InfoSecurity PROFESSIONAL
A Publication for the (ISC)² Membership

COMMUNITY!
A QUARTER CENTURY OF BUILDING INFORMATION SECURITY CAREERS AND CAMARADERIE

Privacy + Security
Ransomware on the Rise
Tapping into Threat Intelligence
A 'Colossus' Problem

SEPTEMBER/OCTOBER 2014
FOCUS 14
SECURITY CONFERENCE

Las Vegas | October 27–29, 2014
The Venetian and the Palazzo Congress Center

Join us for the McAfee FOCUS 14 Security Conference:
Empowering the Connected World, brought to you by Intel Security.
Use promo code FOCUS214 to get $100 off the prevailing rate.

FOCUS 14 will offer a program packed with valuable and timely content on the changing security landscape. Participate in technical deep dives and breakout sessions to help you better manage the security networks within your organization.

Use promo code FOCUS214 when registering to get $100 off the prevailing rate.

Visit http://mcafe.com/focus to learn more

Conference Highlights

- 75+ technical breakout sessions: Learn about the latest security innovations from McAfee technical experts, our customers, partners, and other like-minded professionals.
- Networking: Engage with some of the best minds in the industry—IT managers and executives, McAfee Labs researchers, and product specialists.
- Other conference highlights: Benefit from Targeted Group Meetings, a partner expo, CPE credit and training opportunities, a private concert by Def Leppard on the final evening, and much more.

www.McAfee.com/FOCUS14

Follow us at #McAfeeFOCUS

intel Security
# Features

## Professional Development

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Brief Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>The InfoSec Professional: 25 Years in the Making</td>
<td>As (ISC)² celebrates its silver anniversary, we look at what has happened since its first credential—the CISSP—was introduced.</td>
<td>Anne Saita</td>
</tr>
</tbody>
</table>

## Malware

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Brief Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Data Held Hostage</td>
<td>Despite recent efforts to disrupt malware developers using extortion for financial gain, ransomware is on the rise.</td>
<td>Tom Tollerton</td>
</tr>
</tbody>
</table>

## Risk Management

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Brief Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>Getting 'Left of the Hack'</td>
<td>It’s easy to become so focused on what’s happening inside your network that you neglect the outside actors that may be preying on your weaknesses. Learn how to know thy enemy better.</td>
<td>Randy Borum</td>
</tr>
</tbody>
</table>

## Data Security

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Brief Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Keeping Big Data Within Your Control</td>
<td>Learn how to best manage the risks and rewards of the vast amounts of data being generated as the information economy accelerates.</td>
<td>Colleen Frye</td>
</tr>
</tbody>
</table>

---

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

Opportunities to 'Spread the Word'

Twenty-five years ago, I was a young mother teaching Eskimos and Aleuts, among many others, on an Alaskan island. Little did I know, thousands of miles away, a consortium was convening to help shape an industry. That group, of course, would become (ISC)².

The information security professional of today has far different duties and expectations than the one recruited into the field in the late 1980s and early 1990s—before widespread adoption of the personal computer and the World Wide Web. Today’s information security professional not only must manage the growing risks arising from the latest technologies, but keep up with privacy rules and regulations, and speak the business language.

Today’s practitioners also are evangelists, helping to spread the word on privacy and security best practices. Each October provides an opportunity to better educate our communities as part of National Cyber Security Awareness Month (NCSAM). The now-international movement is widely embraced at (ISC)².

You’ll no doubt be seeing more consumer- and industry-specific articles, blog posts, podcasts, and videos featuring (ISC)² leaders and members during NCSAM. We’re kicking off NCSAM at our annual Security Congress event. Each week during the month of October, we’ll distribute a list of cybersecurity awareness tips for children, parents, seniors, homeowners, CEOs, and software developers.

I’ll be attending ASIS 2014/(ISC)² Security Congress in Atlanta this month and hope to meet some of you in person. Thank you all for doing your part to keep us all a little safer.

Anne Saita, editor-in-chief, lives and works in Southern California.

Anne Saita, editor-in-chief, lives and works in Southern California.

Editor's Note

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

ADVERTISER INDEX

McAfee .................................................2 Trend Micro ..............................................24
Security Compass ..............................5 Promisec .................................................29
Walden University ..............................7 Guidance Software .................................32
Bit9 ....................................................9 Symantec ...............................................38
Microsoft ........................................11 (ISC)² ..................................................39
Capella University .........................15 CA Technologies .................................40
(ISC)² ..................................................21

© Rob Andrew Photography

© Rob Andrew Photography
Do you have the training & skills to hack Security Compass’s Battle Room?

Battle School is an interactive and competitive program designed to teach you about the physical and technical attacks one could attempt on a company’s security system. These challenges will prepare and train you to compete in the battle room hack – if you dare try.

There are four divisions – physical, web, network, and mobile to test your ability and knowledge of security hacking. After successfully completing the four challenges you will raise your chances of conquering the battle room.

**PHYSICAL DIVISION**
Learn how to hack physical infrastructures such as door locks, key pads, and logic circuits.

**WEB DIVISION**
Gain an understanding of common website vulnerabilities, and common phishing and social engineering tactics that attackers use to try and steal user information.

**NETWORK DIVISION**
Learn about different DDoS attack vectors by having access to a monitoring system – choose an appropriate DDoS attack in order to overwhelm that particular monitor.

**MOBILE DIVISION**
Through different examples you will learn how an NFC enabled phone can be leveraged and how to stay protected.

**BATTLE ROOM**
After gaining skills from the four divisions, you will be able to attempt a hack on the battle room - a safe environment to test your skills.
A MORE ‘APP’ WAY TO SECURE SOFTWARE

SOFTWARE IS THE lifeblood of technology. Regardless of where we live and in which industry we work, the devices, tools, and environments we rely on daily all function because of the embedded code programmed into a product. Flawed, maliciously manipulated software is nothing new, but the din from dissatisfied customers is growing louder with each massive security breach making headlines. So is the growing influence of (ISC)²’s Application Security Advisory Council (ASAC) (https://www.isc2.org/ASAC/default.aspx), whose members are committed to embedding security throughout the entire software development lifecycle.

In 2010, the council (then a board) was comprised of people from large companies who were asked to evangelize secure software within their companies. But with the advent of the Internet of Things, even the smallest vendors now can have a huge impact.

So we’ve expanded the ASAC to include more people with a passion for secure software assurance. That includes people like Mikko Varpiola, a security researcher who is an expert on “fuzz testing”—a technique that is commonly used to test for security problems in software.

Leading the ASAC is (ISC)² Sacramento Chapter Co-Founder and President Tony Vargas, CSSLP, CISSP-ISSAP. Tony was instrumental in creating a large developer security awareness program at Cisco Systems. Tony has also taught thousands of school children, parents, and teachers about Internet security through the (ISC)² Foundation’s Safe and Secure Online program.

The council’s work touches every area and is woven into every one of (ISC)²’s certifications (not just the CSSLP®), which means the ASAC is working for all members who create, purchase, use, and sell products and services that run on software.

The list of council members continues to grow as we recruit more people, particularly from Asia and EMEA. ASAC members will promote a culture that values security as a core requirement of software among technology consumers and producers through industry partnerships and advocacy via presentations, white papers, blog posts, articles, and video interviews.

We hope this multimedia approach convinces more companies to stop ignoring security essentials during the software development process just because they are unaware of the requirements and techniques of building security into software. This makes life more difficult when exploited software vulnerabilities lead to stolen identities, fraud, jobs losses, and severe financial hardships.

Our ultimate goal is to make life easier and safer for everyone. People think they can solve security problems with compliance by setting up predefined rules and then following them rigidly. That reduces the risks of breaches, but it doesn’t eliminate them.

I believe secure software will be a reality. We just need to help those with the power and influence to make it happen. That’s what your fellow members on the (ISC)² Application Software Advisory Council are here to do. ✪

Vehbi Tasar is Director of Professional Programs Development. He can be reached at vtasar@isc2.org.
Answer the Call for Cyber Security Experts With an IT Degree From Walden.

• Doctor of Information Technology (D.I.T.)
• M.S. in Information Technology
• B.S. in Computer Information Systems
• And more

Offering specializations such as Cyber Security, Health Informatics, and Software Engineering, our degree programs can give you the skills you need to join the field.

Get Credit for Your Professional Certifications.

• Certified Information Systems Security Professional (CISSP)®
• ISACA Certified Information Security Manager (CISM)®
• Project Management Professional (PMP)®

Explore our programs at WaldenU.edu/cybersecurity.

Visit us at Booth#4951 at (ISC)² Security Congress 2014 in Atlanta Sept. 29–Oct. 2!

Recognized Quality

(ISC)² and the International Association of Privacy Professionals (IAPP) are forming an alliance to foster a global mission that will resonate with professionals in both the privacy and information security realms. While there are similarities between (ISC)² and IAPP, the differences weigh in as pluses for members of both organizations.

“The (ISC)² and IAPP alliance is a dynamic meeting of the minds,” says (ISC)² Executive Director W. Hord Tipton, CISSP, “Along with our shared principles and understanding of our organizations globally, this collaboration will provide added resources and services for our collective members, as well as information security and privacy professionals worldwide.”

The alliance between (ISC)² and IAPP will yield enhanced benefits for members of both organizations, including webinars, jointly hosted events for chapters, and continuing professional education. The relationship will kick off with a joint panel on the convergence of privacy and security at the IAPP conference in March 2015.

Founded in 2000 and headquartered in Portsmouth, N.H., the IAPP is a not-for-profit association with members in 83 countries. The IAPP helps define, support and improve the privacy profession through networking, education and certification. As the largest global information privacy community and resource, IAPP helps practitioners develop and advance their careers and organizations manage and protect their data.

IAPP developed and launched the first broad-based credentialing program in information privacy, the Certified Information Privacy Professional (CIPP), and the Certified Information Privacy Manager (CIPM), the first and only global certification program in privacy program management. The Certified Information Privacy Technologist (CIPT) is also the first and only certification of its kind worldwide. The CIPT is designed for technology professionals so that they can secure data privacy at all stages of IT product and service lifecycles.

The CIPP, CIPM and CIPT are the leading privacy certifications for thousands of professionals around the world who serve the data protection, information auditing, information security, and legal compliance and/or risk management needs of their organizations. Similar to (ISC)², IAPP offers a full suite of educational and professional development services and holds annual conferences that are recognized internationally as the leading forums for privacy policy and practice.

“Through this alliance between IAPP and (ISC)², we will be able to provide a broad spectrum approach to our educational and professional development services and expand our reach on issues related to privacy and information security policies and practices,” says Trevor Hughes, IAPP President and CEO.
MEMBER SPOTLIGHT ON...

WILLIAM NANA FABU

William Nana Fabu, CISSP, came to the United States in 2004 from his native Cameroon, Africa and now works in information security for the financial sector. Working in the U.S.A. in a heavily regulated industry has led him to pay more attention to the weak state of security in Africa, which he says is in an embryonic state at best.

What drew you to the information security profession?

After working as a banking systems integrator and MIS officer for many years in Africa, when I joined the workforce in the U.S., I was ready to explore a challenging and relatively new field in the IT world. Information security was a great choice for me. I was lucky to be offered a job in the identity and access management field and later in the firewall team. I really enjoyed the challenges and rapid changes of the field, and I still do today.

How would you describe the state of information security in your homeland?

It gives me shivers to think there’s no tangible information security program in Cameroon or personnel to put in place some kind of rudimentary security structure. Fortunately,
GLOBAL SPOTLIGHT: (ISC)² COLOMBIA CHAPTER

MEMBERS SEE STRONG INTEREST IN CHILD INTERNET SAFETY

THE BOGOTA-BASED (ISC)² Colombia Chapter, which serves members throughout the country, celebrated its first anniversary on July 30, 2013. The Chapter formed to promote the interest, awareness and training on issues related to information security and ongoing development of professionals working in Colombia.

The Chapter offers members the opportunity to grow professionally, learn new concepts, best practices and technologies, and work in different environments. Colombian Chapter members have the ultimate aim of providing their knowledge and experience in information security to support the Colombian government with programs for the community at large. At present, there are 27 members, with plans to add at least one member a month.

The Chapter has sponsored several events on topics such as challenges in digital investigations; the evolution in security for payment devices; and the new version of the ISO 27001 standard.

On May 29, the Colombia Chapter hosted an event, “Building a Secure Digital Environment for Colombian Children,” sponsored by BBVA and Symantec. The event promoted ways for children to protect themselves while they use the Internet. The main speaker was Col. Freddy Bautista, who heads Cybercrime of the Colombian National Policy. Other speakers included a Ministry of Information and Telecommunications official, an expert in computer law, and a representative from an association dedicated to child protection.

The topic and keynotes proved a popular subject, with the event drawing 130 attendees.

Through its efforts to build a local chapter and gain recognition in the community, Chapter leadership now plans to host monthly conferences and semi-annual events regarding security and privacy.

What impact does this lack of attention in developing countries have on a global scale?

We (the developed countries) look for the best systems, the best algorithms, the best technicians, and the best programs to make sure that our “security bastion” can stand the most challenging attack. But on the other side of the equation is the fast growth of “bad guys” operating outside our walled-up communities. We don’t yet fully grasp the sophisticated threats that exploit the weakest link of our global security model—less developed countries.

What do you suggest be done?

I know we have a shortage of information security professionals within our bastion, but we need to spread the security culture and awareness beyond our own borders and create more “ambassadors” worldwide to empower those with weak or no information security training.

Members of (ISC)² have the resources to share this knowledge. We have the tools to train. We have the tools to build security solutions.

Everything starts with awareness campaigns, followed by training programs that a capable team of professionals need to fight the bad guys before they’ve perfected their damaging techniques and tactics.
ACKNOWLEDGING LEADERSHIP ACHIEVEMENT IN ASIA-PACIFIC REGION

CONGRATULATIONS TO THIS year’s (ISC)² Asian-Pacific Information Security Leadership Achievement recipients, who were honored at a recent gala in Beijing, China.

You can learn more details about each honoree and showcased project at www.isc2.org/isla.

› Senior Information Security Professional Category Showcased Honoree
Dr. Daisuke Inoue - Director of Cybersecurity Laboratory, Network Security Research Institute, National Institute of Information and Communications Technology (Japan)
Showcased Project: DAEDALUS: Novel Alert System based on Large-scale Darknet Monitoring

› Senior Information Security Professional Category Showcased Honoree
Hae-Sul Choi - CEO, WATCH I SYSTEM INC.
Showcased Project: Contribution to Convergence Managed Threat Defense System for Korea Army Cyber Security (South Korea)

› Information Security Practitioner Category Showcased Honoree
Anan Sony - CISSP, CISA, ITIL Expert, manager (Consulting Service Department), ACIS Professional Center Co., Ltd. (Thailand)
Showcased Project: Internet Banking and Mobile Banking Security Assessment

› Managerial Professional for an Information Security Project Category Showcased Honoree
Lal Dias - MBA, MBCS, CITP, chief executive officer, Sri Lanka Computer Emergency Readiness Team, Coordination Centre (Sri Lanka)
Showcased Project: Establishment of Bank CSIRT (Computer Security Incident Response Team) in Sri Lanka

› 2014 Community Service Star
Dr. Yuejin Du - Director, National Engineering Lab for Cyber Security Emergency Response Technology (China)
Community Service Star Project: Cyber Security Public Education Program

For 2025, 4.75 billion people online with 3.75 billion from emerging economies, could lead to three different global scenarios.

Microsoft’s Cyberspace 2025: Today’s Decisions, Tomorrow’s Terrain looks over the horizon, beyond technical trends, and attempts to anticipate future catalysts for change and equip policy makers for tomorrow’s digital landscape.

Download the scenarios that will forecast a global PEAK, PLATEAU, or CANYON for innovation at Cyberspace2025.com
(ISC)² WOMEN ‘POWER UP’ IN SC MAGAZINE LIST

(ISC)² Board member Jennifer Minella (right), and Application Security Advisory Council member Katie Moussouris (below), are among the women listed in SC Magazine’s 10 Women in Security Power Players.

Minella is VP of engineering at Carolina Advanced Digital and, according to the magazine, “one of four principals helping drive business strategy and execution of initiatives ranging from engineering to marketing and communications.”

Moussouris is the chief policy officer of HackerOne, which helps clients with responsible disclosure of vulnerabilities. She told the magazine that she “works toward the public good to legitimize and promote security research to help make the Internet safer for everyone.”

Recognized for their long-term contributions to IT security, the two women are joined by honorees Becky Bace, Lisa Foreman, Stacey Halota, Kristin Lovejoy, Samara Moore, Wendy Nather, Hemma Prafullchandra, and Patricia Titus.

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


“One thing we know for sure: security always comes with a price. It is either privacy, or, most of the time, usability. And it seems that nobody is voluntarily willing to pay this price.”

—SORIN MUSTACA, CSSLP, Product Manager for Avira, from his (ISC)² blog post “Why We Continue to Fail on Cybersecurity”
### 2014 (ISC)² Cyber Security Scholars

**Working to Fill the Gaps in Cyber Security Education**

**Congratulations** to this year’s (ISC)² Foundation Cyber Security Scholars! Here’s a list of recipients for the Women’s, Graduate, and Undergraduate Scholarships. Kudos also to those who earned a Faculty Certification Exam Voucher. To learn more about the Cyber Security student scholars, turn to pages 35-36.

<table>
<thead>
<tr>
<th>Scholarship Awarded</th>
<th>Name</th>
<th>Country of Birth</th>
<th>Institution Enrolled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Women’s</td>
<td>M. Alexis Greenidge</td>
<td>U.S.A.</td>
<td>American Intercontinental University</td>
</tr>
<tr>
<td>Women’s</td>
<td>Sreedevi Sreekandan</td>
<td>India</td>
<td>University of Texas, San Antonio</td>
</tr>
<tr>
<td>Women’s</td>
<td>Shruti Gupta</td>
<td>India</td>
<td>Purdue University</td>
</tr>
<tr>
<td>Graduate</td>
<td>Scott Ruoti</td>
<td>U.S.A.</td>
<td>Brigham Young University</td>
</tr>
<tr>
<td>Graduate</td>
<td>Mark O’Neill</td>
<td>U.S.A.</td>
<td>Brigham Young University</td>
</tr>
<tr>
<td>Graduate</td>
<td>Anna Truss</td>
<td>Turkmenistan</td>
<td>Excelsior College</td>
</tr>
<tr>
<td>Graduate</td>
<td>Lokesh Pidawekar</td>
<td>India</td>
<td>Northeastern University</td>
</tr>
<tr>
<td>Graduate</td>
<td>Chunyue Du</td>
<td>China</td>
<td>Carnegie Mellon University</td>
</tr>
<tr>
<td>Graduate</td>
<td>Cheryl Devaney</td>
<td>U.S.A.</td>
<td>Duquesne University</td>
</tr>
<tr>
<td>Graduate</td>
<td>Pratibha Dohare</td>
<td>India</td>
<td>Carnegie Mellon University</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Saradha Kannan</td>
<td>India</td>
<td>Lewis University</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Christopher Goes</td>
<td>U.S.A.</td>
<td>University of Idaho</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Kyle Murbach</td>
<td>U.S.A.</td>
<td>Rochester Institute of Technology</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Lassine Cherif</td>
<td>Ivory Coast</td>
<td>University of the District of Columbia</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Dulce Gonzalez</td>
<td>Mexico</td>
<td>Governors State University</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Robin Saunders</td>
<td>U.S.A.</td>
<td>River Valley Community College</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Katherine McGinn</td>
<td>U.S.A.</td>
<td>University of Maryland University College</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Fumi Honda</td>
<td>U.S.A.</td>
<td>Stony Brook University</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Rose Reinlib</td>
<td>U.S.A.</td>
<td>University of North Carolina at Charlotte</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Yue Zhu</td>
<td>China</td>
<td>University of Connecticut</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Samantha Houston</td>
<td>U.S.A.</td>
<td>Sam Houston State University</td>
</tr>
<tr>
<td>Undergraduate</td>
<td>Patrick Katamba</td>
<td>Uganda</td>
<td>London Metropolitan University</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Eamon Doherty</td>
<td>U.S.A.</td>
<td>Fairleigh Dickinson University</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Mohamed Kazi</td>
<td>United Kingdom</td>
<td>Higher Colleges of Technology</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Louay Karadsheh</td>
<td>Kuwait</td>
<td>ECPI University</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Tahir Abbas</td>
<td>Pakistan</td>
<td>Lahore School of Accountancy and Finance</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Rizwan Ahmad</td>
<td>Pakistan</td>
<td>Manukau Institute of Technology</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Helio DeCastro</td>
<td>Sao Tome and Principe</td>
<td>ITT-Technical Institute</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Diane Murphy</td>
<td>United Kingdom</td>
<td>Marymount University</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Timothy Perez</td>
<td>U.S.A.</td>
<td>Brandman University</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Vivek Gupta</td>
<td>India</td>
<td>Surendera Group of Institutions, Sri Ganganagar</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Donna Schaeffer</td>
<td>U.S.A.</td>
<td>Marymount University</td>
</tr>
<tr>
<td>Faculty Exam Voucher</td>
<td>Trevor Chandler</td>
<td>U.S.A.</td>
<td>Houston Community College</td>
</tr>
</tbody>
</table>
NEW OPPORTUNITIES FOR INFORMATION SHARING

Perhaps the biggest benefit of being part of the (ISC)² community is the information sharing that takes place, both formally and informally. Whether it is through the ThinkT@nk roundtables and other Security Leadership Series sessions or through the “hallway track” at industry events, we are a community of professionals coming together to elevate the state of the art.

Over the summer months, we have discussed new ways of sharing information among the professional community and new ways to extend that sharing outside of our community. To that end, we are piloting a couple of ideas through the end of the year.

First up, in support of (ISC)²’s newest credentials, we are introducing a new webinar series, “From the Trenches.” During this one-hour panel, we will have frank discussions with practitioners on topics pertaining to forensics and healthcare, providing specific learning opportunities in support of the Certified Cyber Forensics Professional (CCFPSM) and Healthcare Information Security and Privacy Professional (HCISPPSM) credentials.

If you, the member community, find value in these credential-specific sessions, then we will kick off 2015 in earnest by adding these to our educational calendar. As always, we look for your honest feedback on both of these exciting new tracks as they develop over the next quarter.

Our second pilot offering is a bit unique. Realizing that busy security professionals can’t always attend one-hour webinars but would still benefit from panelists’ valuable insights, we will condense these sessions into short summaries, available on the (ISC)² website. Maybe you’ll choose to read the summaries to catch the highlights, then listen to the webcast archive to hear the whole conversation. Or perhaps you’ll attend the live webinar, then grab the summary to share with your boss and colleagues. Either way, this provides a useful reference for learning, as well as a vehicle for further sharing.

“Over the summer months, we have discussed new ways of sharing information among the professional community and to extend that sharing outside of our community.”

Of course, in order to earn the CPE credits, you still must attend webinars or live events. My hope is that you’ll find this a useful service worth continuing.

As your host and moderator for these events, I am always on the lookout for new ways to add value to your membership and the profession as a whole. To better serve your needs, I encourage you to reach out and let me know what you think of these two ideas.

Until next time, I look forward to continuing the conversation.
The projected growth rate for the information security analyst profession between 2012 and 2020

SOURCE: BUREAU OF LABOR STATISTICS, 2014

Do you have what it takes to answer the call?

Elevate your information security career with one of Capella’s new MS in Information Assurance and Security options: Digital Forensics | Network Defense

Your future is waiting. Start now. CAPELLA.EDU/ISC2 OR 1.866.670.8737
HEN W. HORD TIPTON became CIO of the U.S. Department of the Interior in December 2001, the security staff worked on one floor, and the privacy folks were on another. Another 11 specialists were scattered between the two. “They basically never talked to each other,” recalls Tipton, executive director of (ISC)² for the past six years.

Tipton knew such a siloed setup could slow improvements to both data protection and staff members’ professional growth, so he pushed for more collaboration and dual-disciplinary teams. By the time he left the Department of the Interior more than five years later, the security and privacy staff members were working as one unit.

Such a convergence is now happening on a more global scale as governments, consumers, and companies demand much more from those specializing in privacy, and in general and industry-specific security.

“It’s incredibly clear that data in the information economy and emerging technologies are driving not only new and wonderful things for society, but also risks we hadn’t expected or understood previously,” says Trevor Hughes, president and CEO of the International Association of Privacy Professionals (IAPP).
(ISC)²’s new partnership with IAPP is the latest alliance to best prepare members for the information security challenges ahead—just as its founders envisioned.

Number of CISSPs around the world

- **Year 1989**: 0 (the first test wasn’t administered until 1994)
- **Year 2010**: 68,978
- **Year 2014**: 94,437

That’s how many CISSP exams took place in December 2010—the deadline for DoD 8570, which required U.S. federal government employees, contractors and vendors involved in information assurance to be certified in information security. The mandate was first introduced in 2007.

CSSLP

Named one of the hottest security certifications in 2014 by InfoWorld magazine, with a 40 percent growth in premium pay during the past 12 months.

It also tied for second-highest paying IT security certification, according to IT research firm Foote Partners, LLC.

Information security professionals by gender

- **11% female**
- **89% male**

(Source: (ISC)² Foundation Report “Agents of Change: Women in the Information Security Profession”)

Information security professionals by gender:

- **11% female**
- **89% male**

*as of 7/31/14*
“Many of those risks fall under broad titles of privacy and security,” he continues. “We frequently use the terms interchangeably, but there is a distinction between the two fields.”

Indeed, security is a technology-driven field, while privacy relies heavily on law, policy, and compliance. But to succeed and move up the career ladder, those working in either profession must become proficient, if not fluent, in both worlds to provide appropriate risk mitigation in the era of cloud computing, big data, and the “Internet of Everything.”

As a result, (ISC)² members seeking certifications or renewing their certs will soon find more materials on the privacy side of data security. The newest version of the CISSP coursework and exam (coming out in Q1 2015), for instance, will include more depth in privacy.

“It’s not that we try to make a privacy professional out of the CISSP, but they must have a platform of basics to understand what they need to know in privacy. And they can go deeper in that if they choose,” Tipton said.

Nowhere is the merge more apparent than in one of (ISC)²’s newest credential programs—the Healthcare Information Security and Privacy Professional (HCISPP), which gives equal weight to security, privacy, and risk.

And, according to Tipton, nowhere is reassurance more necessary than in patient medical privacy, where research indicates hundreds of thousands—if not millions—of people with terminal or life-threatening illnesses, particularly cancer and HIV/AIDS, refuse to see a doctor for fear their confidential health data will be exposed.

“This loss of trust from the public is something that we’ve got to turn around,” he says. “If people do not trust us because of the risks that we take and ensuing breaches, or the lack of due diligence or due care of their data, then no solution is going to work.”

Eventually, he’d like to see certifications of completion for privacy and security programs grace health-care facilities’ walls the way college diplomas do. “We need to press the point that our healthcare facilities should be as proud of having people in their offices qualified in privacy and security, so their patients are assured they’ve invested in training people in this very important aspect.”

Organizations must also consider the penalties for failing to educate their IT staff continually in data security and data privacy.

“We want data to do amazing things for us—and it can—but it will create enormous risks for organizations and disasters for individuals if we don’t do it properly,” Hughes says.

He adds that lack of resources is no excuse.

“We stand to gain enormously as a society with the information economy that we see before us.”

—TREVOR HUGHES, president and CEO, International Association of Privacy Professionals

“Nobody has enough time or enough budget, but the reality is the march of technology will not slow,” he says. “So either you as an individual in your career or within your organization will fall behind, if not suffer significantly, if you are not staying ahead of these things.”

It’s also a matter of survival.

“We stand to gain enormously as a society with the information economy that we see before us,” Hughes says. Innovations such as cloud computing, big data, and the growth of smart devices and wearable computing hold great promise to improve lives.

“However, that potential will not be realized unless we get information security and information privacy right,” he says. “Consumers will not adopt technologies if they don’t trust them. They will not embrace companies if they don’t trust them and have confidence they will do the right things with their data.”

Both Hughes and Tipton believe those who study and understand both information security and information privacy will not only build consumer trust but also extract the greatest value from promising innovations.

“I think security professionals, if they are to succeed, maintain, or move ahead, cannot do their jobs without enhanced knowledge of privacy,” Tipton says. “They will come up short if they don’t broaden their education in the privacy arena, given that it’s risen to be such a hot topic in the world in which we now live.”

ANNE SAITA is editor-in-chief of InfoSecurity Professional.
study this

YEAR 2004 *

*First (ISC)² Global Information Security Workforce Study conducted and published

PROFILE OF 5,371 RESPONDENTS:

- Carry a variety of titles, including security consultant, security manager, director of security, and chief information security officer, with the majority of respondents being male
- Possess an average of 13 years of general IT experience, along with an average of 7 years of security experience
- Hold multiple security-related certifications, including one vendor-neutral and one or more vendor-specific certifications
- Receive an average of 10 days of information security-related training each year

YEAR 2013 *

*Latest GISW Study

PROFILE OF 12,396 RESPONDENTS:

- More than 80 percent had no change in employer or employment in the past year
- Number of professionals expected to grow by more than 11 percent annually over the next five years
- Fifty-six percent believe there is a workforce shortage, compared to two percent that believe there is a surplus
- Broad understanding of the security field was the #1 factor in contributing to career success; followed by communication skills
- Nearly 70 percent view certification as a reliable indicator of competency

(ISC)² credentials an IT professional is likely to have in 2014

1 Certified Information Systems Security Professional (CISSP) Established: 1994
2 Systems Security Certified Practitioner (SSCP) Established: 2001
6 Certified Authorization Professional (CAP) Established: 2005
7 Certified Secure Software Lifecycle Professional (CSSLP) Established: 2008
8 Certified Cyber Forensics Professional (CCFP) Established: 2013
9 HealthCare Information Security and Privacy Practitioner (HCISPP) Established: 2013

global reach

(ISC)² members now live and work in 169 countries. More than 87,000 of the 100,000+ members are located in the following 10 countries:

<table>
<thead>
<tr>
<th>Country</th>
<th>Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>64,655</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>4,987</td>
</tr>
<tr>
<td>Canada</td>
<td>4,473</td>
</tr>
<tr>
<td>Republic of Korea</td>
<td>3,551</td>
</tr>
<tr>
<td>Australia</td>
<td>1,778</td>
</tr>
<tr>
<td>Netherlands</td>
<td>1,698</td>
</tr>
<tr>
<td>India</td>
<td>1,698</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>1,441</td>
</tr>
<tr>
<td>Japan</td>
<td>1,436</td>
</tr>
<tr>
<td>Germany</td>
<td>1,344</td>
</tr>
</tbody>
</table>
DATA HELD HOSTAGE

BY TOM TOLLERTON

Despite recent efforts to disrupt malware developers from using extortion for financial gain, ransomware is on the rise

ON JUNE 2, 2014, the United States Department of Justice announced that a covert public-private initiative dubbed “Operation Tovar” had disrupted criminal activities emanating from the Gameover ZeuS botnet.

At the time, Gameover included as many as 1 million compromised Windows machines. It served as a platform for malicious activity, including command and control (C&C) servers for Cryptolocker, the notorious malware that employs strong encryption to prevent users from accessing important files until they pay a ransom.

Operation Tovar demonstrates that law enforcement, intelligence agencies, and private sector experts are sharing information about very real threats to consumers and working together to reduce cybercrime.

But security professionals can neither boast, nor even assume, that disabling a single botnet infrastructure has eradicated the threat. It merely buys time and helps reduce risks until the next threat emerges. And in the case of ransomware like Cryptolocker, the momentum remains on cybercriminals’ side.
Cyber forensic knowledge requirements have expanded and evolved just as the nature of digital information has, requiring cyber forensics professionals to understand far more than just hard drive and intrusion analysis.

The Certified Cyber Forensics Professional (CCFP℠) indicates a standard of expertise in forensics techniques and procedures, standards of practice, and legal and ethical principles to assure accurate, complete and reliable digital evidence admissible to a court of law.

Do you have what it takes to become a CCFP?

DOWNLOAD the CCFP Snapshot
Hostage-Taking 101

Ransomware is not a new concept, but in the past year, new variants of the malware that can hold your data hostage have established themselves as lucrative alternatives to more traditional means of stealing financial data and passwords.

The premise is simple. A user opens an infected email attachment, and the malicious software installs itself on the victim’s computer and silently encrypts valuable files. Once encryption is completed, users are informed of the encryption and receive specific instructions for paying a ransom in order to receive the key to decrypt the files.

The ransom for restoring full access to systems and data is currently only a few hundred dollars per infected computer, which makes restoration within reach for almost all users or companies whose computers are compromised.

The low payment, combined with the ease of deployment and high infection rate, has resulted in an extremely attractive revenue stream for cyber-criminals.

One of the unique characteristics separating ransomware from other forms of malicious software, like spyware and credential-stealing Trojans, is the intentional interaction between the attacker and the victim.

More traditional forms of malware are typically designed to maintain a fully silent existence, forcing us to rely almost exclusively upon our antivirus software and system configurations to alert us to successful infection.

Ransomware, on the other hand, specifically demands the attention of the system’s user in order to achieve the attacker’s objective.

A large window or wallpaper is splashed in front of the user explaining how the user’s data has been locked. To fuel user anxieties, count-down timers embedded in the pop-up window slowly tick their way down to zero, while canned text warns users that their files will be forever unrecoverable unless they deposit a sum of money before the timer expires into an account belonging to the attacker.

This threat is not limited to consumers’ personal computers.

Business computers represent even more valuable targets to attackers, as the data stored on corporate computer systems are likely critical to the operation of the organization. Also, a network of computers presents additional potential targets.

There have been breach response cases where Cryptolocker or a newer variant, Cryptowall, has ignored the files on the user’s local hard drive and immediately scanned and began encrypting files on mapped network file shares.

Some well-known anti-malware solutions fail to discover the malware prior to infection, and attempts to clean a system after infection can often be incomplete. Crypto-ransomware is known to create multiple processes on a Windows system and can recreate a terminated process if not all are eliminated during the initial attempt.

Innovation Leads to Escalation

Operation Tovar and the disruption of the Cryptolocker command and control infrastructure demonstrate that the cat-and-mouse game between security professionals and cyber-criminals is alive and well in the ransomware space. As this issue goes to press, malware researchers are discovering new spam surges that suggest criminals are attempting to rebuild the powerful Gameover botnet using code with similar features.

Similarly, while UK-based anti-malware research and consulting firm Sophos has observed a virtual elimination of the Cryptolocker variant of ransomware (thanks to the Gameover botnet disruption), it has also seen an increase in new variants of encryption-based ransomware.

New variants like Cryptowall, Cryptorbit, and CryptoDefense leverage at least some of the same code as the now “dated” Cryptolocker. And security research site Malware Must Die notes that a development kit for creating various crypto-based ransomware can be purchased online, suggesting additional variants may not be far behind.

Mobile is the New Target

Malware developers are already showing significant interest in the mobile platform as smartphones and tablets become effective complements or even replacements for workstation computers.
Multiple variants of ransomware targeting the Android platform are circulating the Internet. The Koler Trojan has demonstrated resilience and is not bound to a particular geographic location or language. Typically, users are redirected from an intentionally infected website and prompted to install an app (generally focused on providing quick access to adult content) which quickly passes unique identifier information about the device to a C&C server. Similar to PC variants, a popup will appear that impairs a user’s ability to access the device. SimplLocker, Reveton, and other variants work in much the same way.

Even the Apple iOS platform, widely considered the most secure platform on the mobile market, has seen cybercriminals attempt to exploit user trust.

While the Apple iOS platform is closed by default (prohibiting non-Apple approved applications from being installed), a successful May 2014 attack concentrated primarily in Australia that locked both iOS devices and Mac computers, reportedly leveraged compromised iCloud accounts. Potentially exploiting weak user passwords, this attack further demon-

---

**1. Beef Up User Security.** Infection starts with a compromised user. Avoiding the installation of malicious software altogether is the best prevention of ransomware, yet unsuspecting and inherently trusting users continue to click on suspicious links and open email attachments from people they don’t know, immediately exposing their computer systems to the risk of infection. Combined with administrative privileges, a malicious file can often install unauthorized software that is difficult to eradicate. If this recommendation could be executed perfectly, there would be no fear of system infection. Unfortunately, human beings will always be the weakest link in the security chain, so we must rely upon the effective implementation of additional layers of protection.

**2. Run Offline Backups.** An important part of IT governance, regardless of the risk of ransomware, is the frequent completion of data backup processes. The latest variants of Cryptolocker and other ransomware have the ability to seek out external hard drives or thumb drives that may be connected to the computer and encrypt backup files alongside primary files. There are cases in which the ransomware has identified and encrypted files within mapped folders associated with centralized network file servers and cloud services like Dropbox. It’s important to conduct backups to external drives or mapped file shares and disconnect them from the computer. Alternatively, backups can be performed to a remote location using software that doesn’t rely upon traditional Windows drive mapping.

**3. Limit Administrative Privileges.** Usually for reasons of convenience or lack of awareness, general users’ Windows login accounts often inadvertently have administrative privileges. Administrative privileges grant a user and any application they run control over a computer to perform tasks, such as changing configurations, disabling anti-malware software, and installing unauthorized software. It is this administrative privilege that Cryptolocker and other ransomware variants rely upon to execute their malicious functions and block access to the user’s files. Limiting privileges associated with a general user’s account reduces the opportunity for ransomware to complete its mission.

**4. Limit Applications.** Application white-listing is a Windows feature that allows IT administrators to limit the nature of applications that are allowed to be installed on a particular system. If properly configured, white lists can prevent a user from activating a ransomware installation by unknowingly clicking on a malicious file.

**5. Install Anti-malware Software.** While extremely helpful, anti-malware software cannot be considered an organization’s only defense against ransomware. Basic best practice controls like ensuring that anti-malware software is installed with real-time scanning enabled can at least make users and system administrators aware of a potential infection. Signature files should, of course, be updated regularly.

**6. Increase Security for Mobile Devices.** Most end users don’t have the same concerns for the security of their mobile devices as they do for their PC’s. Security professionals must make extra effort to impress upon users the importance of employing the same defenses used in securing computer workstations. Further, only downloading and installing apps from Android, Windows, and iTunes stores helps prevent malicious code from running on the devices.

---

**By Tom Tollerston**
strates that the threat of ransomware starts with basic user awareness controls for protecting systems and security.

**Establishing Cyber Barricades**

There are several steps you can—and in many ways, already should—take to reduce the risk of you or your enterprise becoming victim to ransomware (see “Suggestions for Ransomware Prevention,” p. 23).

While it remains an option, most security consultants advise victims not to pay any ransom associated with an infection. There is always a chance that you might not be able to access your system or data, despite following payment instructions.

Infections could be dependent upon communication with command and control or payment servers to unlock the system or deliver the decryption key. If this communication cannot be established, the system may not unlock, making the decryption key unretrievable.

Further, increasing attackers’ revenue only encourages the expanded use of this malware. And if a victim pays the ransom, they set themselves up as an attractive target in the future.

When it comes to ransomware, it’s important that security professionals help organizational leadership stay calm and encourage them to take a risk-based approach to addressing the potential loss of data control and preventing ransomware infections.

TOM TOLLERTON, CISSP, CISA, GCIH, QSA is a cybersecurity, digital forensics, and incident response consultant with Dixon Hughes Goodman LLP. He provides data breach response services, as well as security testing, audit, and compliance procedures. Tom can be reached at tom.tollerton@dhgllp.com.
GETTING LEFT OF THE HACK

HONING YOUR CYBER INTELLIGENCE CAN THWART INTRUDERS

BY RANDY BORUM

When it comes to information security, it is easy to become so focused on what’s happening inside your network that you neglect the outside actors that may be preying on your weaknesses. The knowledge of our adversaries’ intentions, capabilities and activities in the cyber domain, or cyber intelligence, enables us to intervene before an attack occurs—or to get “left of the hack.” Intelligence collection and analysis provide essential tools for staying ahead of the adversary.
Although the term “intelligence” may be unfamiliar or unclear to many traditional cybersecurity practitioners, both NIST’s National Cybersecurity Framework (http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm) and DHS’s Task Force on CyberSkills (http://www.dhs.gov/homeland-security-advisory-council-0) emphasize the value of the intelligence function.

Intelligence is not just a national security activity. It concerns a range of organizations in the private and public sectors. At the broadest level, intelligence might be thought of as “actionable knowledge,” but as John Felker, director of Cyber Intelligence Strategy for Hewlett-Packard (Palo Alto, Calif., U.S.A.), points out, “intelligence for cybersecurity is more than 1s and 0s.” Felker also co-chairs a national task force on cyber intelligence for the Intelligence and National Security Alliance (INSA) (http://www.insaonline.org).

The Cyber Intelligence Task Force uses a common three-part framework to describe the different levels at which actionable knowledge influences decisions and activities within an enterprise. The three overlapping levels are strategic, operational, and tactical (see “Cyber Intelligence Task Force’s Three-Part Framework,” p. 27). The defining features of each level are based on the intended consumer, decision requirements, timeframe, adversary characterization, collection scope and methods.

The strategic level focuses on setting an organization’s mission, direction, and objectives and developing a plan for how the organization will achieve those objectives. Intelligence collection broadly assesses the threat landscape for macro trends (e.g., political, social, economic) affecting the industry and the organization and discerns who the bad guys are, what they want to achieve, why, and how they will likely attempt to achieve those aims.

The operational level focuses on enabling and sustaining day-to-day operations and output, including logistics. At this level, cyber intelligence looks at the organization’s internal operations and collateral partners and at external threats posing the greatest risk to business continuity and with the greatest potential business impact. Those analyses inform risk-based decisions about resource allocation and defensive actions.

The tactical level focuses on the specific steps and actions the organization takes to protect assets, maintain continuity, and restore operations. In the cyber domain, the tactical level is where on-the-network actions take place and malicious actors and network defenders maneuver actively against each other. Intelligence examines the technical/logical tactics, techniques and procedures (TTP) used to target the organization.

The three-level framework—strategic, operational, and tactical—illuminates the “big picture” of cyber intelligence. Too often, “threat intelligence” focuses only on the tactical level: the technical dimensions of an attack such as implants, tools, and artifacts. There is no question that this information is valuable, but it is only one dimension of actionable information in cyber defense. Cyber intelligence must collect and analyze more than network logs; it must go beyond the network.

Developing Smart Defenses
Cyber intelligence should drive the cybersecurity mission and form the foundation of effective cyber defense. An intelligence-led approach can transform the organization from a reactive to a proactive security/risk management posture.

With finely honed cyber intelligence, an organization can align valued assets with prioritized threats and available resources. Troy Mattern, deputy head of cyber security for Zurich Insurance Group, describes the traditional cyber defense posture as a “Maginot Line,” a static approach in which the central guiding principle is to “defend everywhere.”

Mattern says that “risk-based, intelligence-driven security allows you to focus not just on generic threats and risks but your threats and risks. You have to know the specific risks that threaten your organization and develop your strategy around them. You can’t do that without intelligence.”
A Roadmap to Cyber Intelligence

At the core of a risk-based, intelligence-driven security approach is a function that continuously collects, processes, analyzes, and disseminates information about the vulnerability of valued assets in relation to the risk posed by internal and external threats and uses that information to guide its decisions and operations. There are several steps organizations can take to achieve an intelligence-led approach to cyber defense.

- **Approach Cyber Defense as a Dynamic, Ongoing Process:** After WWI, France built the Maginot Line, a massive fortified wall, along its border with Germany. The rationale for building the Maginot Line was very similar to the rationale for deploying firewalls today—to provide time for their army to mobilize in the event of attack. But in response to the Line, the Germans just changed their attack strategy. They adopted an approach based on speed and surprise rather than direct, frontal assault. The Germans went around the fortress and attacked France from Belgium. The Line did not falter, but by itself, it could not defend against the intrusion.
Just as the Maginot Line could not defend against ever-changing intrusions, neither can firewalls. Information security methods have evolved considerably since the early days of broad, static perimeter defense. Security assessment and response must be a continuous process, and security mechanisms must be multi-layered and dynamically deployed. Adversaries adapt, and they will prevail without a dynamic defense.

• **Look Beyond the Network**: Most security teams say that they monitor “threat intelligence,” but those activities occur almost exclusively on the network. Organizations must widen their collection aperture for threat intelligence. Intrusion indicators are often found only after the adversary is already “inside the wire.”

• **Understand the Attack**: The intrusion is just the endpoint of a longer and more complex process of planning and preparation that has come to be known as the “Cyber Kill Chain.” Originally articulated by Lockheed Martin, it describes the phases of a cyber attack:
  - Reconnaissance
  - Weaponization
  - Deliver
  - Exploit
  - Install
  - Command & Control
  - Act on Objectives

• **Discerning attack activity before an intrusion requires off-network information**. Relevant data may come from specific network activity, global cyber activity, organizational policy and action, industry/sector trends, or from geopolitical events. It can be open source, proprietary, or classified. What matters most is that the information is timely, actionable and relevant.

• **Map Your Threat Surface**: Each organization has its own risk profile based on the assets it possesses and the competitors or adversaries vying for their space. This combination is the organization’s “threat surface.” First, the organization must assess and prioritize its assets, analyzing security risks and vulnerabilities in all sections. Then, the organization can assess and characterize its adversaries and competitors, their intentions, their objectives, their methodologies and their opportunities on a continuous basis.

• **Total Alignment Needed**: Effective security requires clear priorities and alignment among the security team, as well as executive and senior management involvement. Cyber intelligence analysts can provide information about assets’ exposure and vulnerability, but ultimately, prioritizing value, business impact (e.g., loss and disruption), and risk tolerance are executive decisions.

### An Evolving Discipline
Cyber intelligence continues to evolve as a discipline and an area of practice. Some companies have created sophisticated capabilities, with dedicated personnel integrated across the enterprise working at strategic, operational and tactical levels. Others, however, may have no analytic capacity but serve a security function that is compartmented and gathers intelligence only from their CERT feeds. A range of vendors and firms has emerged over the past several years offering cyber intelligence solutions for companies that cannot create their own.

A number of groups also continue their work to advance the science and practice of cyber intelligence. In addition to the INSA Task Force, researchers and analysts at Carnegie Mellon University’s Software Engineering Institute (SEI) (http://www.sei.cmu.edu) are an active cadre of professionals seeking to shape and expand the discipline of cyber intelligence.

In 2012, the SEI team developed the Cyber Intelligence Tradecraft Project (http://sei.cmu.edu/about/organization/etc/citp.cfm) to explore best practices used within different industry sectors. Extending the Tradecraft Project, this summer, SEI launched the...
Cyber Intelligence Research Consortium (http://www.sei.cmu.edu/about/organization/etc/overview.cfm), a collective of cross-sector institutions working to improve collection and analytic methodologies, technologies and practices in cyber intelligence.

**Moving Toward the Cyber Intelligence Future**

Most information security professionals would say that they have a risk assessment and management approach. Some even say they use “threat intelligence,” but in reality, they have no systematic intelligence capability at all.

Without an inventory of requirements and a collection management process, organizations cannot focus or prioritize the cyber threat information they collect. This makes for a “noisy” stream of threat information, within which the most useful data becomes more difficult to identify. Some try to cope by subscribing to as many feeds as possible and hoping information relevant to them will appear in the mix—but that approach is profoundly inefficient.

Cyber intelligence capabilities can make any cybersecurity enterprise more proactive and effective. By understanding their threat surface and looking well beyond the network, organizations can take on an intelligence-led approach to cyber defense and make it a dynamic, ongoing part of their culture.

DR. RANDY BORUM is a professor and the coordinator for Strategy and Intelligence Studies in the School of Information and Academic Coordinator for Cybersecurity at the University of South Florida. Additionally, he developed one of the first systematic, graduate-level, academic programs of study in Cyber Intelligence and serves on INSA’s Cyber Intelligence Task Force.

---

Promisec: because complete detection at your endpoints is a must.

Promisec Integrity is the first cloud based security, compliance and system management suite built for the unique needs of your business.

**Come see what we see... FREE for 30 days.**

Get a FREE Promisec Integrity health check. Receive immediate and comprehensive visibility into all of your endpoints – without installing any agents.

Promisec
Actionable Endpoint Intelligence
www.promisec.com
TERABYTES OF DATA, petabytes, exabytes—massive amounts of information are being collected and parsed daily by more and more entities. As big data becomes the commonality in business, the challenge to infosecurity professionals to secure the data is growing exponentially.

According to Gartner, Inc., the technology research and advisory firm headquartered in Stamford, Conn., U.S.A., big data “is high-volume, high-velocity and
high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making.” For businesses, the ability to analyze big data “will become a key basis of competition,” predicted McKinsey Global Institute in a 2011 report (http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation). And if you look at Apple, Google, Amazon and Walmart, to name a few, it’s clear that competition now has boots on the ground.

For information security professionals, big data is “the yin and the yang,” says Larry Ponemon, CIPP, chairman and founder of the Michigan-based Ponemon Institute LLC, a research organization focused on privacy, data protection, and information security policy. “On one hand, it creates a lot of risk. But if you harness the information properly, you can get a lot of value to help you understand your security environment in ways you can never imagine, and you can focus resources there.”

The Bigger the Bucket, the Greater the Risks
Big data is not a new problem for infosecurity, according to Bill Sieglein, founder of CISO Executive Network, a Maryland-based peer-to-peer professional organization, but rather “an expansion of an existing problem. We’ve determined that it isn’t a whole lot different than any other regulated data in our environment; we’ve just created more data. All of our same policies apply; we’ve just got a bigger bucket to protect. It’s a richer target for adversaries, so it puts us in a higher-risk category.”

Chris Apgar, CISSP, agrees: “Big data shouldn’t make their life harder if they’re doing what they should be doing all along.” Apgar is CEO and president of Apgar & Associates, LLC in Portland, Ore., U.S.A., a security consultancy to healthcare organizations. He adds, “More due diligence is necessary when vetting a [third-party] vendor,” and suggests checking with that vendor on an annual basis to demonstrate their security posture.

Keeping It Private
Privacy is one of the big issues with big data, says Ponemon. “You collect information, and unbeknownst to consumers, it is suddenly in the hands of a third-party data organization. A big dilemma many organizations are facing now is how to honor the commitment they made when they collected the data.”

The collection and subsequent combinations of these large data sets also puts businesses at risk of violating privacy and compliance regulations. Sieglein says it’s not necessarily the collection of “gobs of data” that’s the problem, but rather “it’s putting that data together that becomes toxic.” Separately, data “may not have fallen under any regulated requirements” and is not categorized as protected health information (PHI) or personally identifiable information (PII). “But if you now have name, social security number and address all in one bucket, that’s called PII. It didn’t used to be PII, but now it’s subject to state laws, and you have to start protecting it.”

“All of our same policies apply; we’ve just got a bigger bucket to protect. It’s a richer target for adversaries, so it puts us in a higher-risk category.”

—BILL SIEGLEIN, founder, CISO Executive Network

On top of privacy concerns, John Pescatore, director of emerging security trends at SANS Institute, points out that two of the biggest challenges to protecting big data are people and immature technology. “Every new technology invariably starts with very little security built in, and over time, it becomes more secure. Hadoop [the Apache open source framework for processing big data] is a good example. It’s an early model that is great for doing big data functions faster, and oh yeah, we grafted security on.”

The people issue is what Pescatore calls “the Snowden risk.” He explains, “The typical technology used in big data gives every DBA and analyst full access to everything.” So a marketing person who uses this data for malfeasance is an example of an insider overusing their privileges,” he explains. Conversely, “bad guys who phish that marketing guy and get control of his PC” is an example of an outsider threat.
Defense of the Data—A Case Study
Cardinal Health, a healthcare services company based in Dublin, Ohio, U.S.A., began incubating the concept of big data in the enterprise architecture lab more than two years ago. Jeff Graham, Cardinal’s senior advisor, Data Analytics, Enterprise Architecture, is on the front line: “Since then, we’ve been using it in a lot of places to help us understand click-stream analysis on our customer website and for clinical research. The goal with big data is to increase our analytics agility. Big data allows us to do this in a cost-effective way because it allows our data scientists to dig in deeper.”

Cardinal generates a lot of data internally, as well as purchases third-party data, and takes advantage of free and open resources available from sites such as data.gov and medicare.gov.

The strategy for securing big data falls more on the process side than on the technology side, explains Graham: “You have to be careful of the three V’s of big data—volume, velocity, variety. With new data processing engines like Hadoop, you have to make sure everyone in the group understands what HIPAA and PHI data means—from the business analyst to the data scientist. Education of all the team members is the most crucial. You can have technology, but if you don’t have people who understand what security is, you will have issues.”

Cardinal is using the Hortonworks distribution of Hadoop, which has three different levels of security: the hardware level, the network level, and within Hortonworks itself. Cardinal is also using the big data analytics tool from Datameer, which Graham says also has a security layer.

In addition to being “attached at the hip” to Car-
dinal’s director of security, Graham’s department partnered with human resources to develop training material for anyone working with data inside Hadoop. Workers are tested on the material, which is refreshed as appropriate, he explains.

Graham adds that Cardinal has also established policies for transferring data with external parties, such as utilizing secure FTP. And internal requests for data brought into Hadoop go through a centralized governance board. “Ninety percent of our data is not data that needs to be secured, but we want to make sure we’re covered. Governance plays a huge part in this.”

"Accurate anomaly detection is the key to detecting threats/breaches."
—SREERANGA RAJAN, director, Fujitsu Laboratories of America

Tools Needed to Fit the New Paradigm

Although traditional security tools are not designed to handle big data, Larry Ponemon warns that it’s hard to stop the tidal wave. “We do things that are convenient, and then we repent,” he says, paraphrasing musician Bob Dylan.

“Accurate anomaly detection is the key to detecting threats/breaches,” advises Sreeranga Rajan, director, Software Systems, at Sunnyvale, Calif.-based Fujitsu Laboratories of America. “With big data, there are typically very many varieties of unstructured data sources across which correlation and anomaly detection has to be performed. Traditionally, intrusion detection and SIEM [security information and event management] tools can process only structured data. Therefore, intrusion detection and SIEM tools cannot scale up to the demands of big data.”

Rajan is co-chair of the Cloud Security Alliance’s Big Data Working Group. In its report, “Expanded Top 10 Big Data Security and Privacy Challenges,” April 2013, the working group identified these top 10 challenges:

1. Secure computations in distributed programming frameworks
2. Security best practices for non-relational data stores
3. Secure data storage and transactions logs
4. End-point input validation/filtering
5. Real-time security monitoring
6. Scalable and composable privacy-preserving data mining and analytics
7. Cryptographically enforced data-centric security
8. Granular access control
9. Granular audits
10. Data provenance

Knowing the risks can help when going down the big data path, particularly when choosing a third party, says Chris Apgar. One of Apgar’s clients is a vendor that provides data to large healthcare entities. He relates how a large client of that vendor adopted the CSA’s threat list and “added things to it to cover themselves, from the physical security of the data to disaster recovery, and told the vendor to prove you’ve done all these things.” The client also requested the vendor be SSAE 16 compliant, he says (SSAE 16 is an auditing standard for services organizations; it replaced SAS 70).

Fighting Cybercrime with Big Data Tools

Looking ahead, it won’t be just the marketing department and data scientists who will be using big data tools, experts say, but infosecurity will start to add big data analytics to its arsenal. Gartner predicts that by 2016, 25 percent of large global companies will have adopted big data analytics for at least one security or fraud detection use case.

The Big Data Analytics in Cyber Defense study (http://www.ponemon.org/library/big-data-analytics-in-cyber-defense), sponsored by Teradata (an analytic data platforms, marketing applications, and services company, based in Dayton, Ohio, U.S.A.) and conducted by Ponemon Institute, revealed the following:

• 56 percent of respondents (IT and IT security practitioners) are aware of the technologies that provide big data analytics;
• 61 percent say they will solve pressing security issues, but only 35 percent have them;
• 82 percent of respondents would like big data analytics combined with anti-virus/
anti-malware; and
• 80 percent say anti-DoS/DDoS would make their organizations more secure.

The study also concluded that big data analytics, combined with security technologies, will give organizations a stronger cyber defense posture.

The CSA’s Big Data Working Group projects that in the area of intrusion detection, the next generation of SIEM tools will include big data analytics. “Security analytics tools address two of the top 10 challenges, namely, real-time security monitoring [and] scalable and composable privacy-preserving data mining and analytics,” predicts Fujitsu Labs’ Rajan.

“Security officers want to get their hands on anything that will help them assess their security posture in real time,” adds Bill Sieglein, citing their use of analytics tools like Splunk and SIEM provider LogRhythm Labs.

"Security officers want to get their hands on anything that will help them assess their security posture in real time."
—BILL SIEGLEIN, founder, CISO Executive Network

That’s exactly what’s starting to happen at Cardinal Health. Jeff Graham explains that his group began analyzing the logs from Datameer and Hortonworks with the original intent of determining which data sets and transformations were the most helpful—who was generating the most useful data sets, and who was using them. Then they realized they could use the analysis for integrity monitoring and started with intrusion detection. “If certain trends can give us insight into potential for abuse, that part is pretty neat. We started this a while back to support reasons for having different data sets, and it turned into so much more.”

Yet Sieglein suggests treading carefully with big data security analytics. “The security folks are also a culprit in that they want to collect as much information as they can. The danger is if there is data in the log information that is regulated” or privacy-related.

“We’re almost as bad as the marketing folks we scream at all the time.”

So while privacy regulations remain in flux and tools are still maturing, “big data is here to stay,” says Sieglein. “Companies understand the value [of big data], so security and privacy officers have to advise management continually on what they should be doing to protect data, knowing that the regulators will be coming down heavy handed in the next few years, especially as it pertains to consumer data.”

Risk and reward—the yin and the yang of which Ponemon speaks.

COLLEEN FRYE is a freelance writer and regular contributor to InfoSecurity Professional.
Judging from this year’s recipients of the 2014 (ISC)² Foundation Cyber Security Scholarships, passion, dedication, drive, and determination are never in short supply for those seeking a career in information security. But funds to finish their formal education are often hard to come by. That’s why we created these scholarships, which ultimately help bridge the gap in the workforce for qualified information security professionals.

I am so inspired by this year’s winners in the Women’s, Graduate, and Undergraduate categories, many of whom shared expressions of gratitude and a glimpse of their pasts, present, and promising futures.

A full list of scholars is available in “Field Notes” on page 13. Here are responses from some of this year’s recipients, all of whom said they were honored by the recognition and show of support they received from the (ISC)² community.

Shruti Gupta, India (Women’s)
“The scholarship offers the opportunity to continue with my graduate studies, allowing me to contribute more toward the information security realm. It will help me focus on my research and fulfill my dreams of becoming a Ph.D. The CISSP certification will enable me to join the elite ranks of highly skilled infosec practitioners, greatly benefitting my career.”

M. Alexis Greenidge, U.S.A. (Women’s)
“Freedom in a world of security. A seeming paradox, but the scholarship frees up my finances so that the degree that I am going for is more manageable. As a single parent with two children currently in college, this is a tremendous help to my family. It relieves the stress that comes along with debt. Unfortunately, education is very costly in our country, but with foundations like yours, it makes a great impact on my life. I am sure that every recipient has been honored and has been positively impacted in more ways than one.”

Sreedevi Sreekandan, India (Women’s)
“I consider this scholarship a recognition and approval of my decision to specialize in cybersecurity as part of my continuing education. The scholarship committee also recognized the hard work I put into the first year of the graduate level course work. On a personal level, I believe this award also shows the Foundation’s commitment to bring more women into the cybersecurity profession and to extend a helping hand in their journey to become a confident and knowledgeable IT security professional. I hope this award will continue to encourage women all over the world to take a keen interest in cybersecurity education in future.”

Cheryl Devaney, U.S.A. (Graduate)
“The assistance provided by the (ISC)² Foundation allows me to pursue research within the field of information security while completing a Master of Science degree in information systems management. I hope to pursue a career in information security after completing my degree, and the funding provided will give me the opportunity to gain vital experience within this field while a student.”
Anna Truss, Turkmenistan (Graduate)
“I’ve been through a lot of challenges throughout my life to get to where I am now, and getting this scholarship will definitely help me achieve my goals in life. One of my many goals is to receive a Master of Science degree in cybersecurity. This scholarship, for me, is not the end but rather the beginning of a brighter future.”

Lokesh Pidawekar, India (Graduate)
“My interest and passion for learning in the field of information security grows day by day. I had spent more than three years implementing system and network security controls for various clients. The Master’s program in information assurance has given me deep understanding of information security and related issues. Along with my current graduate program schedule, the (ISC)² scholarship will help me conduct extensive research and design secure systems to fight against cybercrime. I would like to dedicate my efforts in securing open source software and APIs to prevent any further security breaches due to vulnerabilities like ‘Heartbleed’. This scholarship will also help me in designing security solutions as part of my capstone project and will be able to serve in the security community.”

Robin Saunders, U.S.A. (Undergraduate)
“In addition to easing the financial strain of my senior year at River Valley Community College, this scholarship reinforces my belief that the pursuit of scholastic success—as grueling as it may be at times—does not go unacknowledged. This award allows me to focus on my career and intellectual development. Not only has it allowed me to finish my Associate degree, but this scholarship also acknowledges all the work I have done thus far and that I will continue to do in the future.”

Fumi Honda, U.S.A. (Undergraduate)
“There’s a saying in my culture that you must first help yourself before others do. I am very grateful that someone out there, namely the (ISC)² Foundation, would help fund my education. I can then focus more on learning as much as I can during my prime years. I plan to have two and a half majors in five years: computer science, psychology, and business. Stony Brook University has a Center for Cyber Security; I will take full advantage of the resources here and give back by using my cross-disciplinary perspective to solve complex problems for society. Thank you!”

Katherine McGinn, U.S.A. (Undergraduate)
“Receiving this scholarship affords me the ability to focus on my studies and not be overwhelmed with managing tuition costs. I can continue with my cybersecurity program at University of Maryland University College with ease. Thank you to the (ISC)² Foundation Information Security Scholarship Program! I am proud to be a member of the (ISC)² organization.”

Dulce Gonzalez, Mexico (Undergraduate)
“This scholarship is a wonderful reminder to me that good things do happen to good people. This scholarship is a reminder of the endless possibilities out there for me. Being a first generation college student has been a struggle, but now I am more motivated than ever to follow my dreams and conquer my goals.“

Samantha Houston, U.S.A. (Undergraduate)
“I am so grateful to receive the (ISC)² Foundation Undergraduate Scholarship because it is a stepping stone on my path to success in the field of cybersecurity. It is an investment in my future and will help me to further my studies and gain experience that I would not have had otherwise. Many times I have questioned how I am going to afford to continue my education and see my career ambitions become a reality, but the support of this scholarship has helped alleviate those worries and given me confidence that I am making the right decision about what to do with the rest of my life.”

Lassine Cherif, Ivory Coast (Undergraduate)
“By selecting me, the (ISC)² Foundation gave me a luxury of focusing on my education rather than worrying about how to pay for it. It gives me a unique opportunity to obtain both a degree and a globally recognized certification; skills that I need to achieve my goal which is help secure cyberspace.”
RISKY BUSINESS
Is it time to ‘just suck it up’ when it comes to data security?

The Target breach, the VA’s massive inadvertent disclosure, the TJX hack, Sony’s disastrous loss of almost all data associated with PSN users, Choicepoint’s data theft by internal actors...all these incidents have something in common: an almost total dearth of appreciable consequences.

Nobody went to jail. And punitive monetary judgments were less significant than other external factors. For instance, Sony claimed that the financial impact of their breach was less than that of an earthquake in Japan that same year.

It’s heresy to say this in our industry, but the pragmatic way to address security risks might be the least expensive, most cost-effective technique: risk acceptance. In other words, just suck it up.

The costs of implementing security measures that actually...well...secure the data they’re intended to protect are massive, both in terms of capital investment and decreased operational capability. And the means to realistically transfer data security risk simply have not manifested in any meaningful way. Underwriters are understandably reticent to predict potential “foreseen” threats. And, without assurance that insurers will pony up the costs of damages, who would purchase those instruments?

Of course, there are statutory requirements for data protection, but we’ve seen even the federal government, including agencies with their own enforcement arms (yes, IRS, we’re looking at you), fail to adhere to even basic security precautions—and not suffer any significant adverse consequences. Proving a good-faith effort to comply with legislative mandates is sufficient to absolve liability, and good-faith efforts are far less expensive than actual security. If you max the minimum requirements, that suffices. If the minimum wasn’t good enough, it wouldn’t be the minimum.

Liability is the name of the game. Why haven’t customers risen up and decried this carelessness, this callous treatment of their precious information? In years past, the industry held that customers didn’t understand the value of what they were losing, that they didn’t grasp the inherent price and cost of their own data. That assertion probably no longer holds. This one might be more apt: customers don’t care because they don’t have to. Victims of credit card theft are not held liable for illegal transactions, by statute, beyond a negligible minimum expense. Why care if someone steals your card, if you don’t have to pay for it?

This is why PCI is driven not by statute, but by those with the most to lose from credit card breaches—and probably why it’s more strict and sensible than regulatory attempts at the same goal.

So, when mitigation efforts are not cost-effective, and transfer-
ence is not feasible, what response is left?
By 2020, we might see everyone, from businesses to government agencies to consumers, just put away their fears of data theft and dispose of their addiction to expensive security solutions in exchange for the most practical of approaches: know that engaging in data-driven transactions incurs an element of risk. That risk can be minimized but never eliminated. It’s important to simply accept the chances of risk and go on about their lives without worrying about it or expending effort and money to alleviate it.
It’s what we all already do with a car—the place we’re most likely, by far, to die.

BEN MALISOW is a freelance consultant who conducts training and instruction. He has taught computer science and technology in Las Vegas and college-level English, information security, and computer security courses throughout the United States.

NEXT ISSUE What will be the biggest security and/or privacy issue[s] by 2020, particularly in the healthcare industry? Send a paragraph or two to asaita@isc2.org by Oct. 15, 2014.

“THE ‘INTERNET OF EVERYTHING’ controlled by a smart phone, as the trend seems to be (home alarm systems, thermostats, home locks, automobiles—one of the auto companies some months ago demonstrated in a commercial a remote start capability from a distant airport with Internet access—etc.) really scares me. Companies and people know how to build functional applications, but they do not know how to build secure applications, and it does not help when the operating systems for these phones are not secure by design, and, in many cases, are not updated (this is particularly a problem for Android, where the phone vendors, not Google, control the decision to issue OS updates for a particular model of phone). My secondary concern is that you have your pick of vendor to collect the data for all of the things done through those applications—Google, Apple, or Microsoft.”
—JEFFREY HARRIS, CISSP, New York
CSSLP® is the only certification that validates your knowledge and experience in secure software development practices.

Enabling the next generation to BUILD HACKER RESILIENT SOFTWARE

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

education.isc2.org/csslp-webcast
Preventing Security Breaches by Eliminating the Need to Transmit and Store Passwords

Learn More