Unix, Windows, Linux
- CLOUD ENCRYPTION GATEWAY**  
Box, Amazon S3 for Cloud Storage
- VAULTLESS TOKENIZATION**  
Dynamic Data Masking with REST APIs
- ENTERPRISE KEY MANAGEMENT**  
Secure KMIP, TDE Keys, Certificates

Vormetric.com Search: Vormetric

# SURVIVAL STRATEGIES IN A CYBER WORLD

## What Happens in the Cloud Stays in the Cloud: Data Protection of Public Cloud Storage



Jason Paul Kazarian: Senior Architect, Hewlett Packard Enterprise

### Application Security

11/3/2016, 2:30 pm - 3:15 pm  
Cumberland G/H

Many cloud service providers are now offering encryption of object stores through a Java or other API. Amazon S3 and Azure Blob Storage are examples. Developers may use these services in one of two ways: allow the cloud provider to store the encryption keys or retain keys on-premises and “loan” them to the cloud provider during encrypting and decrypting API calls. This session will demonstrate Java code that implements the latter approach: generating and storing keys via KMIP interface while providing keys only when necessary to a cloud storage API.

## Breakout Session Nine: 3:30 pm - 4:15 pm

### Featured Speaker



## Mr. Robot – Can it Really Happen?



Candy Alexander: Director, ISSA Cyber Security Career Lifecycle, @NH\_Candy

### Business Skills

11/3/2016, 3:30pm – 4:15pm  
Landmark B/C

We’ve all seen how hackers are portrayed in movies and television shows. From Mr. Robot to CSI Cyber, this presentation will debunk the Hollywood view of cybersecurity and make it real. Time to separate the fact from the fiction!



## Compliance in the Cloud



Andrew Plato: CEO, Anitian, @andrewplato

### Infrastructure

11/3/2016, 3:30 pm - 4:15 pm  
Cumberland L

We are all in the cloud. But, are we compliant in the cloud? As organizations move a big part of their infrastructure into the cloud, compliance has to adapt to this changing environment. In some ways, compliance in the cloud is simpler than on-premise. However, there are many misconceptions about compliance in the cloud. Anitian has built a comprehensive library of strategies and reference architectures that can both accelerate and sustain compliance with common standards such as PCI DSS, ISO 27001, and HIPAA. In this presentation, the Anitian team will present some of those strategies. Furthermore, we will discuss how to make compliance efforts more

dynamic and agile using risk-based methods. Additionally, we will demonstrate how you can accelerate compliance using cloud services, such as key management and directory services.



## Business Continuity and Cybersecurity – Partners in Crime (Cyber)



Laura Mosley: Business Continuity Program Manager, Southern Wine & Spirits

Ron LaPedis: Workforce Continuity Strategist, SunGard Recovery Services

### Incident Response

11/3/2016, 3:30 pm - 4:15 pm  
Cumberland K



Crime fighters Laura and Ron will lead you through how to integrate business continuity and cybersecurity to ensure a comprehensive assessment, plan, and response is in place to protect your organization. So put

on your capes and superhero glasses and be prepared to participate in a workshop where you will walk through the basics of business continuity and identify integration points for cyber components. This will be a highly collaborative workshop session.

## Cyber Defense Center - Diamond Sessions: 11/3/2016, 4:30 pm - 5:30 pm



## Tool Time with Tanium: With All the IT Tools Available Today, Which One Is Best for the Job?

Santino Salyards: Tanium

11/3/2016, 4:30 pm - 5:30 pm  
Cumberland G/H



Today’s organizations are being flooded with endpoint tools for security, operations, and other various IT needs. Many of these tools claim to provide next-gen security, incident response, forensics, patching, compliance, and other general operations features. All of them have their own console, management infrastructure, and yet another agent. How do you prioritize endpoint real estate and budget? During this demonstration, we will discuss the problems that everyone is trying to solve with these tools, the overlap in functionality, the challenges they present, and why everyone should have a simple toolkit that is fast, easy to use, effective, and gives you the flexibility to switch out parts so that you can adapt to tomorrow’s problems.

## Thanks to the Conference Steering Council:

Stefano Zanero, Committee Chair

### Content

Elliott Franklin, *chair*  
James McQuiggan, *chair*  
Subhash Bhatia  
Rob Borkowski  
Meg Bridgeman  
Michael Brown  
Jennifer Byers  
Curtis Coats  
David Cruz  
Allan Cytryn  
Drew Daniels

Meenaxi Dave  
Gerardo Di Giacomo  
Carole Dicker  
Pam Fusco  
Mariana Hentea  
Derek Hill  
John Jordan  
Srikant Mantravadi  
Shawn Murray  
Chandhrashekar Pandhiri  
Bill Petersen  
Terry Quan

Arthur Richard  
Jim Robison  
Antonio Russell  
Dean Sorensen  
Richard Starnes  
Marv Stein  
Manoj Tripathi  
Roy Wattanasin  
Glenn York

### Vendor Relations

Michael Horsch Fizz, *chair*  
Matthew Idelkhani, *chair*  
Yazan El-Hamwi  
Shahab Nayyer  
Anjola Oluwa Adeniyi  
Shane Perry  
Aby Rao  
Almir Rocha

### Audience Development

Meenaxi Dave, *chair*  
Olawale Adeyemo  
Ofer Amrami  
Jennifer Byers  
Curtis Coats  
Bob Folden  
Colleen Murphy  
Bill Petersen  
Terry Quan  
Arthur Richard  
Thomas Tardy

ly resolved with need for six million practitioners by 2019.<sup>16</sup> Unfortunately, cybersecurity needs new practitioners now, as well as in the next three to five years.

### Consider digital immigrants as well as digital natives

Today's workplace is unique in that it is multi-generational with up to four generations represented. Building a cybersecurity team that reflects this workforce might be better positioned to address the diversity in behaviors, attitudes, and policy compliance that exists within the current workforce,<sup>17</sup> as well as expand the pool of potential job candidates. Both digital natives (Millennials and beyond) and digital immigrants offer unique advantages for a cybersecurity team.

Digital natives grew up online and embed technology into almost every part of their lives, especially social media. They embrace emerging technology, but their attitudes and behaviors can potentially create security risks for the enterprise, such as blurring the boundaries between personal and work behaviors.<sup>18</sup>

Digital immigrants are individuals who entered school and/or the workplace before widespread use of digital technologies and adopted them later in life.<sup>19</sup> This group covers pre-millennial generations such as Baby Boomers and Gen-Xers. These groups may present some challenges in regards to level of comfort with technology, but they tend to follow policies and recommended security practices.<sup>20</sup>

By recruiting and hiring a mixture of digital immigrants and digital natives, the cybersecurity team will be better equipped to manage the security challenges faced in today's multi-generational workforce. Another benefit is that digital immigrants have a wealth of experience with the adoption of technology and securing it to maximize the benefits and minimize potential risks because during their careers they have had to assimilate new tools such as operating systems, applications, and devices and find ways to secure them appropriately. For example, digital immigrants have had to adopt a number of telecommunications devices ranging from text pagers to smartphones over the last two decades and develop a combination of policies and procedures to secure their usage in the workplace.

16 Millard Snipplewitz (2016) "Cybersecurity Talent Gap: We're Looking in All the Wrong Places," SecureWorld – [http://www.secureworldexpo.com/cybersecurity-talent-gap-were-looking-all-wrong-places?utm\\_source=SW+Post+June+9,+2016&utm\\_campaign=SW+Post%3A+June+9,+2016&utm\\_medium=email](http://www.secureworldexpo.com/cybersecurity-talent-gap-were-looking-all-wrong-places?utm_source=SW+Post+June+9,+2016&utm_campaign=SW+Post%3A+June+9,+2016&utm_medium=email).

17 Anderson, K. (2014) "Managing Security Awareness in a Multi-Generational Workforce," ISSA Journal January 2014.

18 Cisco Annual Security Report (2013) – [https://www.cisco.com/web/offer/gist\\_ty2\\_asset/Cisco\\_2013\\_ASR.pdf](https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2013_ASR.pdf).

19 "Digital Immigrant" Urban Dictionary – <http://www.urbandictionary.com/define.php?term=Digital+Immigrant>.

20 Zone Alarm, "The Generation Gap in Computer Security: A Security Use Survey from Gen Y to Baby Boomers," (2012) – [http://www.zonealarm.com/products/downloads/whitepapers/generation\\_gap\\_research\\_2012.pdf](http://www.zonealarm.com/products/downloads/whitepapers/generation_gap_research_2012.pdf).

**Cybersecurity experts are in demand.**

**MS Cyber and Information Security**

**DSc Cybersecurity**

**CAPITOL TECHNOLOGY UNIVERSITY**

1927

Earn your degree in live online courses

## Retain and train existing cybersecurity team

This is common sense, but it is cheaper and easy to take steps to retain existing staff than recruiting new employees. This can result in significant cost savings to employers. The true cost of replacing an employee can cost up to nine months salary on average. For high-skilled positions, such as cybersecurity professionals that require higher educational levels and/or specialized training, the real cost can be as much as 213 percent of the yearly salary of an employee.<sup>21</sup>

Unfortunately, cybersecurity can be a burnout profession. According to Joshua Corman, an expert in security intelligence, it is important to consider this in leading and working in this high-stress discipline. While little research is available on the topic, an RSA 2012 survey of stress levels among cybersecurity practitioners showed some disquieting data around indicators of burnout, such as high levels of cynicism and exhaustion.<sup>22</sup> It is important to mitigate this situation with opportunities for practitioners to recharge their batteries, especially participating in professional development activities. Some cybersecurity managers may discourage professional development activities because of a mistaken belief that staff will use new skills to move on to new positions in other organizations. However, the opposite may be true: cybersecurity practitioners may leave because of the lack of professional development training opportunities.

If organizational funding is limited, at least offer work days to pursue self-funded training or consider having team members develop training modules in their specific cybersecurity domains for the group. If organizations offer tuition reimbursement, encourage its use<sup>23</sup> to pursue degrees or certificate programs in cybersecurity or other related areas. The need

21 Merhar, C. (2016) "Employee Retention – The Real Cost of Losing an Employee," Zane Benefits – <https://www.zanebenefits.com/blog/bid/312123/Employee-Retention-The-Real-Cost-of-Losing-an-Employee>.

22 Thomson, I. (2012) "IT Staffers on Ragged Edge of Burnout and Cynicism," *the Register* – [http://www.theregister.co.uk/2012/02/27/it\\_staff\\_stress\\_survey/](http://www.theregister.co.uk/2012/02/27/it_staff_stress_survey/).

23 Anderson, K. (2014). *The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture*. CRC Press.

to renew knowledge and skills is not unique to cybersecurity. The accelerated rate of technology and business change means that organizations will need their workforce to continuously refresh their skill sets to remain competitive. In 2016, Randall Stephenson, the CEO and Chairman of AT&T, stated that his employees need to engage in five to 10 hours a week educating themselves or they will "obsolesce themselves with technology."<sup>24</sup>

## Hope for the future: Increasing the cybersecurity workforce in the long run

### Encouraging Generation Z

Gen Z are the younger brothers and sisters of Gen Y and share many of their characteristics in that they are digital natives with the Internet existing all their lives and embracing technology in every life activity. Even more than their older siblings, they have integrated mobile technology rather than the personal computer as a primary communication mechanism and adopted social networking at an earlier age. Gen Z differs from Gen Y in their early life experiences that have included the war on terror, continuing overseas military conflicts, and the Great Recession. *Modern Family's* Alex is an example of some common Gen Z traits: responsible, industrious, and concerned about the future. While there is some debate around defining Gen Z, most demographic researchers put its start around the early 1990s to mid-2000s, its membership currently between nine to 19 years olds. Gen Z is representative of the multicultural nature of population with a significant expansion of the Hispanic and mixed-race population, according to the US Census Bureau.<sup>25</sup>

Gen Z's technical prowess makes them excellent candidates for cybersecurity's next wave of practitioners. Social changes that occurred over their lifetime may reduce the potential influence of gender stereotypes on educational and career options. In addition, technology companies and non-profit organizations offer early exposure to programs that might ultimately create an interest in cybersecurity careers. Many of these immersion opportunities target populations that have traditionally been under-represented in cybersecurity, such as women and minorities.

One example is Girls Who Code,<sup>26</sup> a non-profit organization that provides a seven-week summer immersion program focused on preparing young women for opportunities in technological fields in major cities such as New York, Boston, Miami, Seattle, and San Francisco. In addition to training, participants have the opportunity to meet individuals working for start-ups. Program sponsors include Twitter, Gold-

24 Carson, B. (2016) "People Who Don't Spend 5 Hours a Week Online Learning Will Make Themselves Obsolete, Says AT&T CEO," *Business Insider* – <http://www.businessinsider.com/people-who-dont-spend-5-hours-a-week-online-learning-will-make-themselves-obsolete-says-att-ceo-2016-2>.

25 Williams, A. (2015) "Move Over, Millennials, Here Comes Generation Z," *the New York Times* – [http://www.nytimes.com/2015/09/20/fashion/move-over-millennials-here-comes-generation-z.html?\\_r=0](http://www.nytimes.com/2015/09/20/fashion/move-over-millennials-here-comes-generation-z.html?_r=0).

26 Girls Who Code – <https://girlswhocode.com>.



**Don't Miss This Web Conference**  
**How to Recruit and Retain Cybersecurity Professionals**

**2-Hour live event Tuesday, October 25, 2016**  
 9 a.m. US-Pacific/ 12 p.m. US-Eastern/ 5 p.m. London

[Click here to register!](#)

**For more information on this or other webinars:**  
[ISSA.org => Web Events => International Web Conferences](#)

man Sachs, and Intel.<sup>27</sup> Since its start in New York City with twenty learners, over a thousand girls have participated.

Google's Made with Code<sup>28</sup> is their \$50 million initiative with the overarching focus of getting more girls involved in software engineering and shattering any existing stereotypes about careers in technology. According to Google vice president Megan Smith, "Our industry has lots of stereotypes, including the notion that coding means sitting at a computer alone. We hope to show girls that coding is fun. But there's also the simple fact that supply and demand is not working. There are millions of jobs out there going begging."<sup>29</sup> In 2015, Google announced an expansion of its efforts to encourage the participation of women and minorities to pursue technology careers by offering vouchers for these individuals to acquire software development skills.<sup>30</sup> These programs are important because information technology often serves as a stepping stone to careers in cybersecurity. In addition, a number of organizations are offering scholarships to women, minorities, and veterans. Some examples include:

- (ISC)<sup>2</sup> Foundation women's cybersecurity scholarships
- International Consortium of Minority Cybersecurity Professionals cybersecurity scholarships<sup>31</sup>

## Conclusion

There is no "silver bullet" to resolving a shortage of practitioners in the cybersecurity workforce. However, there are several approaches to fixing a problem.

1. Do nothing
2. Manage the consequences
3. Have an action plan to fix it

The current shortage of cybersecurity practitioners requires an active approach to resolving the problem both in the near and long term. While colleges and universities are offering more cybersecurity degree options for Gen Y and Gen Z, many older practitioners, especially older Baby Boomers, will leave the workplace over the next few years, creating a talent void that will require filling. Meeting business and societal needs for sufficient cybersecurity practitioners will entail a multi-faceted approach.

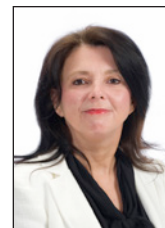
In the near-term, an approach is the establishment of strategic collaborations between education, professional associations, and public/private employers such as developing education/training programs to provide transitioning professionals with the necessary core competencies to "hit the ground run-

ning" in cybersecurity positions. Organizations will need to looking "outside the box" in cybersecurity hiring, such as actively recruiting under-represented groups such as minorities, women, veterans, and older workers.

While seeking new potential practitioners, we need to continue to retain and develop our exiting cybersecurity workers. As a long-term strategy, we need to actively promote and develop Gen Z as the next generation of cybersecurity practitioners.

## About the Author

*Kerry A. Anderson is an information security and records management professional with more than 18 years of experience in information security and IT across a variety of industries. She holds the CISSP, CISA, CFE, CISM, GIAC, CRISK, ISSAP, ISSMP, CCSK, and CSSLP certifications. Ms. Anderson has an MBA, MS in Computer Information Systems, and a Master's in Information Assurance. She recently completed her Master's of Arts in Adult Education and Training with a focus on social learning and distance education. Ms. Anderson is the author of The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture, published by CRC Press. She can be reached at [kerry.ann.anderson@verizon.net](mailto:kerry.ann.anderson@verizon.net).*



## ISSA CAREER CENTER

### Looking to Begin or Advance Your Career?

ISSA.org => Career => Career Center

The [ISSA Career Center](#) offers a listing of current job openings in the infosec, assurance, privacy, and risk fields. [Visit the Career Center](#) to look for a new opportunity, post your resume or post an opening. Among current 1,025 job listings you will find the following:

- **Group Manager, Offering Information Security Governance** – Avana, Seattle, Washington
- **Information Security Technical Risk Analyst** – University of Minnesota, Minnesota
- **IT Security Analyst I** – Teacher Retirement System of Texas, Austin, Texas
- **Security Architect PCI Lead** – Aspect Software, Orlando, Florida
- **Information Security Specialist** – Rotating Shifts – SecureWorks – Dell, Inc., Bucharest, Romania

[Visit our Career Center online](#) for a full listing of job openings! Questions? Email Monique dela Cruz at [mdelacruz@issa.org](mailto:mdelacruz@issa.org).

27 de la Cruz, R. (2013) "Girls Who Code Debuts Their Much Lauded Summer Camp in Boston," Venture Fizz – <https://venturefizz.com/blog/girls-who-code-debuts-their-much-lauded-summer-camp-boston>.

28 Made with Code – <https://www.madewithcode.com/>.

29 Cook, J. (2014) "Google Invests \$50 Million in 'Made With Code' Program to Get Girls Excited about CS," TechCrunch – <http://techcrunch.com/2014/06/22/google-invests-50-million-in-made-with-code-program-to-get-girls-excited-about-cs/>.

30 Smith, D. (2014) "Google Is Offering Free Coding Lessons to Women and Minorities," Business Insider – <http://www.businessinsider.com/google-free-coding-lessons-to-women-2014-6>.

31 "Educational Funding," International Consortium of Minority Cybersecurity Professionals – <https://icmcp.org/programs/educational-funding/>.

# Cyber Workforce Strategy: Developing Professionals Internally

By Jeff Fenton – ISSA Senior Member, Silicon Valley Chapter



**This article outlines one organization’s approach to developing cybersecurity professionals internally from its existing workforce, creating an internal training program administered by its Security Education and Awareness team.**

## Abstract

Cyber workforce strategy is a major issue for many organizations across government and the private sector. Sourcing talent externally is challenging and many positions go unfilled [1]. This article outlines one organization’s approach to developing cybersecurity professionals internally from its existing workforce. The company created an internal training program administered by its Security Education and Awareness team. The program has produced many graduates filling a variety of roles. Participants include early-career and experienced professionals seeking broader knowledge and potentially new or increased responsibility.

## Cyber workforce needs

Lockheed Martin Corporation (LMC) is a major international enterprise in the aerospace and defense sector with about 115,000 employees. Cybersecurity at LMC includes a Corporate Information Security (CIS) organization that works closely with the corporation’s business areas to address the security of its core network, perimeter-facing and program networks, supply chain and joint ventures, and delivered products and services. In addition to CIS, many system administrators and other employees in operational groups also have some security responsibilities. The company must enable business at acceptable risk while meeting a variety of compliance mandates including Department of Defense (DoD) and other United States government (USG) regulations; local country regulations; privacy legislation in the US, Canada, European Union, and other countries; the Payment Card Industry (PCI) standards; and the US Sarbanes-Oxley Act and Health Insurance Portability and Accountability Act.

The CIS team collaborates with the LMC business areas, government, industry partners, and the academic and professional community to shape and share best practices. CIS also collaborates with stakeholders across the enterprise including

legal, human resources, physical security, internal audit, international trade compliance, global supply chain operations, and the corporate privacy office. (Systems and networks that are classified under USG and other country government direction are administered separately by the business areas.) Cybersecurity roles at LMC and many other large organizations include:

- Governance, risk, and compliance
- Security education and awareness
- Supply chain cybersecurity
- Industry and customer liaison
- Security readiness testing (collaborative “blue team” and simulated opposition “red team”)
- Vulnerability management
- Cybersecurity architecture and engineering
- Security program management
- Identity and access management
- Endpoint and data protection
- Firewall, gateway, and perimeter security operations
- Intrusion detection and response
- Investigation and forensics Support

## Finding the fit and filling the roles

Most organizations, large and small, source cybersecurity talent through typical advertised job search channels and external recruiters. Developing a job description and qualifications is challenging, and finding suitable external candidates can be even more difficult. There is always a certain amount of risk with vetting and evaluating unfamiliar candidates. Engaging current employees for referrals and working with professional organizations can help to identify candidates who may be a better match. Organizations such as ISSA play a vital role by assisting its members with career preparation and helping to link candidates with openings [2].



Defining and staffing cybersecurity roles is especially challenging for small and medium-sized organizations. Many organizations utilize external service providers for some security tasks, especially tasks requiring around-the-clock coverage. Cloud service providers, with their economies of scale, can provide security support that would be difficult for a customer to staff in-house. Cloud providers can also standardize their offerings and maintain a simpler, more up-to-date infrastructure, enabling their customers to avoid or reduce the burden of legacy systems and the complexity, “technical debt,” and resulting higher risk that often come with maintaining them.

Once the enterprise identifies the organization structure and roles for cybersecurity positions it will staff, as well as the functions it chooses to outsource, the next step is finding suitable candidates. Enterprises seek relevant hands-on experience and many also specify one or more professional certifications as a requirement or preference for certain positions. A professional certification demonstrates diligence to prepare for and achieve, though many certifications emphasize broad knowledge of principles rather than hands-on operational skills and are technology vendor-agnostic rather than vendor-specific. This sampling covers some certifications and their characteristics:

- Broadly-based, vendor-agnostic certifications such as the Certified Information Systems Security Professional (CIS-SP) [3] require demonstrated knowledge and experience across the cybersecurity field and are often preferred or required for senior technical and leadership roles.
- The CISSP advanced concentration certification, Information Systems Security Management Professional (ISSMP) [4] and the Information Systems Audit and Control Association (ISACA) Certified Information Security Manager (CISM) certification [5] are especially focused on leadership and program management roles.
- Vendor-agnostic advanced and specialty (ISC)<sup>2</sup> credentials include cybersecurity subfields such as architecture or forensics and industry segments such as health care [6].
- The SANS Global Information Assurance certifications cover a variety of technical specialties, many of which are vendor-agnostic [7].
- The (ISC)<sup>2</sup> Systems Security Certified Practitioner (SSCP) certification emphasizes hands-on technical skills for operational roles [8].
- Vendor-specific certifications focus on specific technologies for operational roles.

### **An alternative approach: Developing cybersecurity professionals internally**

LMC has taken an alternative approach to fill many cybersecurity roles by identifying and developing professionals internally. Very often, the best person to fill a position is already in the enterprise, understands the business and culture, and wants to learn and grow. LMC’s diverse workforce includes

many professionals already performing specialized roles with some security content and others seeking to prepare themselves for cybersecurity opportunities across the corporation. Many are military veterans with related service experience.

Professionals who have learned on the job often have gaps in their knowledge. In the context of the ISSA Cybersecurity Career Lifecycle (CSLC) [9], some of these individuals are Pre-Professionals since they have not yet worked in the cybersecurity field. Others may be at any point along the CSLC. Their current or potential future positions may be in CIS or in operational groups across the LMC business areas. LMC employees transitioning into cybersecurity or advancing in the field benefit from this approach. The corporation benefits by retaining their knowledge, experience, and commitment.

LMC developed an internal training program, the Common Body of Knowledge (CBoK), to leverage the talent on hand and help fill the gaps. This four-day, in-person course has been presented two to four times each year at several locations, with 20-25 students per session. The course has been offered since 1999. Participants work on in-class exercises in small teams and gain valuable networking opportunities. The course includes a final exam, and credit is recorded in each student’s training record.

The objectives of the LMC CBoK are to:

- Define the common body of knowledge for cybersecurity professionals within LMC
- Provide a framework for understanding the overall role of cybersecurity to support the business, the role of risk-based governance, and types of cybersecurity job functions across the enterprise
- Raise awareness of cyber threats facing industry and personally
- Show the value of “building security in” for systems and how cybersecurity fits within the system development life cycle

The sections of the course include:

- Program overview
- Introduction to information security – role and importance
- Life cycle process – the system development life cycle and cybersecurity activities in each phase
- Risk management – threat, vulnerability, and risk identification and mitigation, including a team exercise
- Security policy and requirements – the role of security policy for an organization, the importance of security requirements for a system, and the relationship of requirements with policy and architecture
- System security – fundamentals of computer and database security, operating modes, and basic technologies; includes a team exercise
- Introduction to cryptography – overview of symmetric and asymmetric cryptography concepts, implementation, and usage

- Network security – overview of network security fundamentals and technologies to make networks more resistant to attack
- Security architecture – basics for designing a secure system architecture, including trade-offs among security, cost, and convenience; includes a team exercise
- Risk management framework – introduces certification and accreditation of systems for USG customers and USG regulations for contractors
- Legal and homeland security issues – introduces cybersecurity- and privacy-related laws, regulations, and policies (primary focus on USG and US state laws) and European Union privacy legislation
- Disaster recovery – overview of business continuity and information technology disaster recovery planning; includes a team exercise

Although the LMC CBoK course parallels the domains in the CISSP Common Body of Knowledge [10], it is not intended as a preparation course for the CISSP or other certification examinations. It provides a foundation for students who eventually attain the CISSP and other certifications. For certain positions that directly support US Department of Defense (DoD) systems, DoD regulations require designated professional certifications [11]. The foundation gained through the CBoK enables LMC participants who need certification to start their path toward it.

## Challenges and measures of success

The LMC CBoK course has achieved significant success in developing and retaining cybersecurity talent. The main challenges have been funding for attendees and keeping the course up-to-date in a rapidly changing field. The Corporate Information Security (CIS) Education and Awareness team sponsors the course and improves it continuously, based on student feedback and subject matter expert input. Each student's department must cover an internal cost for course tuition plus travel, which has been a challenge for some attendees. CIS has considered offering the course virtually, but has kept the face-to-face format with several instructors sharing the teaching during the four days. The live format enables small-group teamwork on problem-solving exercises. Students have consistently noted the value of this format. Students evaluate each section of the course and each instructor as well as the course overall. With the large number of students who have taken the course—over 1,000 since 1999—this feedback has consistently shown strong course effectiveness and provided many ideas for improvement.

## Conclusion

Lockheed Martin Corporation's Common Body of Knowledge course is a model for internal cybersecurity training programs. With a record of success of over 15 years, it enables LMC to leverage its diverse workforce by preparing current employees for near-term or eventual cybersecurity job roles. The program is an integral part of talent sourcing and talent

management. It strengthens the culture and benefits the corporation and the employee.

## References

1. Colm Gorey, "Intel Report Finds Global Cybersecurity Talent Shortage," Silicon Republic – <https://www.siliconrepublic.com/jobs/cybersecurity-report-intel-csis> (accessed July 28, 2016).
2. Information Systems Security Association, Cybersecurity Career Lifecycle, <http://www.issa.org/?page=CSCL> (accessed July 26, 2016).
3. Certified Information Systems Security Professional (CIS-SP), International Information Systems Security Certification Consortium (ISC)<sup>2</sup> – <https://www.isc2.org/cissp/default.aspx> (accessed July 26, 2016).
4. (ISC)<sup>2</sup>, Concentrations – <https://www.isc2.org/concentrations/default.aspx> (accessed July 26, 2016).
5. Information Systems Audit and Control Association (ISACA), Certifications – <http://www.isaca.org/CERTIFICATION/Pages/default.aspx> (accessed July 26, 2016).
6. (ISC)<sup>2</sup>, Certifications – <https://www.isc2.org/credentials/default.aspx> (accessed July 26, 2016).
7. SANS (<https://www.sans.org/>) and GIAC (<http://www.giac.org/certifications/categories>) (accessed July 26, 2016).
8. (ISC)<sup>2</sup>, Certifications – <https://www.isc2.org/credentials/default.aspx> (accessed July 26, 2016).
9. Security Career Lifecycle, ISSA – <http://www.issa.org/?page=CSCL> (accessed July 26, 2016).
10. (ISC)<sup>2</sup>, CISSP Domains – <https://www.isc2.org/cissp-domains/default.aspx> (accessed July 28, 2016). The Lockheed Martin Corporation (LMC) Common Body of Knowledge (CBoK) is supported only internally within LMC and distinguished from the (ISC)<sup>2</sup> CISSP Common Body of Knowledge trademarked as CBK. (See also Gordon, Adam, ed., *Official (ISC)<sup>2</sup> Guide to the CISSP CBK*, 4th ed. (Boca Raton, FL: CRC Press, 2015).)
11. US Department of Defense (DoD) Directive 8140.01, Cyberspace Workforce Management (2015) – [http://www.dtic.mil/whs/directives/corres/pdf/814001\\_2015\\_dodd.pdf](http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf) (replaced DoD Directive 8570.01). Reference (d) of DoD Directive 8140.01 cites DoD Directive 5144.02, DoD Chief Information Officer; and it is under this authority that DoD Manual 8570.01M, Information Assurance Workforce Improvement Program (<http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>, updated Nov. 10, 2015) was issued and is still in force. DoD Manual 8570.01M specifies cybersecurity job roles and certification requirements. The DoD lists the approved baseline certifications at <http://iase.disa.mil/iawip/Pages/iabaseline.aspx> (all accessed July 28, 2016).

## About the Author

Jeff Fenton, CISSP, ISSEP, ISSMP, CISM, CRISC, CIPP/US, GBLC, CBCP, is a Sr. Staff Cybersecurity Governance, Risk, and Compliance Analyst with Lockheed Martin's Corporate Information Security organization. He may be reached at [jeff.fenton@lmco.com](mailto:jeff.fenton@lmco.com).





Certified Cloud  
Security Professional

# **Have confidence in your cloud security knowledge.**

Become a CCSP and lead your organization to the cloud.

## **Be a leader in the field.**

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



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

**Download the CCSP Exam Outline:**

[cert.isc2.org/ccsp-exam-outline](http://cert.isc2.org/ccsp-exam-outline)

# The Role of the Adjunct in Educating the Security Practitioner

By Karen Quagliata – ISSA member, St. Louis Chapter



**The cybersecurity industry faces a shortage of qualified professionals. Part of the solution is to better deliver cybersecurity education in colleges and universities. The purpose of this article is to equip cybersecurity professionals working as adjunct instructors with resources to deliver a more efficient and effective class.**

## Abstract

The cybersecurity industry faces a shortage of qualified professionals. Part of the solution is to better deliver cybersecurity education in colleges and universities. While other professionals have addressed the issue by proposing a formal university curriculum, this article approaches the subject from the perspective of professional security personnel teaching as adjunct instructors. The purpose of this article is to equip cybersecurity professionals working as adjunct instructors with resources to deliver a more efficient and effective class.

A key battle in the cybersecurity war today is not being fought with firewalls and encryption. It is not being fought between cybersecurity professionals and cybercriminals. And it is not being fought in corporate networks and the Internet. No, this struggle is between academia and the information security profession. It is being fought in the classroom.

## Challenges

The cybersecurity industry continues to fall short of qualified professionals. Prominent information security organizations have stated that the shortage is real. For example, (ISC)<sup>2</sup> predicts that the cyber world will be short 1.5 million cybersecurity professionals by 2020.<sup>1</sup> Furthermore, Enterprise Strategy Group (ESG)<sup>2</sup> research shows that 28 percent of organizations

have a “problematic shortage” of IT security skills.<sup>3</sup> Meanwhile, as a society we are living in the world of the Internet of Things and ransomware. The threats are numerous, the criminals are resilient, and the rewards are rich.

The US Bureau of Labor Statistics projects great growth in the computer and mathematical occupations, which include cybersecurity.<sup>4</sup> In fact, they project that this group of industries will produce more than 1.3 million job openings within the next six years. This equates to an 18 percent increase, which they label as faster than average. For information security analysts, the outlook is even better. It is expected that this occupation will grow at a rate of 36.5 percent. The bureau attributes this fast growth to the increased use of electronic medical records and mobile technology.

However, some of the greatest growth areas come with higher educational requirements as illustrated in table 1. The bureau reports that the fastest growing occupations within the business and financial operations sectors will require at least a Bachelor’s degree. For the computer and mathematical occupations the educational requirements are even higher. As seen in table 2, the bureau projects that most of the new jobs occurring in this group will require a master’s degree.

## Solutions

The shortage of qualified cybersecurity professionals is a complex problem, which means there is no easy answer. One of the issues that must be addressed is properly educating a cybersecurity workforce. In their 2014 article, “Application of Pedagogical Fundamentals for the Holistic Development of

1 Jon Oltsik, “Creating a Cybersecurity Center of Excellence,” Network World (2015) – <http://www.networkworld.com/article/3016593/security/creating-a-cybersecurity-center-of-excellence.html>.

2 Enterprise Strategy Group – <http://www.esg-global.com/>.

3 Jon Oltsik, “Creating a Cybersecurity Center of Excellence,” Network World (2015) – <http://www.networkworld.com/article/3016593/security/creating-a-cybersecurity-center-of-excellence.html>.

4 Bureau of Labor Statistics – <http://www.bls.gov/opub/mlr/2013/article/occupational-employment-projections-to-2022.htm>.

Education level	Employment		Projected change, 2012-2022	
	2012	2022	Number	Percent
Bachelor's degree	5,344.3	6,131.4	787.1	14.7
High school diploma or equivalent	1,809.7	1,921.4	111.7	6.2
Postsecondary nondegree award	13.5	12.8	-0.7	-5.3

Source: US Bureau of Labor Statistics

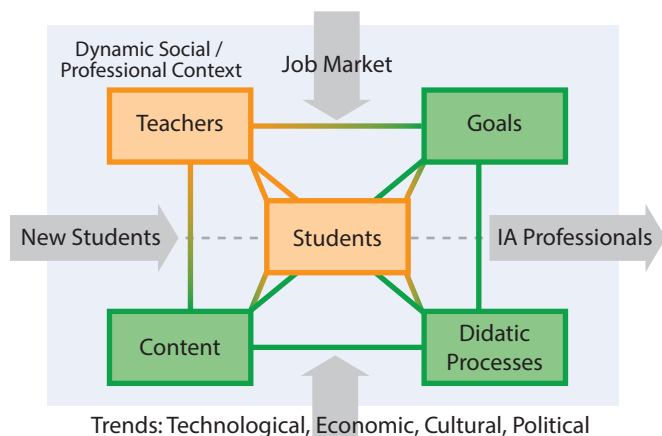
**Table 1 – Business and financial operations occupations employment by educational requirement, 2012 and projected 2022 (employment in thousands)**

Education level	Employment		Projected change, 2012-2022	
	2012	2022	Number	Percent
Bachelor's degree	2,893.1	3,415.2	522.1	18.0
Some college, no degree	547.7	658.5	110.8	20.2
Associate's degree	316.1	356.6	40.6	12.8
Master's degree	31.1	39.2	8.2	26.3
Doctoral or professional degree	26.7	30.8	4.1	15.3

Source: US Bureau of Labor Statistics

**Table 2 – Computer and mathematical occupations employment by educational requirement, 2012 and projected 2022 (employment in thousands)**

### KBP Pedagogical Model for Information Assurance Curriculum Development



**Figure 1 - The KBP Pedagogical Model: CIAC as a pedagogical system**

Cybersecurity Professionals,” authors Barbara Endicott-Popovsky and Viatcheslav Popovsky provide a wealth of information for universities looking to develop a formal curriculum for information assurance education.<sup>5</sup> Figure 1 illustrates the Kuzmina-Bespalko-Popovsky (KBP) Pedagogical Model developed at the Center for Information Assurance and Cybersecurity (CIAC) at the University of Washington.<sup>6</sup> The model takes into consideration such influences on education as the current job market as well as technical, economic, cultural and political trends.

5 Barbara Endicott-Popovsky and Viatcheslav Popovsky, “Application of Pedagogical Fundamentals for the Holistic Development of Cybersecurity Professionals,” ACM Inroads (2014 March) – <https://niccs.us-cert.gov/sites/default/files/documents/files/p57-endicott-popovsky.pdf?trackDocs=p57-endicott-popovsky.pdf>.

6 Ibid.

As seen in figure 2, the KBP model is a multi-discipline approach to information assurance. Multiple schools within the university play a role in educating the security professional. They include the business school, the IT school, and the law school.<sup>7</sup>

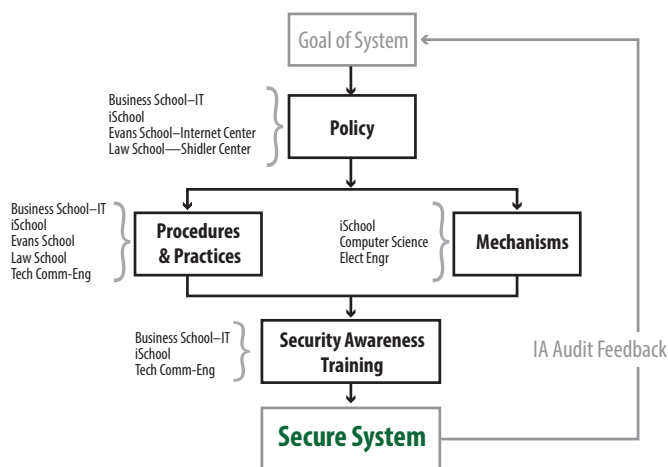
### Education transformation

Such formal approaches to education delivery as the KBP model are vital to the cybersecurity workforce. However, they rely on a more traditional education delivery model. What is becoming more evident, though, is that higher education is undergoing a transformation. That transformation is a move from a staff of tenured professors with degrees in education to the use of adjunct instructors who are often professionals working in the industry. For a multitude of reasons, colleges and universities are now relying more heavily on adjunct instructors. In fact, in 2014 adjuncts made up more than 70 percent of all college and university faculty.<sup>8</sup> Adjunct instructors teach classes on a contract basis. Often a master’s degree in the subject that they will teach and professional experience are the main requirements. They can be trained teachers, but many are individuals who work in a given profession full-time and teach part-time. It is the latter category where the cybersecurity world must focus.

It is the responsibility of cybersecurity professionals to teach cybersecurity courses in an effective and efficient manner. Part of the problem, though, is that often a cybersecurity adjunct is handed only a course name, brief course description, and textbook name along with his/her contract. In some cases another teacher who previously taught the class will share

7 Ibid.

8 J. Fruscione, “When a College Contracts ‘Adjunctivitis,’ It’s the Students Who Lose,” PBS Newshour - <http://www.pbs.org/newshour/making-sense/when-a-college-contracts-adjunctivitis-its-the-students-who-lose/>.



**Figure 2 – Multi-disciplinary approach to information assurance**

his/her syllabus and notes with the cybersecurity adjunct. Predictably, the results can be varying degrees of class quality.

## Recommendations

Cybersecurity professionals teaching as adjuncts need a strong support system of resources in the form of professional organizations, industry research and publications, and assistance from experienced cybersecurity adjuncts. Figure 3 shows the suggested model needed to produce an effective adjunct-led cybersecurity classroom.

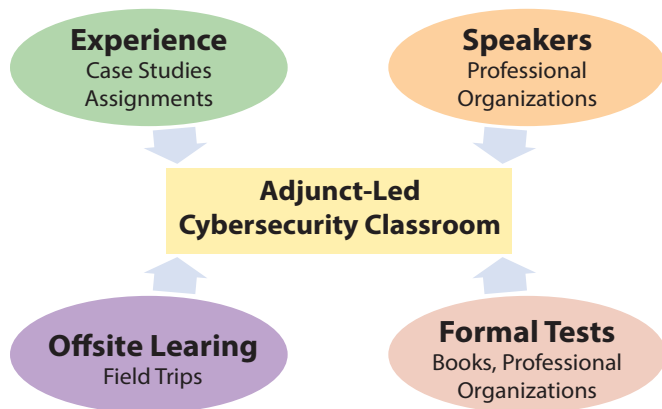


Figure 3 – Adjunct-led cybersecurity classroom model

The following are some recommendations for cybersecurity professionals who are entering the world of adjunct teaching.

### Topics

Be sure to cover the key topics and pain points of the security industry today. Sure, the (ISC)<sup>2</sup> Common Body of Knowledge (CBK)<sup>9</sup> is a great foundation to build the class, but do not stop there. Go beyond the CBK basics—address the reality of implementing security in a corporate setting, address the struggle of trying to implement a security culture when senior leadership is lukewarm (at best) to the idea, address funding and threat landscapes specific to industries.

- Be sure to address the sometimes forgotten risk areas such as third-party vendor management. Data breaches that can be attributed to third-party vendors are still occurring. For example, a 2015 study by the Ponemon Institute shows that 39 percent of respondents attributed their healthcare organization's data breach to a third-party issue.<sup>10</sup>
- Adjunct instructors should certainly discuss any recent data breaches in their classes, but they should do so in an analytical manner. For example, compare three major data breaches and identify any similar aspects (compromised credentials, third-party backdoors, unpatched systems, etc.)
- Adjunct instructors should use industry resources to address key aspects of cybersecurity, such as the Verizon

Data Breach Investigations Report<sup>11</sup> and Ponemon Institute's Cost of a Data Breach Report.<sup>12</sup> These two free resources will not only help the adjunct address causes of breaches, but also how much they will cost an organization.

- Adjunct instructors owe it to their students to address certifications. Students of higher education are painfully aware of the cost of a degree. Some may question whether it is better to forgo the degree and just pursue the certification route. Share a list of some of the more in-demand security certifications and what is required to obtain them. Go the extra mile and study the want ads to see what certifications employers want their candidates to have.

### Tests

Strongly consider using standardized tests for introductory security classes only. It can be assumed that at higher course levels the students already have a firm grasp of basic security topics, such as bios, authentication methods, basics of encryption, etc. At the higher level courses adjunct instructors should be looking for analytical skills in their students. Writing in a clear, concise, analytical manner is vital to any industry, including information security.

### Assignments

Adjuncts should make their assignments as realistic as possible. The goal of education is to expand the mind, but it should also prepare students for the real world. A good way to make realistic assignments is to draw upon actual work experiences, or use prewritten case studies. One approach is to propose a business problem that must be solved by IT. Ask the students to research and propose a solution, complete with a cost summary and risk assessment. Adjuncts can expand upon that assignment by instructing the students to present the solution both to a technical audience and a business audience. Another possible assignment is to have students on a weekly basis choose a topic in security news and write a summary. While not an overly complex assignment, it forces students to get into the habit of staying abreast of current issues and topics in the industry. It also helps students hone their writing skills.

### Textbooks

If the university does not already have a textbook in mind for the class, then the adjunct should consider using certification study guides. These resources lend themselves to a good foundation because of the breadth and depth of the material they cover.

### Professional organizations

The classroom is also a good platform for encouraging students to consider how professional organizations, such as

9 (ISC)<sup>2</sup> Common Body of Knowledge – <https://www.isc2.org/cbk/default.aspx>.

10 Ponemon Institute, Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data Report – [https://iapp.org/media/pdf/resource\\_center/Ponemon\\_Privacy\\_Security\\_Healthcare\\_Data.pdf](https://iapp.org/media/pdf/resource_center/Ponemon_Privacy_Security_Healthcare_Data.pdf).

11 Verizon Data Breach Report – <http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/>.

12 Ponemon Institute's Cost of a Data Breach Report – <http://www-03.ibm.com/security/data-breach/>.

# Data Protection

## With Management, Speed and Trust

**TRANSPARENT ENCRYPTION**  
Database and Files Unix, Windows, Linux

**APPLICATION ENCRYPTION**  
Format Preserving and Field-Level

**CLOUD ENCRYPTION GATEWAY**  
Box, Amazon S3 for Cloud Storage

**VAULTLESS TOKENIZATION**  
Dynamic Data Masking with REST APIs

**ENTERPRISE KEY MANAGEMENT**  
Secure KMIP, TDE Keys, Certificates

ISSA, can help them at any stage of their careers. The adjunct should provide a list of website links to pertinent organizations. The adjunct can also invite presidents of local chapters to speak during a class, or ask permission for students to come to a future event on a trial basis.

### Innovation

Adjuncts should try to go beyond the typical lecture. Information security is a vibrant, constantly changing industry. Traditional lectures do not do it justice. While it is not always possible to avoid a lecture while speaking about the vulnerabilities of a kernel, there are other opportunities to educate without producing glazed stares.

- **Field trips** – Adjuncts should take the education outside of the classroom. Even professionals working in the industry welcome a field trip. Reach out to local law enforcement to see if the class can visit a forensics lab, or if a local company will allow students to view its network monitoring system.
- **Guest speakers** – Guest speakers can also provide an innovative way to impart knowledge. No matter how exciting an adjunct may be as a speaker, students always seem to pay more attention to a guest speaker. Adjuncts can use a guest speaker to reinforce the topic of the day. For example, if the class discussion is authentication, the adjunct can bring in an expert on biometrics. Sources for speakers are abundant. Adjuncts can use professional organizations and/or colleagues as a source for speakers. Local law enforcement can be another source. Finally, with web conferencing there is no geographical boundary.
- **Video** – Adjuncts should not be afraid to incorporate video into their lectures. YouTube provides a plethora of security-related videos and instructions that will go beyond the typical lecture. There are also plenty of free webinars available from vendors and professional organizations. Along those lines, the adjunct can have students play free interactive phishing games available online.

### Implications for professional security organizations

The changing dynamics of the information security industry and the higher education system are providing a perfect storm for professional security organizations to play a greater role in promoting and supporting the profession. Professional security organizations, such as ISSA, can play a vital role in helping to ensure the level of quality delivered by security professionals teaching in an adjunct capacity. Professional security organizations can be a repository of resources to help the new—or established—adjunct instructor. Some of the possible ways that organizations can help include:

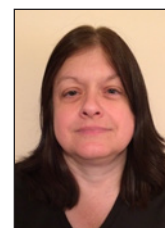
- **Classroom material** – Professional security organizations can solicit their members to submit case studies, test questions, and project ideas to their local chapters to help establish a repository of classroom material. Participation can be counted toward CPEs.
- **Speaker’s bureau** – Professional security organizations contain a wealth of experience. Organizations can establish a speaker’s bureau to help bring some of that experience to the classroom. The local chapter can establish a repository of speakers based on their area of expertise and availability. Participation can be counted toward CPEs.
- **Mentoring program** – Almost certainly there will be members of a professional security organization who are already working as adjunct instructors. Organizations can establish a mentoring program where experienced adjuncts can help new adjuncts with lesson plans, tips, and effective teaching strategies. Participation can be counted toward CPEs.
- **Textbook recommendations** – Professional security organization members can also provide support to the adjunct community by recommending potential textbooks or supplemental reading material for cybersecurity classes.

### Conclusion

The growing cybersecurity field is expecting its personnel to have terminal degrees. At the same time colleges and universities are relying upon adjunct instructors to help supplement their staff of tenured professors. The result is that cybersecurity programs at colleges and universities are turning to cybersecurity professional to fill adjunct instructor roles. Often cybersecurity adjunct instructors are thrown into the classroom with little support. To help ensure a consistent level of quality of cybersecurity classes, cybersecurity adjunct instructors should follow guidelines outlined in this article. Furthermore, professional security organizations should act as a support system by providing classroom material and experienced professionals.

### About the Author

Karen Quagliata, PhD, PMP, CISA, CISSP, is an information security analyst working in risk management and governance. She is also an adjunct instructor for multiple universities and colleges. Karen can be reached at [Karen.quagliata@gmail.com](mailto:Karen.quagliata@gmail.com).



**ISSA Journal Back Issues – 2015**

Past Issues – digital versions: [click the download link:](#)

ISSA.org => Learn => Journal

- Legal and Regulatory Issues
- The State of Cybersecurity   Physical Security
- Security Architecture / Security Management
- Infosec Tools   The Internet of Things
- Malware and How to Deal with It?
- Privacy   Academia and Research
- Infosec Career Path   Social Media and Security

**EDITOR@ISSA.ORG • WWW.ISSA.ORG**



# Infosec Staffing

By Steve Riess – ISSA member, Chicago Chapter



**This article discusses current employment market conditions for information security professionals.**

## Abstract

This article will discuss current employment market conditions for information security professionals. It will cover insight and possible solutions for employers to find and successfully land the information security professionals they need, and it will also offer suggestions to those thinking about finding a new opportunity.

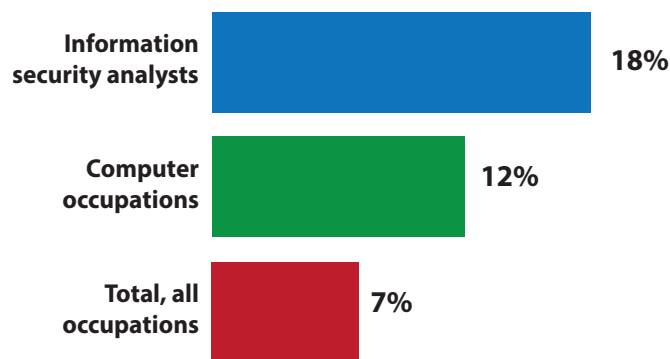
The current demand for information security professionals is at an all-time high, with both corporate America and security product and services companies looking for talent in a market with a very limited supply. It seems most everyone is receiving multiple solicitations for new opportunities on a weekly basis, and everyone has noticed that salary ranges are spiraling upward, sometimes hard to believe. Michael Brown, CEO at Symantec stated in 2015 that “The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million” [1]. *US News and World Report* ranked a career in information security analysis eighth on its list of the 100 best jobs for 2015. They state the profession is growing at a rate of 36.5 percent through 2022 [2]. The US Bureau of Labor Statistics compares the projected growth of information security analysts with computer occupations and all occupations (figure 1).<sup>1</sup>

This is all good, right? Well, not always. And not for everyone.

When market demand for anything far outstrips supply, it usually creates problems that are not immediately or clearly understood. For employers, it usually means they are unable to address the security issues they need, or are demanding far more from their existing team than they really should, which often creates turnover and further exasperates the problem. Or worse yet, because they’re short staffed, they cannot address the vulnerabilities as quickly as they really

## Information Security Analysts

Percent change in employment, projected 2014-2024



Note: All occupations includes all occupations in the US economy.  
Source: US Bureau of Labor Statistics Employment Projections program

Figure 1 - Projected occupation growth through 2024, US Bureau of Labor Statistics

need. According to a 451 Research study, based on responses from more than 1,000 IT professionals primarily in North America and EMEA, security managers reported significant obstacles in implementing desired security projects due to lack of staff expertise (34.5 percent) and inadequate staffing (26.4 percent) [3].

In the case of the information security professional seeking an opportunity, it often translates into typically finding opportunities at environments with an apparent lack of maturity in the security posture/process, opportunities that lack the resources/tools required to properly perform the required tasks, or worse yet, a lack of buy-in from upper management to get “on-board” with what needs to be done. According to Marc van Zadelhoff, general manager IBM Security, the biggest companies in the world are still “highly immature” in key information security domains [4]. This is often the result when you don’t have the necessary resources. The reality is that very few companies have a seasoned, well-traveled security process. That is just the way it is. The security demands and broader security awareness requirements have just moved far too fast to keep up with. There is not going to be any quick remedy to this disparity either. The next major breach that receives widespread media notoriety will only serve to increase the frenzy level.

<sup>1</sup> <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm> - tab-6.

I will address some of these concerns and offer some suggestions to both employers and employees and those looking for new opportunities.

## Employees/staff

### \$\$ should not be the only goal

A workforce shortage means healthy salaries for experienced cyber people. The 2016 Dice report states that the top five IT security salaries are lead software security engineer, chief security officer, global information security director, chief information security officer, and director of security [5]. These positions barely existed six to eight years ago, and now they're some of the top paying positions in all of IT.

**Getting more money is easy to do in today's market, but building a career is not just about changing jobs for more money.**

Getting more money is easy to do in today's market, but building a career is not just about changing jobs for more money. It is also about adding breadth *and* depth to your experience, making you a more valuable (and therefore, better compensated) member of the team. While finding a new "job" is a relatively easy task with the existing market disparity,

simply changing from one employer to the next does not always add to your career. You can easily add to your salary, but adding more money without gaining more or new experience is only a short-term fix. With the constantly shifting security landscape, many professionals have to wonder if they should stay in the same SME area, or should they/would they be able to evolve as well? I think there is a time in your career for each of these. If all you know how to do is work with Splunk, and you keep changing jobs doing the same thing and repeating the same experiences, you will reach a point where your earnings cannot move up. And when that next hot product comes along, you will be left behind. You have to evolve.

### Finding the right fit

Job descriptions are usually "normalized" to comply with salary grade levels or EEOC requirements and often do not really reveal what is required or what you might be expected to do. Most often, this happens because they cannot offer a grade 38 unless it calls for 10+ years experience in the field

and 5+ years experience in technology XXX or YYY, but does anyone really have that? And, quite often, that tool did not really exist in the same manner five years ago, so how can you have that experience? Who was really using Splunk or EnCase more than five years ago?

More often than not, the first communication regarding a new opportunity is not with a peer-level or security leadership-level person but from a recruiter or HR person who only knows what is on the job description and is tasked with "taking your inventory" as it relates to the position. Do you have three cups of IAM and at least two tablespoons of Oracle Identity Manager? Even if you were to ask a finite technical question about the company environment, that first contact person usually would not have a clue. You cannot really start making those discoveries until you have an interview with the person who is capable of answering those questions.

A few smart and dynamic organizations are shifting that model, making the infosec team the first communication with potential candidates. That shift alone says something positive about the organization. The only way you can discover what this position really entails is to go through this process until you finally get to talk to someone who can answer some of your key questions. Do not disregard a possible opportunity just because the job description is vague or contains a single requirement you do not have. Most everyone I have seen hired has some deficiencies as compared to the ideal job description. It is just the way it seems to work these days. Not ideal, but it works.

### How to find growth

If you are seeking a new opportunity, you want to make sure that you clearly understand the environment you are going to be working in, but this understanding is often a secondary consideration for many job seekers because the \$\$ are so seductive. In the most common interview process, the hiring manager outlines what the position will entail and then asks questions during an interview process that reveals your experience, *but typically only as it relates to this job*. Often times, the new employee does not really grasp the entirety of the challenges and shortcomings until being on the job for a few months, and then it is too late. In order to *grow* your career, you need to build upon what you already have. If you take a new role that repeats the same experience you already have, you're not growing your career. Look for opportunities that

## ISSA Special Interest Groups

### Security Awareness

Sharing knowledge, experience, and methodologies regarding IT security education, awareness and training programs.

### Women in Security

Connecting the world, one cybersecurity practitioner at a time; developing women leaders globally; building a stronger cybersecurity community fabric.

### Health Care

Driving collaborative thought and knowledge-sharing for information security leaders within healthcare organizations.

### Financial

Promoting knowledge sharing and collaboration between information security professionals and leaders within financial industry organizations.

**Special Interest Groups — [Join Today!](#) — It's Free!**

ISSA.org => Learn => Special Interest Groups

offer to push your envelope a little, or perhaps in a completely new area of security that complements your existing experience. Build, add, grow. Repeat.

### Be the investigative reporter

The security landscape is changing at a pace faster than ever, and allocating or justifying the resources to address these changes is a constant challenge. Most IT departments (where most security departments still are) are accustomed to working with a budget that covers a typical period of time. New attack vectors demand new responses in a much more timely manner than budgets allow. How do they deal with this? If they do not have the mechanisms in place to address these fast moving situations, what makes you think it is going to change when you come aboard?

What tools are they currently using, how did they arrive at this tool set, and how committed or stuck are they to this investment or portfolio. What was their last security incident, and how did they respond to it? (Hopefully they would not say something like “we have never had an actual incident.”) How mature is their security process, and how can you help that continue to evolve? Is there a succession plan if someone from the team is suddenly gone? If I start working on the security architecture of XXX, can I work on something different when that project is completed? Why are things structured this way, how long have they been like this, and how do they plan to evolve with all the changes happening in security today?

All of these questions, and many more that are similar, have a goal in mind that you already focus on every day...discovery. You should investigate a potential opportunity with much of the same interest and skill you would investigate a breach. Anything less and you are not doing it right. Make your decisions about what you want to discover at a new employer before you even update your resume, and then ask the questions. If they do not know the answers, perhaps you can help provide them once you have joined the organization. If they cannot answer the questions, perhaps you should consider not working there. It is career evolution, not just a job change.

### Your future

In a market like we have today, you can find pretty much exactly what you want to find: closer to home, smaller firm, bigger firm, different tools...whatever. You can find a new opportunity in a different part of the country or in a different industry. No problem. You can take on leadership responsibility, or leave it behind. The key is making employment decisions that BUILD your career, not just about changing jobs. Think about how you want your career to evolve. Write out your discovery questions first, always keep your resume up to date, and keep an eye on your career evolution. Opportunity is knocking all the time.

### Employers/hiring company

A conversation I had with a CISO at a recent security conference in Chicago was very enlightening concerning his situ-



Past Issues – click the download link: [↓](#)

ISSA.org => Learn => Journal

#### JANUARY

[↓](#) Securing the Cloud

#### FEBRUARY

[↓](#) Big Data / Data Mining & Analytics

#### MARCH

[↓](#) Mobile Apps

#### APRIL

[↓](#) Malware Threat Evolution

#### MAY

Breach Reports – Compare/Contrast

#### JUNE

Legal, Privacy, Regulation

#### JULY

Social Media Impact

#### AUGUST

Internet of Things

#### SEPTEMBER

Payment Security

#### OCTOBER

Cybersecurity Careers & Guidance

#### NOVEMBER

Practical Application and Use of Cryptography

*Editorial Deadline 10/5/16*

#### DECEMBER

Security Architecture

*Editorial Deadline 10/22/16*

You are invited to share your expertise with the association and submit an article. Published authors are eligible for CPE credits.

For theme descriptions, visit [www.issa.org/?CallforArticles](http://www.issa.org/?CallforArticles).

[EDITOR@ISSA.ORG](mailto:EDITOR@ISSA.ORG) • [WWW.ISSA.ORG](http://WWW.ISSA.ORG)

ation and the demands of work. He summed it all up in one word: frustrating: bullets on the firing line coming from all directions, C-level management asking questions like never before, and not enough resources to get it all done. He has given up or conceded many times on what his “ideal” security posture would be, is not comfortable with that, but does not have an answer on how to change it quickly. I do not think he is alone with that assessment.

**If HR departments are not finding viable candidates...it is because they are not competing for those candidates.**

The existing staff is holding the fort, but so much more needs to be done. Many companies are often just throwing additional staffing at the problem without understanding where that is going to take them. They often seek to replace the person that just left, rather than assessing what they need now. “We are so busy bailing the boat, we haven’t had time to fix the hole.” “If we can just find the right candidate, everything will be all right.” Everyone is competing

for security resources and the biggest demand is for staff. Smaller firms are seeking utility players, while larger firms are seeking subject matter experts (SME) in one discipline or tool. Security product and security service providers are looking for anyone who has a previous track record in infosec and has the personality to interface at the customer level. The last time a similar market demand existed was during the dot.com boom, where anyone who could even spell C# could get hired.

If HR departments are not finding viable candidates, it is not because they do not care; it is because they are not *competing* for those candidates. They don’t know how. They are probably using the same mechanisms and tools they use to hire admin

staff or accountants, and that just does not work today. Your position, however unique it might be, looks just like all the rest using those mechanisms. It is very easy to be like everyone else. It is very hard to stand out, but this is what you will have to do in order to find the right people.

**How do I find them?**

The US Bureau of Labor Statistics [6] shows the demand is prevalent across the entire US and across most every industry sector, so while it might be comforting that you’re not alone in this difficulty, it doesn’t help you solve the problem.

Most security professionals I know will browse the job sites once in a while just to see what is out there. They will even click on some positions to see what the position entails, and what they are usually seeing does not motivate them to do anything but click *BACK*. The description does not really tell them anything at all. Most major firms have normalized their descriptions to be EEOC compliant, but this is exactly the opposite of what you need to attract top talent. And, if they do have *some* interest, their only option is *APPLY* or *SEND YOUR RESUME*. Well...they do not want to apply but want to find out more about it, but there is not have that option. So they do nothing. You have to give them other options. Providing other options gives you the opportunity to engage them, and engaged people will take the next step or action.

**How do I engage them?**

Advertise everywhere and do not use the standard company job title for the advertisement. Include the actual title somewhere in the text, but make the title descriptive of what the work actually is. Sherlock Holmes – Forensics; Intrusion Detection Genius; Join Our Security Battlefield Team. You then **MUST** provide an alternative to the standard *APPLY HERE* click in order to achieve or provide some positive results. You



**Click here for On-Demand Conferences**

  
[www.issa.org/?OnDemandWebConf](http://www.issa.org/?OnDemandWebConf)

**Security Architecture & Network Situational Awareness**  
2-Hour Event Recorded Live: September 27, 2016

**IoT: The Information Ecosystem of the Future--And Its Issues**  
2-Hour Event Recorded Live: August 23, 2016

**Hacking the Social Grid: Gullible People at 670 Million Miles per Hour**  
2-Hour Event Recorded Live: July 26, 2016

**Legislative Impact: When Privacy Hides the Guilty Party**  
2-Hour Event Recorded Live: June 28, 2016

**Breach Report Analysis – SWOT or SWAT?**  
2-Hour Event Recorded Live: May 24, 2016

**The Sky Is Falling... CVE-2016-9999<sup>(mth)</sup>?**  
2-Hour Event Recorded Live: April 26, 2016

**Security Software Supply Chain: Is What You See What You Get?**  
2-Hour Event Recorded Live: March 22, 2016

**Mobile App Security (Angry Birds Hacked My Phone)**  
2-Hour Event Recorded Live: February 23, 2016

**2015 Security Review & Predictions for 2016**  
2-Hour Event Recorded Live: January 26, 2016

**Forensics: Tracking the Hacker**  
2-Hour Event Recorded Live: November 17, 2015

**Big Data–Trust and Reputation, Privacy–Cyberthreat Intel**  
2-Hour Event Recorded Live: Tuesday, October 27, 2015

**Security of IOT–One and One Makes Zero**  
2-Hour Event Recorded Live: Tuesday, September, 22, 2015

**A Wealth of Resources for the Information Security Professional – [www.ISSA.org](http://www.ISSA.org)**

might consider another email click/link to ask a question directly to the CISO, which is an email alias or comes to the inbox of the hiring manager. The manager can then reply directly, or have someone from HR reply, but make sure you give the interested party a mechanism to continue the dialog directly to the manager, either via the HR person or through that original clickable link. If she has to go find that job posting again, she will not move forward. You want to engage a dialog, not ask (yet) for a resume.

Set up a 15-minute webinar or toll-free dial-in conference number that happens every week on Tuesday at 12:30pm for anyone interested. Publish that prominently in your ads, and have the hiring manager talk about YOUR opportunity and the culture of their environment, as well as answer questions each week. But make no requirement for callers to identify who they are upon login. If the subject of salary comes up, be prepared to answer with exact information, or merely state that you will modify the salary for the right candidate. Advertise everywhere—job sites, professional associations, conferences, etc. Advertise everywhere, advertise everywhere, advertise everywhere.

A very successful mechanism is a referral bonus program for your employees. Your infosec staff know other infosec people who know other infosec people. Six degrees of separation [7] is the theory that everyone is six or fewer steps away, by way of introduction, from any other person in the world so that a chain of “a friend of a friend” statements can be made to connect any two people in a maximum of six steps. Why do you think LinkedIn works so well?

If you are not offering an employee referral bonus of \$2,500 – \$5,000, you are missing opportunities. And make sure you make the same or similar offer to your vendor reps. If they sell to infosec, they know infosec people. Some firms have started offering other incentives like Starbucks or dinner gift certificates to employees for just referring a qualified resume—no requirement of hire, just the action of a referral. It helps motivate your staff to keep these things in mind. Referred candidates will already have a level of interest because someone they know has initiated this process. That by itself changes the whole dynamic.

### The Interview process

I have seen more great candidates slip away because of the interview process than any other cause. I tell my clients the same thing. If they cannot be timely and on top of the process, I will not work for them. I know sometimes that change is really hard for an organization, but if they are not willing to bypass the usual same-o same-o process in order to address the critical need in a timely manner, they will not get what they are looking for.

When you start the interview process, you should make it clear to potential candidates how your process works and what the expectations might be from a time investment perspective: two 30-minute phone interviews and two one-hour in-person interviews or one phone interview and one in-per-

son interview. Whatever the process is, make sure you outline it at the start. Having someone from HR do an inventory interview and getting back to the candidate a week later will not get you anywhere. Your prospect has already forgotten or lost interest. If HR comes first (I would not recommend having HR as the first communication), then you must get back about the next step right away. Someone has to respond within 24-48 hours of every communication from a candidate, either with the next step in the process or a polite “no thank you” email. The candidate emails you his resume, you must respond. He asks you a question via the previously discussed mechanisms, you must respond. If you want to invite him in for an interview, send two to four possible time slots. DO NOT just send an email asking when he might be available. If

## Why Advertise in the ISSA Journal?

Access nearly 11,000 ISSA members, of which 74 percent are **CISO/Security Leaders, Senior Executives, and Mid-Career Professionals** either making decisions or highly influencing decisions on products and services to evaluate or purchase.

The ISSA Digital Edition of the Journal boasts a minimum 56 percent open rate!”

For monthly Journal themes, [click here!](#)  
Or visit [www.ISSA.org](http://www.ISSA.org) => Learn => Journal

### For a limited time:

- » Purchase a series of 6 quarter-page digital ads in the ISSA Journal, and receive 1 ISSA Home Page one-month web banner—**A \$1,000 VALUE!**
- » Purchase a series of 6 half-page digital ads and receive 1 ISSA Home Page three-month web banner— **A \$3,000 VALUE!**
- » Purchase a series of 6 full-page digital ads and receive 2 Biweekly E-News Web Banner ads free —**UP TO \$6,000 VALUE!**

ISSA’s special advertising “Concierge Service” is your one-stop shop to manage all your ISSA advertising needs. For more information, email ISSA Director of Business Development at [jcavarretta@issa.org](mailto:jcavarretta@issa.org).

ISSA  
JOURNAL

**IT'S GOOD FOR BUSINESS**

Learn More Today

Contact Joe Cavarretta  
[jcavarretta@issa.org](mailto:jcavarretta@issa.org)

he sends you alternatives to those originally offered, you must respond. Remember, you are in competition with everyone else out there looking for the same talent; if you cannot keep them engaged, they will just float away off to another opportunity. There is far too much “noise” and activity out there to distract them.

### Hire potential

Purely my opinion, but I think too many firms are trying to hire someone who is an absolutely exact fit for their open position and ignore all of the other qualities that make up a good employee. Granted, your choices are fewer now than ever before and the stakes are high, but I still think most firms are best served by hiring the right employee rather than just the right technical skill. If she is the right employee, she will gain the technical expertise to continually perform better and better. Just hiring the right skill has limitations, and can lead to problems on the team and increase turnover. I know of one firm that hired a new CISO and within 60 days the two security managers under the CISO quit, and then the CISO quit six months later. Not a good hire, but he certainly fit the specs.

### Conclusion

I like to think of recruiting in terms of fishing anecdotes. If you’re not “catching any fish,” and you keep going to the same place with the same equipment and the same bait, you’re probably going to get the same results. In order to attract and engage a candidate’s attention, you have to do something different. Your challenges/environment/culture may not be entirely unique, but they’re definitely different than most. That’s what you have to attract candidates, so flaunt it.

### References

1. Steve Morgan, “Cybersecurity Job Market to Suffer Severe Workforce Shortage,” CSO Online – <http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html>.
2. “Information Security Analyst Overview,” *U.S. News and World Report* – <http://money.usnews.com/careers/best-jobs/information-security-analyst>.
3. Richard Harris, “New Report Highlights Wide Ranging Cybersecurity Challenges,” *App Developer Magazine* – <https://appdeveloper magazine.com/3159/2015/9/2/New-Report-Highlights-Wide-Ranging-Cybersecurity-Challenges/>.
4. Warwick Ashford, “World’s biggest companies lack maturity in security, says IBM Security,” *ComputerWeekly.com* – <http://www.computerweekly.com/news/450281218/Worlds-biggest-companies-lack-maturity-in-security-says-IBM-Security>.
5. Steve Morgan, “Cybersecurity job market to suffer severe workforce shortage,” CSO - <http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html>.

6. “Occupational Employment Statistics,” The US Bureau of Labor Statistics – <http://www.bls.gov/oes/current/oes151122.htm#st>.
7. “Six Degrees of Separation,” Wikipedia – [https://en.wikipedia.org/wiki/Six\\_degrees\\_of\\_separation](https://en.wikipedia.org/wiki/Six_degrees_of_separation).

### About the Author

Steve Riess has been doing information technology staffing for over 25 years. Steve is an active member in the local ISSA Chicago Chapter, and is also a member of ISACA and AITP, attending conferences and learning opportunities on a continuous basis. He may be reached at [SRiess@nu-waysearch.com](mailto:SRiess@nu-waysearch.com).





**ISSA  
STORE**

Easy and  
Convenient!

www.issa.org/store/default.asp

















**Computer Bags**  
**Short-Sleeve Shirt**  
**Long-Sleeve Shirt**  
**Padfolio**  
**Travel Mug**  
**Baseball Cap**  
**Fleece Blanket**  
**Proud Member Ribbon**  
**Sticky Note Pads** (12 pk.)

We’ve stocked our shelves with ISSA merchandise featuring our logo.  
  
 Visit our online store today – it’s easy and convenient to securely place your order and receive great ISSA-branded items.  
  
**Just click the links!**

Place Your Order Today:  
ISSA Store !



# Half protected is half not.

Full identity security for the enterprise

Centrify provides a unified solution for securing and managing privileged users' identities. Centrify leverages an organization's existing identity infrastructure to enable identity consolidation, privilege management and auditing for security and compliance, and a simplified identity infrastructure for IT.



[www.centriky.com](http://www.centriky.com)

Free trial: [www.centriky.com/free-trial](http://www.centriky.com/free-trial)  
Learn more: [www.centriky.com/resources](http://www.centriky.com/resources)

# DIGITAL DANGER ZONE

ISSA 2017 INTERNATIONAL CONFERENCE



October 10-11, 2017

San Diego, California



#ISSAConf

 **ISSA** International  
**CONFERENCE**