

› BUILDING SECURE SYSTEMS—TOGETHER

InfoSecurity PROFESSIONAL

JULY/AUGUST 2014

A Publication for the (ISC)² Membership

Bring It!

What's working and what's not in BYOD security



isc2.org facebook.com/isc2fb twitter.com/ISC2

+
**Mobile
Malware**
**GISLA[®]
Recipients**
**'At-Risk'
Youth**

The Future of Bring Your Own Identity (BYOID)

Ponemon Institute research report examines key trends in digital and social identities

[Learn more](#)





^ Is malware feasting on your mobile devices?
PAGE 23

FEATURES

> TECHNOLOGY

17 The Future is in Our Hands

If we were to look back on 2014 several years from now, what would we say about how we are securing devices in and outside the workplace? **BY MICHELE KRIEGMAN**

> MOBILE MALWARE

23 Old Tricks on New Platforms

As consumers continue to embrace all things mobile, so do malware developers. Devices with an Android OS may be a bigger target at the moment, but Apple users also remain at high risk. **BY CRYSTAL BEDELL**

> PRIVACY

26 Life of a Child: 2014 Version

A cyber rights advocate shows how easy we make it for identity thieves and other cybercriminals to exploit our children.
BY RAJ GOEL

DEPARTMENTS

5 EDITOR'S NOTE

The 'Smart' Crowd

BY ANNE SAITA

7 EXECUTIVE LETTER

Leveraging Our Past

BY WIM REMES

8 FIELD NOTES

Spotlight on (ISC)² Sri Lanka Chapter; new conference for EMEA members; GISLA[®] recipients; Security Congress U.S.A. at a glance

15 MODERATOR'S CORNER

BYOD Legal Risks

BY BRANDON DUNLAP

30 GIVING CORNER

Many Happy Returns

BY JULIE PEELER

31 2020 VISION

Where should we be most concerned with mobile security?

5 AD INDEX

Cover Image by ©JOHN KUCZALA




Illustration (above) by
©ENRICO VARRASSO

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.

(ISC)²® FOUNDATION

_____ Empowering Everyone to Secure Their Online Life _____

The (ISC)²® Foundation was born through the deep conviction of (ISC)²'s 100,000-plus members who believe that:

-  Research is a powerful tool that helps forecast new trends and illuminates the road ahead for information security professionals in a multitude of specialties.
-  Increasing public education, awareness and safety in the field of cyber security is not an option; it is an honor and an obligation.
-  Encouraging and investing in future information security professionals starting with secondary school and beyond is a powerful step for the future of the cyber security industry.



Get Involved Today!



www.isc2cares.org

HANGING WITH THE 'SMART' CROWD

THE OTHER MONTH I was listening to a series on NPR's "All Tech Considered" on Project Eavesdrop. A California-based journalist enlisted the assistance of some security experts to tap Internet connections to his home office, his desktop and smartphone for intel. They used a professional grade pen testing tool called Pwn Plug.

As soon as Steve Henn's iPhone connected to the network, "torrents of data began flowing over the line" being monitored in Vermont, he said.

"The iPhone was just sitting on my desk—I wasn't touching it," he said in the first of his reports. "We watched as my iPhone pinged servers all over the world. ... My iPhone sent Yahoo my location data as unencrypted text. The phone connected to NPR for email. It pinged Apple, then Google. There was a cascade of bits."

Later he added, "Google's search traffic is supposed to be encrypted, but the subject of my searches seeped out. Links to the sites I visited provided strong hints about what I was searching for."

The reporter was astounded. Something tells me (ISC)² members wouldn't be.

So in this edition, we revisit what's been happening in the BYOD world, with CISSP Michele Kreigman interviewing CISOs about what works, what doesn't, and why. Crystal Bedell reminds us in a second piece that malware developers still favor those miniature machines, especially ones with an Android OS.

Our third feature focuses on the most vulnerable segment of society—our children. We all try to protect them from real-life and cyber dangers, but as CISSP Raj Goel notes, in many ways we undermine protections just by being proud and safety-conscious parents and grandparents.

Finally, thank you to everyone who contributed to this issue's 2020 column. Our next one is on Big Data. Let me know your biggest security concerns surrounding the massive amounts of data being generated by what vendors have come to call the "Internet of Things."

Email me your thoughts by Aug. 15 at asaita@isc2.org.

➤ ANNE SAITA



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

ADVERTISER INDEX

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

| | | | |
|--------------------------|----|--------------------------|----|
| CA Technologies..... | 2 | (ISC) ² | 16 |
| (ISC) ² | 4 | (ISC) ² | 21 |
| McAfee | 6 | (ISC) ² | 22 |
| EWf | 14 | (ISC) ² | 32 |

(ISC)² MANAGEMENT TEAM

EXECUTIVE PUBLISHER

Elise Yacobellis

727-785-0189 x4088

eyacobellis@isc2.org

DIRECTOR, MEMBERSHIP
RELATIONS AND SERVICES

Erich Kron, CISSP-ISSAP

727-785-0189 x4070

ekron@isc2.org

SENIOR MANAGER OF
MEMBERSHIP MARKETING
AND MEDIA SERVICES

Jessica Smith

727-785-0189 x4063

jsmith@isc2.org

PUBLISHER

Timothy Garon

508-529-6103

tgaron@isc2.org

MANAGER, GLOBAL
COMMUNICATIONS

Amanda D'Alessandro

727-785-0189 x4021

adalessandro@isc2.org

MEMBERSHIP MEDIA
SERVICES ASSISTANT

Michelle Fuhrmann

727-785-0189 x4055

mfuhrmann@isc2.org

SALES TEAM

EVENTS SALES MANAGER

Jennifer Hunt

781-685-4667 jhunt@isc2.org

REGIONAL SALES MANAGER

Lisa O'Connell

781-460-2105

loconnell@isc2.org

EDITORIAL ADVISORY BOARD

Elise Yacobellis (ISC)²

Erich Kron (ISC)²

Javvad Malik EMEA

J.J. Thompson U.S.A.

Carlos Canoto South America

Dr. Meng-Chow Kang Asia

TWIRLING TIGER PRESS INC. EDITORIAL TEAM

EDITOR-IN-CHIEF

Anne Saita

asaita@isc2.org

ART DIRECTOR & PRODUCTION

Maureen Joyce

mjoyce@isc2.org

MANAGING EDITORS

Deborah Johnson

Lee Polevoi



www.twirlingtigerpress.com



FOCUS¹⁴

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 (Early Bird ends July 31).



Visit <http://mcaf.ee/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.
- Keynotes: Hear from impressive industry leaders and security experts.
- Other conference highlights: Benefit from Targeted Group Meetings, a partner expo, CPE credit and training opportunities, extraordinary special events, and much more.

www.McAfee.com/FOCUS14



Follow us at #McAfeeFOCUS





THE LATEST
FROM (ISC)²'S
LEADERSHIP

EXECUTIVE LETTER > WIM REMES

LEVERAGING THE PAST TO IMPROVE OUR FUTURE

OVER THE PAST few months, I have taken a long trip down memory lane. While I'm hovering around that age where some may be inclined to inform me that I'm suffering from a midlife crisis, I'd like to clarify that this was definitely not the driver behind my meandering thoughts. Information security is a tough space and some have argued extensively that one of the reasons is that we are a young profession. But are we? And, more importantly, is there anything in our past that we can learn from?

Some of my research has taken me back as far as 1970, a whopping 44 years ago. It was at that time that Willis H. Ware delivered what is now commonly known as "The Ware Report."

It provided a detailed analysis of the issues that came up with the transition from single-use computer systems to multi-use, resource sharing computer systems. While I understand that your time is precious, I would recommend this report to anybody who is involved in information security. It is sobering to realize that the issues identified by Mr. Ware and his team back then are eerily similar to the issues we are trying to solve today.

Information security, sometimes to its own detriment, is very much a forward-looking profession. As Dan Geer mentioned in his [2008 Source Boston keynote](#), we are focused on preventing events from happening in the future. As such, how can we force ourselves to leverage the past to improve our future?

Firstly, I strongly believe that redefining a problem doesn't bring us closer to a solution. While marketing is an essential

component of any commercial industry, finding yet another catchy name for the same problem does not improve the solution. As security professionals, we have the responsibility to help build secure systems, regardless of our badge color.

Secondly, in order to actually build secure systems, we do not help ourselves by narrowing down the problem space. As intelligent devices become part of our daily lives, the boundaries between software, platforms, network and hardware have become blurry to say the least. As security professionals, we should strive to follow this integration and actually understand the subtle interactions between the different areas.

Lastly, we have a very big responsibility to collaborate. While I do understand that some of us are competitors, and there might even be geo-political forces at play, information sharing between professional peers and organizations is key to continued and joint progress. We, as a profession, will not improve by monopolizing information; but we will thrive by sharing it.

There is no doubt that we are facing some very interesting and important challenges. However, I strongly believe that we are well-positioned to address them. We are, and that is crucial, not alone in our desire to improve the world. With a focus on building secure systems, together, I am convinced that we can do this and I'm excited to be working with professionals like all of you. ●

Wim Remes, CISSP, is chair of the (ISC)² Board of Directors and a managing consultant at IOActive. He lives in Belgium.

GLOBAL SPOTLIGHT: (ISC)² SRI LANKA CHAPTER

PROMOTING PROFESSIONALISM THROUGH CERTIFICATIONS

MEMBERS OF THE (ISC)² Sri Lanka Chapter understand the need to strengthen the Southeast Asian nation's information security industry. A big part of the chapter's mandate—in fact, its founding—involves sharing knowledge by providing a common forum for the information security professionals and the public. The Chapter also encourages information security professionals in Sri Lanka to earn (ISC)² certifications.

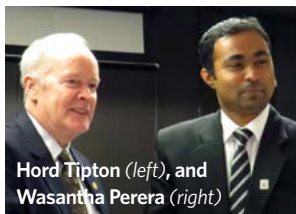
Back in December, the Chapter conducted the inaugural (ISC)² CIO Forum at Cinnamon Grand in Colombo. The forum brought together a strong gathering of Sri Lankan CIOs from diverse industry verticals, such as government, defense, telecommunications, and banking, along with (ISC)² Executive Director Hord Tipton, for an evening of insightful discussions.

"It is a privilege to be able to host the inaugural (ISC)² CIO Forum in Sri Lanka with Mr. Tipton," (ISC)² Sri Lanka Chapter President, Wasantha Perera, said. "And we are glad to make this an opportunity to demonstrate the commitment from the highest level at (ISC)² for the development and continued support to the local chapter."

In conjunction with the event, the Sri Lanka Chapter signed an agreement with (ISC)² to become an **Official Training Provider** to assist security professionals and practitioners in obtaining the "Gold Standard" in information security certification through Official (ISC)² CBK Training Seminars.

By becoming an (ISC)² Official Training Provider, the (ISC)² Sri Lanka Chapter joined a global network of authorized organizations committed to delivering the highest educational standard in cyber security training.

Now the (ISC)² Sri Lanka Chapter is authorized to conduct training and examinations to issue (ISC)² credentials. ●



Hord Tipton (left), and
Wasantha Perera (right)

MEMBER SPOTLIGHT ON...

KAREN KABEL

Karen Kabel joined the Great-West Life Assurance Company, in Winnipeg, Manitoba, Canada as Operational Support and Security Technology manager in January 2014.

An (ISC)² member for more than nine years, she is the founder and immediate past president of the (ISC)² Manitoba & Saskatchewan, Canada Chapter.



Karen Kabel

Kabel's early work in network consulting evolved into security, which took her to EdgeTech Services, an IT Service and Solutions provider (Winnipeg, Manitoba, Canada) and then Seccuris, a security provider (Winnipeg, Manitoba, Canada), a position she held for nine years.

In addition to her (ISC)² credentials, she also holds credentials from ISACA (CISA, CISM).

Through Kabel's work in tech security, and as a single mother of four, she has developed a passion for educating young people in the field. Working with Canada's Cyber Defense Challenge competition for high school students and with the (ISC)² Safe and Secure Online program, Kabel's goal is to not only get young people interested in tech and cybersecurity, but to make the learning exciting and accepted.

"Years ago, the

CONTINUED
ON PAGE 9

➤ (ISC)² SRI LANKA CHAPTER CONTACT INFORMATION

CONTACT: Kanishka Yapa

EMAIL: kanishka@cert.gov.lk

WEBSITE: <http://www.isc2chaptersrilanka.org/>

BOBBIE STEMPFLEY RECEIVES 2014 LYNN McNULTY AWARD

DEPARTMENT OF HOMELAND Security leader Roberta “Bobbie” Stempfley recently was honored with this year’s F. Lynn McNulty Tribute U.S. Government Information Security Leadership Award (GISLA®).

Stempfley, the deputy assistant secretary for Cybersecurity and Communications (CS&C) within the DHS National Protection and Programs (NPPD) Directorate, is the third recipient of this (ISC)² honor named after the late McNulty, CISSP, known for his dedication to professionalizing the U.S. government workforce.

The GISLA recognizes a member of the U.S. federal information security community who upholds McNulty’s legacy as a visionary and innovator through outstanding service and commitment. Recipients are hand-chosen by the (ISC)² U.S. Government Advisory Board for Cyber Security annually.

“Bobbie has overcome many challenges while growing an effective organization that is dedicated to preventing disruptions to our critical information infrastructure and to protecting the public, the economy, government services, and the overall security of the United States,” said W. Hord Tipton, CISSP, executive director of (ISC)² and former CIO of the U.S. Department of Interior. “Thanks to her vision and tenacity, the CS&C leads interagency and public-private initiatives that enable all to better secure their parts of cyberspace.”

Stempfley came to DHS in 2010 to serve as the director for the National Cyber Security Division (NCSD), and was later selected to serve as the deputy assistant secretary for CS&C. Prior to her work at DHS, she was the chief information officer for Defense Information Systems Agency (DISA) where she oversaw IT systems and services used by the major branches of the U.S. military. ●



Bobbie Stempfley

CONTINUED
FROM PAGE 8

cheerleaders and jocks had the attention; now the cyber kids are the cool kids.” And she believes it’s working. She points to one school where IT class enrollment grew from 30 students to 120 students.

“It lit a fire under me... educating students, making security a way of life so when you go into the profession, it’s a culture.” —KAREN KABEL

Since joining (ISC)² and founding the chapter, Kabel says what has surprised her the most is the need for more awareness of tech security, especially on the part of young people, “It lit a fire under me,” she exclaimed. “...educating students, making security a way of life so when you go into the profession, it’s a culture.” Kabel laments the perception that the “security guys are the bad guys, making everyone’s life miserable,” and she feels confident that is helping to change that perception.

Kabel points to two mentors as key people in her professional growth. She says she was inspired by the energy of Michael Legary, founder of Seccuris, who started working at a young age and has built an extremely successful security boutique. And she credits Pat Hoyer, chief information security officer for the Province of Manitoba for his support and encouragement: “He was always my sounding board...he would point me in the right direction.”

—Deborah Johnson

CPEs

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

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&PCAT=7777&CAT=8732

5 WINNERS

CONGRATULATIONS TO THIS YEAR'S GISLA RECIPIENTS

The 11th annual U.S. **Government Information Security Leadership Awards** were presented at a gala in Arlington, Va. (U.S.A.).

Below is a list of the 2014 GISLA recipients.

Jaime Vargas • *Technology Improvement*

Jaime Vargas, chief information security officer (CISO) of the Department of Homeland Security (DHS) Office of the Inspector General (OIG) designed, developed, and implemented an Information Security Continuous Monitoring (ISCM) Program for the IT infrastructure of the OIG. The program encompassed a state-of-the-art architectural solution using automated tools to support the Risk Management Framework, and improved the effectiveness of the safeguards and countermeasures that remediate vulnerabilities. As a result, OIG's FISMA compliance scores ranked among the highest in the federal government. OIG stands as a model component within DHS for information security compliance.



Erich Fronck • *Community Awareness*

Erich Fronck, regional information security director for the Northeast Region at Veterans Administration (VA) led an awareness initiative utilizing a 100 percent stand-down approach that significantly raised the training compliance level for regional users. As a result, compliance rose to 99.62 percent in this sizable region with the number of individuals deficient in training decreasing from approximately 8,000 to fewer than 2,000. The success of this initiative has contributed to the improvement of the VA's overall security posture.



Cyberspace 200/300 Professional Continuing Education Team • *Workforce Improvement*

The 27-member Cyberspace 200/300 Professional Continuing Education (PCE) Team, led by Dr. Robert F. Mills, director of the Center for Cyberspace Research for the Air Force's Cyberspace Technical Center of Excellence, faced the herculean task of planning, establishing, and implementing intermediate and advanced

cyber security courses (Cyber 200/300). Their innovative tactics included the development of 40 joint network attack/defend/exploit capstone exercises with multiple virtual networks to give real-world hands-on training.

Approximately 400 U.S. Department of Defense joint and allied cyber professionals graduated with these crucial skills and the AF cyberspace security workforce now has a program in place that fills a critical void in cyber workforce education.



Jeff Harriss • *Process/Policy*

Jeff Harriss, team lead, Access Control, OCIO-ITS-IOD Operations Security Branch at USDA, set out to reduce risk in the Department's 37,000 member user base by limiting the significant number of users granted elevated (administrator) permissions on their desktop computers. Jeff worked closely with customer development communities to pilot and test a solution that not only resolved technical and procedural issues, but built and fostered positive working relationships. By March of 2014, the number of local administrators was reduced from 10 percent of the population to less than 1 percent, thereby increasing the overall security of this sizable user base.



Sunny Tuteja • *Federal Contractor*

Sunny Tuteja, founder, president and chief executive officer of AssurIT Consulting Group, developed a Plan of Action and Milestones (POAM) Dashboard for the U.S. Department of Agriculture's Natural Resources Conservation Service that brought previously unavailable visibility into the difficult and costly task of managing POAMs. His unique and innovative dashboard delivered a strategic view of system weaknesses that resulted in an anticipated closure of more than 75 percent of the agency's POAMs and an overall improved security posture at the Natural Resources Conservation Service.



For more information on the GISLA program, including past recipients, selection criteria and eligibility requirements, please visit www.isc2.org/gisla. ●

LONDON CALLING

Inaugural Security Congress for EMEA Set for December

"This event presents a unique opportunity for professionals at all levels to come together, share what they are experiencing on the front lines, and learn from each other."

—JOHN COLLEY, CISSP,
managing director, (ISC)² EMEA

levels to come together, share what they are experiencing on the front lines, and learn from each other."

Building on the experience of the U.S.A.-based (ISC)² Security Congress, now in its fourth year, (ISC)² Security Congress EMEA will offer more than five focused tracks, a pre-conference day of training workshops and special interest sessions, along with a gala dinner.

Keynotes and plenaries will be complemented by a broad review of current industry concerns in the following tracks: Governance, Risk & Compliance; Mobile Security; Human Factor; Architecture; and Data Security. ●

INFORMATION SECURITY professionals in the Europe, Middle East, and Africa region are invited to the inaugural (ISC)² Security Congress EMEA taking place Dec. 8 through 10 at The Bloomsbury Hotel in London, U.K.

The multi-day conference, with the overall theme of "Strengthening Cybersecurity Defenders," is being organized in partnership with MIS Training Institute.

"(ISC)² EMEA has delivered

educational conferences across the region for nearly 10 years, allowing us to develop a strong network of top-notch speakers who offer real insight into the issues we are all facing," says John Colley, CISSP, managing director, (ISC)² EMEA.

"What makes this initiative really interesting is the opportunity we have to showcase the wealth of experience within the membership. This event presents a unique opportunity for professionals at all

Photograph ©Mapics-iStock

> "Large retailers maintain centralized connections to these [point of sale] machines for updating, and an attacker can exploit that to distribute malware efficiently and collect large swaths of magnetic stripe data from the cards," according to Philip Casesa of (ISC)². "Without proper detection of this malware on the retailer's part, these breaches can run almost unfettered until the attackers have enough or their exploit window is somehow closed."



—PHILIP CASESA, CSSLP, Director of IT/Service Operations for (ISC)², as told to eWEEK in an article on the P.F. Chang's security compromise that mirrors one against Target last year. He also said that attacks would continue until security on retail PoS systems was pervasive.

Photograph ©Triloks-iStock

The fourth annual (ISC)² Security Congress offers invaluable education to all levels of information security professionals, not just (ISC)² members. This event will provide information security professionals with the tools needed to strengthen their security without restricting their business. (ISC)² and ASIS International have teamed up again to bring education and networking opportunities to the largest security conference in the world. Register today at <https://congress.isc2.org>.

| SCHEDULE AT-A-GLANCE | Cloud Security | Swiss Army Knife | Application Security/ Software Assurance | Mobile Security |
|--|--|---|---|--|
| MONDAY, SEPTEMBER 29 11 a.m. to 12 p.m. | Session 2140 • Securing Big Data: Lock it Down or Liberate It? | Session 2141 • Gamification of Security | Session 2146 • A Client-Side View on API Security | Session 2142 • A Day in the Life of Your Mobile Phone |
| 1:45 p.m. to 3 p.m. | Session 2240 • Challenges for Next-Generation Security Operations Metrics and Management | Session 2241 • Cyber-Security Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals | Session 2246 • DevOps & Appsec Panel - Why DevOps and Appsec are So Important in an IoT World | Session 2242 • Mobile for Education: Getting it Right the First Time |
| 4:30 p.m. to 5:30 p.m. | Session 2340 • Auditing Your Cloud: Layered Security Assurance | Session 2341 • Scaling the Mountain: Building an SOC in 106 Days | Session 2346 • Building a Successful Bug Bounty Program | Session 2342 • Inside an Android Spyphone |
| TUESDAY, SEPTEMBER 30 11 a.m. to 12 p.m. | Session 3140 • Leverage Your SOC to Detect Use of IAAS/PAAS/SAAS | Session 3141 • Neuro-Hacking 101: Taming Your Inner Curmudgeon | Session 3146 • How to Run an Application Security Testing Proof of Concept | Session 3142 • PLEASE, PLEASE, PLEASE Defend Your Mobile Apps! |
| 1:45 p.m. to 3 p.m. | Session 3240 • How to Leverage Endpoint Compliance Cloud Service to an Early Warning System Against Advanced Threats | Session 3241 • Business Skills for Cybersecurity Professionals | Session 3246 • Threat Modeling: It's Not Out of Fashion | Session 3242 • Mobile App Security: Myths and Realities |
| 4:30 p.m. to 5:30 p.m. | Session 3340 • Building and Maintaining a Security Team in the Cloud | Session 3341 • Wearables: Deep Integration Needs Deep Security | Session 3346 • Warning Ahead: Security Storms Are Brewing in Your Javascript | Session 3342 • Mobile Device Tracking and Security |
| WEDNESDAY, OCTOBER 1 11 a.m. to 12 p.m. | Session 4140 • Cloud Security—Securing in AWS and Azure Environments | Session 4141 • All the Gear, No Security | Session 4146 • How to Pentest Web Apps with Kali Linux | Session 4142 • Blowing in the Wind: Security & Privacy within Mobile Applications and Use of the Cloud |
| 1:45 p.m. to 3 p.m. | Session 4240 • Data Privacy in the Cloud: Are You Protecting Your Customers and Employees? | Session 4241 • Architecture of Global Surveillance | Session 4246 • Are REST APIs Inherently Insecure? | Session 4242 • Improving Mobile and Mobile Application Security with Hardware Roots of Trust |
| 3:30 p.m. to 4:30 p.m. | Session 4340 • Building Secure 'Open Clouds': Security Dynamics of Utilizing Integrated Open Technologies in Provisioning Next Generation Clouds | Session 4341 • How to Make a Security Awareness Program Fail | Session 4346 • Do You Have a Mature Application Security Program? | Session 4342 • Bring Your Own Destiny: The End of Mobile Privacy Expectations |

Conference schedule subject to change.

CONTINUED ON PAGE 13

| SCHEDULE AT-A-GLANCE (CONTINUED FROM P. 12) | Governance, Regulation and Compliance | Threats— Inside and Out | Forensics | Malware | Healthcare Security |
|--|--|--|--|--|---|
| MONDAY, SEPTEMBER 29 11 a.m. to 12 p.m. | Session 2148 • Civilianization of War: Paramilitarization of Cyberspace and Its Implication for Civilian Information Security Professionals | Session 2143 • Executing Converged Attacks | Session 2147 • TBA | Session 2144 • Malware Analysis 101 - N00b to Ninja in 60 Minutes | Session 2145 • Medical Device Security as Part of the Overall Risk Management Process |
| 1:45 p.m. to 3 p.m. | Session 2248 • Ripped from the Headlines: What the News Tells Us About Information Security Incidents | Session 2243 • How to Hack a Bank | Session 2247 • App Analysis and Finding the Hidden Data During a Forensic Exam of a Smartphone | Session 2244 • MAC Pwnage | Session 2245 • Healthcare Case Study—Anatomy of a DLP Incident |
| 4:30 p.m. to 5:30 p.m. | Session 2348 • Security Decay: Identify and Manage Failing Security Before Security Fails | Session 2343 • Hacking Critical Infrastructure: From Cyber Myth to Startling Reality | Session 2347 • Bitcoin Forensics Analysis | Session 2344 • The Wonderland of Malicious Social Networks | Session 2345 • TBA |
| TUESDAY, SEPTEMBER 30 11 a.m. to 12 p.m. | Session 3148 • Dude. Again? Really...? | Session 3143 • Getting Smart about Threat Intelligence | Session 3147 • Critical Infrastructure Attacks and Forensics | Session 3144 • TBA | Session 3145 • Five Common Mistakes Most Healthcare Security Programs Make—and How to Fix Them |
| 1:45 p.m. to 3 p.m. | Session 3248 • Building an Agile Risk Assessment Program—Keeping Up with the Pace of Hackers | Session 3243 • Orlando Doctrine: Bringing Balance to the Asymmetric Threat | Session 3247 • What is Hiding in the Virtual Environment Host Memory Space and Should We Be Worried? | Session 3244 • Lessons Learned from Managing Malware Attacks | Session 3245 • The Evolving Cyber and Insider Risks of Healthcare—10 Things Every Healthcare Organization Should Know |
| 4:30 p.m. to 5:30 p.m. | Session 3348 • What the Behavior of Children Today Can Tell You About Tomorrow's Risks | Session 3343 • Supply Chain: The Exposed Flank | Session 3347 • Cloud Computing Forensic Challenges | Session 3344 • The Mad World of POS Malware | Session 3345 • Dodging Breaches from Dodgy Vendors: Tackling Vendor Risk Management in Healthcare |
| WEDNESDAY, OCTOBER 1 11 a.m. to 12 p.m. | Session 4148 • Holistic Vendor Risk Assurance: A View from the Trenches | Session 4143 • Advanced Red Teaming: Ghosts in Your Building | Session 4147 • Windows 8 - File-history Exfiltration Artifacts | Session 4144 • Malware Analysis for the Incident Responder | Session 4145 • Survey: Security-Related Issues of Wirelessly Connected Implantable Medical Devices |
| 1:45 p.m. to 3 p.m. | Session 4248 • Advances in Continuous Monitoring As an Integrated Component of Cybersecurity Management | Session 4243 • Tired of Being Hunted? Targeted Attack Detection, Analytics and Mitigation | Session 4247 • Cryptographic Backdoors | Session 4244 • Zeus Command and Control, for Fun and No Profit | Session 4245 • Cybersecurity and Networked Medical Devices: Assuring Patient Safety and Managing Risk |
| 3:30 p.m. to 4:30 p.m. | Session 4348 • Cyber Investigations without Borders | Session 4343 • Advances in Cross-Domain Threat Modeling | Session 4347 • Incidents are Against Our Policy: Conflicts Between Good InfoSec and The Forensics/e-Discovery Process | Session 4344 • Demystifying Malware & Unmasking Its True Risks | Session 4345 • Moving Healthcare to the Public Cloud |

12th Annual



Alta Associates'
**Executive
Women's Forum**
Information Security, Risk Management & Privacy

*Invest
in
Yourself!*
.....
ROI

EARN
UP TO 19 CPE CREDITS

BUILD A NETWORK
OF THE
MOST DYNAMIC WOMEN
IN OUR INDUSTRY

TAKE HOME TOOLS,
BEST PRACTICES
& SOLUTIONS TO
ACHIEVE SUCCESS

Women of Influence Awards

Nominate your peers, clients
and customers for the
Women of Influence Awards.

Co-presented by CSO Magazine and
Alta Associates, the awards honor four
women for their accomplishments and
leadership roles in the fields of security,
risk management and privacy.

Winners will be announced at a
ceremony during the EWF event.

**FOR NOMINATION FORM
GO TO: www.ewf-usa.com**

**Nominations must be submitted
by July 31, 2014**

October 21-23, 2014

Hyatt Regency at Gainey Ranch | Scottsdale, AZ

Protecting Brand, Data & the Internet of Things

A summit to build and enable forward thinking
Information Security, IT Risk and Privacy leaders.

Big Data – Big Opportunity

Hear how companies leverage agile analysis and acquire the skills you
need to distill complex ideas into an enterprise-wide call to action.
Gain an understanding of how big data analytics will change all of us.

The Yin/Yang of IdM & IoT Identity management in a ubiquitous world

Managing complexity is more than a word game. Learn how to manage
identities with devices that might be swallowed by a person, or part of a
general consumer ecosystem yet still inextricably connected to your
company's reputation and stock price.

Cyber Risk: This is not your father's playbook

Run and hide or stand and fight? This interactive panel will consider
hacktivism, reputation management and practical mitigation strategies
which reflect today's realities.

How Did I Get Here?

A C-level executive walks us through her journey to success, and
explains the twists and turns, skill and luck, and surprises along the way.

FORUM HOST &
AWARDS CO-PRESENTER



FORUM HOST &
AWARDS CO-PRESENTER



DIAMOND SPONSORS



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



TEACHABLE
MOMENTS FROM
(ISC)² SECURE
WEBINARS
AND EVENTS

MODERATOR'S CORNER > BRANDON DUNLAP

BYOD

Why you need to know your legal exposure

JUST AS THE adoption rate of enterprise mobility has accelerated in recent times, so have the definitions of the risks that it brings. Where we once had granular control over the mobile devices within our user community, with corporate-issued devices and the homogeneity and (relative) ease of management that they afforded us, those times have changed dramatically.

Whether forced upon us from the top down in the name of cost savings or from the bottom up in a user-driven campaign, we have been slower to react to the legal risks than we have to the legal exposures. Perhaps this is due to the technical roots of our profession, or maybe there is a knowledge gap in how we identify and communicate risks outside of our immediate area of comfort. But one thing I am sure about: the legal frameworks that we are dealing with are just now beginning to address this wave of change.

Brandon Dunlap is Managing Director of Research for Seattle-based Brightfly. He can be reached at bsdunlap@brightfly.com.

Earlier this year, on our Security Leadership Series ThinkT@nk, “[From The Trenches: BYOD Program Deployments](#),” I had the pleasure of interviewing Matt Pellowski, Support Services Manager at Capella University; Chris Trautwein, former CISO of (ISC)²; and Keith Young, ISO of Montgomery County, Md. All of these experts shared their real world experiences in rolling out a BYOD program.

This session offered interesting insights into the drivers and technological implications of a BYOD program (some of which are included in this issue’s feature article on the same subject). But this barely scratched the surface of the legal and sometimes ethical issues that can arise from such a tectonic shift in how we address user-computing needs.

As with other live events where I develop material, I do extensive research on the topics we bring to you every month via the

Web. I often turn up surprising and useful items as I wander the Internet. In the past, I have kept my notes and references largely to myself, but today, I thought I would start sharing that material so you can explore to the depth that best suits you.

“We have been slower to react to the legal risks than we have to the legal exposures.”

I have started curating articles on BYOD legal, privacy and technology issues using [Flipboard](#). You can browse my research files on BYOD here. I also maintain another “magazine” of news and informational sources on [Social Media and Privacy Issues](#), which intersects with mobility at an increasingly alarming rate. Let me know what you think of these resources, and feel free to send along any interesting topics or articles that you think might better inform my moderation of future events. I’ll add them to the magazines for all to see.

One more thing before I leave you to the rest of this issue: Do you have a story to tell? Do you want to be on an upcoming panel? Drop me a line. We are looking to get you involved!

Until we meet again online, I look forward to continuing the conversation. ●



Certified Cyber
Forensics Professional

THE STANDARD in CYBER FORENSICS

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 (CCFPSM) 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





the future is IN OUR HANDS

**EXPERTS REFLECT
ON WHAT'S
WORKING AND
WHAT'S NOT IN
BYOD SECURITY**

BY **MICHELE KRIEGMAN**

THE PHILOSOPHER KNOWN as George Santayana more than 100 years ago warned, “Those who cannot remember the past are condemned to repeat it.” So let’s imagine for a moment that we’ve fast-forwarded into the future, where information security practitioners are looking back on 2014 and specifically at the BYOD world, where “bring your own device” to work is common and even company-issued devices are routinely used for personal tasks.

Will this year’s gains in the battle against mobile malware and data loss be later viewed as valiant but now outdated efforts? Or can we learn

from what's working presently, what isn't, and which strategies promise traction to meet the next iteration of mobile threats?

InfoSecurity Professional magazine asked a group of IT security veterans whose expertise spans financial services, telecommunications, and pharmaceuticals to highlight what from our immediate past (and present) can be applied strategically and tactically over the next five years to secure a safe platform for those who carry their lives in their hands.

These are predictions, not promises, and several in our group pointed out that IT security is probably the most dynamic area within the broader technology space.

What countermeasures are we implementing today that will improve our immediate future?

LESSONS LEARNED: FIVE SILVER BULLETS...THAT HAVE BEEN SPENT

Here are five solutions currently employed to reduce the risk of mobile malware and improve mobile device management. If our CSOs and CISOs are correct, not all will end up working as well as planned.

1 Remote wipes

The technology behind remote wipes, in which sensitive data is remotely removed from a lost or stolen device, has been around for a while.

But the technique continues to have serious limitations when mobile device management (MDM) expands to include employee-owned devices with employee-owned content.

There have also been legal challenges to the technique, according to Brandon Dunlap, managing director of Research at Brightfly, Seattle, Wash., U.S.A., in an (ISC)² ThinkTank BYOD webinar.

Jim Klinck, chief security officer of ProSight Specialty Insurance, Morristown, N.J., U.S.A., after serving in executive leadership positions at AIG, ALICO, and MetLife, believes that with the proliferation of wearable devices, legal rulings discussed elsewhere in this article will see more play: "As access moves to iWatch or clothes it will only get harder to build security policy around wiping a personal device."

He points out that, "as an individual, I'm not comfortable with a remote wipe of my granddaughter's photo," and from a corporate standpoint, "the security focus needs to be on apps. The employer encrypts the app and

maintains the right to disable that app," thereby shifting away from full hardware wipes. By encrypting an app on an employer-issued device, a company can disable access or disable a device's instance of the app.

Timing is also critical when it comes to remote wipes. A lot can happen before someone notices a device is gone.

Just ask Keith Young, information security officer for Montgomery County, Md., U.S.A. He recalled during a recent (ISC)² webinar how a BYOD security fail that took place at a well-known security conference.

"The security controls that we thought would be effective, weren't. An individual had her cell phone stolen. We noticed [it] in about a minute of it being stolen. Being the IT professionals that we were, we, of course, went looking for that phone and found that in less than 10 minutes, the thieves already had the SIM chip out and had taken all the information. So thinking that there's going to be a golden bullet for any of these MDM solutions, whether they be traditional mobile device management or containerization, is not really true. You have to weigh the effectiveness of the controls as you implement them."

2 Dual containerization and encryption

Young's anecdote leads to another approach that has spread from its origins with the Java sandbox to "encapsulate data in a container requiring login for that specific use in addition to device authentication," said John R. Morgan, director of Capacity Planning at Horizon Blue Cross and Blue Shield of New Jersey, U.S.A. The company recently launched its ACA (Affordable Care Act) portal, which means that its customers can now access highly sensitive data from any device with a Web browser. Morgan served as a de facto security architect on that massive project and voiced concerns about what can happen if patients or insurance customers are allowed to store private data on a mobile device.

That's why he would limit containerization to instances where it's necessary to forgo the design ideal of "never having PII [personally identifying information] or PHI [personal health information] on devices and instead have all data in a datacenter with a secure connection." By their very ability to be easily lost, stolen or shared, handhelds or wearable devices grow the number of threat vectors exponentially.

3 SMS

Cynthia Cullen, whose IT security career spans Citi, Bristol-Myers Squibb, SAFE BioPharma Assoc., and Telcordia, believes two-factor authentication is bound to be a prime target.

Employees “use short message service as an out-of-band authentication on the assumption that the phone network is secure. This vulnerability leads to a false sense of security at the core of multi-factor authentication.”

For example, for secure access using BYOD, a company might require a user to enter a VPN token code or PIN and then text a second password using SMS over the phone line. However, that phone line, far from providing secure, second-factor, out-of-band communication might actually introduce a second threat vector if the phone line itself isn’t adequately protected.

4 The budget argument

BYOD has been embraced by management as a tool to raise employee productivity and also lower costs. Consumers, too, now expect mobile access to company websites and online tools, which at least theoretically saves on back office support costs.

That, according to Morgan, is both good and bad.

His company’s massive portal project did not come cheap because it had to be built with mobile users in mind. This meant a mechanism to detect and authenticate mobile devices and then be sure presentations rendered correctly on smaller screens. “We had to broaden our support matrix and testing bed for all mobile devices,” which added new costs.

However, Klinck noted that mobile isn’t going away, despite price point concerns. “In a niche company, there’s a lot of interest in mobile because it is a differentiator. It’s not just a sideline but an important part of what we plan to deliver, how we architect and provision data, and design the UI of devices.”

5 Silence isn’t golden

For at least the last two years, mobile malware has been at the top of many quarterly and annual threat lists. This is no surprise, given consumers’ growing reliance on devices and fascination with wearables like Google Glass. Mobile apps in particular have been a handy tool for hackers to infiltrate devices and mobile networks. It doesn’t help that convenience still trumps security and privacy concerns.

Some breaches and malware make the evening news; others don’t. And, of course, the most successful hacks go undetected for as long as possible. This can give end-users a false sense of security.

“I’m worried if we’re not seeing or hearing anything,” said Horizon’s Morgan. “They are there, so it could mean they aren’t being detected.”

Security was top-of-mind when Horizon BCBS was building its ACA portal, which fared better than the U.S. government’s health insurance website during its initial launch.

“We performed very well. Anybody who logged in was able to do so. We accomplished ‘available and functioning’ on 70 to 80 percent of Tivoli graphs [and] BMC patrol agents. No sessions timed out. No users were forced out because the site was busy.”

Yet at the same time, “There are always security alerts coming up on consoles, but there were no compromises. There were none deemed security events regarding the portal since the portal was launched. We did constantly monitor. Patch levels, for example, are always an issue, staying on top of them.”

Silence isn’t golden may be the corollary to that other security industry warning: “It’s not if, it’s when you’re hacked.”

STRATEGIES FOR MOBILE SECURITY

As the complexity of security environments threatens to outpace yesterday’s solutions, there are already mobile strategies on the horizon to meet new risks. Some current mobile security strategies are gaining legs.

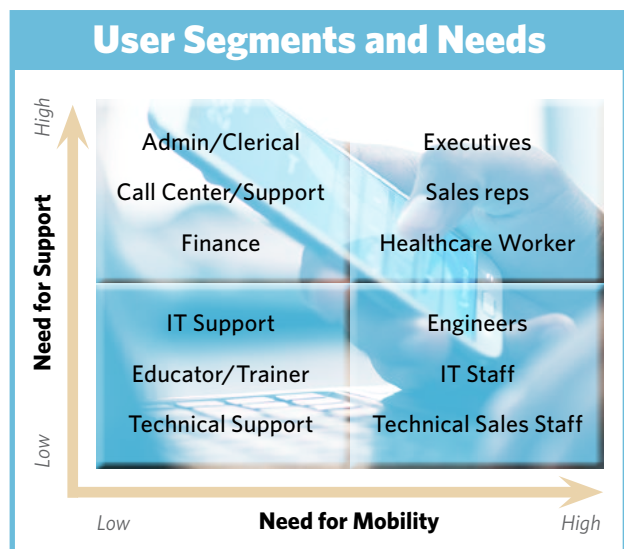
We asked each of the interviewees, “Looking ahead five years from now, what strategies are you putting in place now that may prove to be the most important from a mobile information security point of view?”

Here are their answers.

Risk-based approach. “[A risk based approach] is what I will be focusing on and where a new company can rethink and do things differently,” explains Jim Klinck of ProSight. “A lot of traditional security programs only say we’re going to block all access to this, or all access to that, with global policies, but increasingly, security needs to be risk focused. Direct IT security spending on focused, high-risk areas.”

As a starting point for balancing security and other support costs against benefits of mobility, Cisco Systems’ Neil Anderson, director of Systems Architecture, Sys-

tems Development Unit, in 2012 created a suggested needs quadrant to prioritize user segments:



Segmentation and subnetworks. Segmenting users is becoming more common, as is the idea of using subnetworks to enhance security. Klinck elaborates: “We’re seeing a trend toward more isolation, with internal subnetworks. One example is that IT doesn’t need to be on the same subnetwork as production servers.”

In a sense, this is a more mature version of what he describes as the historical IT concepts of “blocking, stopping, and preventing.”

Security analytics and a single pane of glass.

A competing security strategy is the combination of security analytics and its related concept, monitoring through a “single pane of glass.” Cultivated from the disciplines of database marketing and data mining, “security analytics” uses artificial intelligence and pattern analytics to identify trends and anomalies of behavior.

Klinck explains: “Rather than blocking someone from doing something, I’ll also need to look at patterns of behavior. Once we move further in that direction, breaches will be detected through behaviors that look different from those of a normal user. A good strategy will have been the use of the big data analytics, like Hadoop and others, for huge volumes of data. The more you can do that real time, the better and faster you can respond to a problem.”

But to increase the transparency of these metrics, Horizon’s Morgan found that security architecture

almost had to be monitored through what he calls “a single pane of glass.” “There are multiple control points to watch for intrusion. We had a lot of tools and capabilities, but were fragmented. There’s been a trend to do that in the operational space where all tools consolidate to one point like a network operations center (NOC). They’re also watching MF, network availability, storage performance, application availability. Any alerts could go there.”

Cullen points out that the lack of a consolidated view may prevent adequate incident management, noting “...the big challenge is going to be honing big data back to useful information with few false positives. In the Target security breach, for example, the Fire Eye product was able to detect the malware and send an alert to the security operations center (SOC), but they didn’t act. We don’t have the big picture on false positives to know if that crucial alert was one in tens of thousands that day or one in a few.”

Single Sign-On (SSO). There is no silver bullet but, “there’s a lot right with single sign-on as an open solution that contributes to security,” says Klinck. “That, along with Active Directory and its controls—so it’s changed on a regular basis—is probably the closest thing we have to a silver bullet for a newer company.” These controls fall under P & P for Access & Identity Management (AIM), such as requiring regular changes of passwords and regular updates to the access control lists (ACLs).

SSO facilitates the new trend of federated data centers or a hybrid cloud. “There’s a non-intuitive axiom: as more technologies emerge [including mobile], it doesn’t make sense to run your own data center,” says Klinck. “We have a hybrid cloud contracted with vendors. We offer users SSO with unified password rules, despite behind the scenes going to different cloud providers.”

Cloud security. Devices can be stolen, along with any files or data on them. Klinck refers to this vulnerability as the “what’s-left-sitting-on-the-device risk” because whatever’s left sitting on the device instead of (what’s believed to be more) secure in the cloud is more easily stolen.

Former (ISC)² CISO Chris Trautwein uses the cloud to treat files as protectively as an app, creating a model whereby a device uses a Web interface to access anything of value regardless of whether it’s an app or even a

file. Users are slightly more accustomed to using an interface to access an app remotely, but less so with a file.

This security architecture has been called “thin client” when applied to traditional office computers. So now that we are treating mobile devices this way, too, we can think of them as “mobile-device-as-thin-client.”

Young concurs that, more often, this will be the trust model where “we have to treat our internal environment almost the same as the Internet...to meet a low protections/high needs environment. Our recommendation is to use these devices for the cloud and to not store data on the devices themselves.... Treat them as if the users are sitting in a Starbucks or a McDonald’s and give them access at that trust level.”

Mobile security standards for the secure software development life cycle. Cullen says that the concept of defense in depth or “security by design” faces new obstacles, “through the secure software development life cycle (S-SDLC) process at corporations. Where OWASP has defined and fleshed out how to secure Web applications, there’s no counterpart deep dive for mobile

apps to define threats, mitigate them, and design tools to address them through the S-SDLC.”

Of course, several experts note that before any deployment, you must gain buy-in further down the SDLC.

According to Matt Pellowski, Support Services, Capella University, speaking at an (ISC)² webinar, “One of the best things we did was before we announced this out. We had focus groups come in and I showed our MDM solution up on the big screen, and I said, ‘I’m going to open this up and let you see what’s on my call. I cannot see personal emails outside our servers. Here’s what we can and cannot see.’ It really did something for that trust level for a really good roll out.”

Ease of Use = More Security. “The easier you make it for a user to use a device securely, the more secure the device is,” explains Klinck. “If it’s too difficult to use, that’s when we’ve found that humans will program around it.”

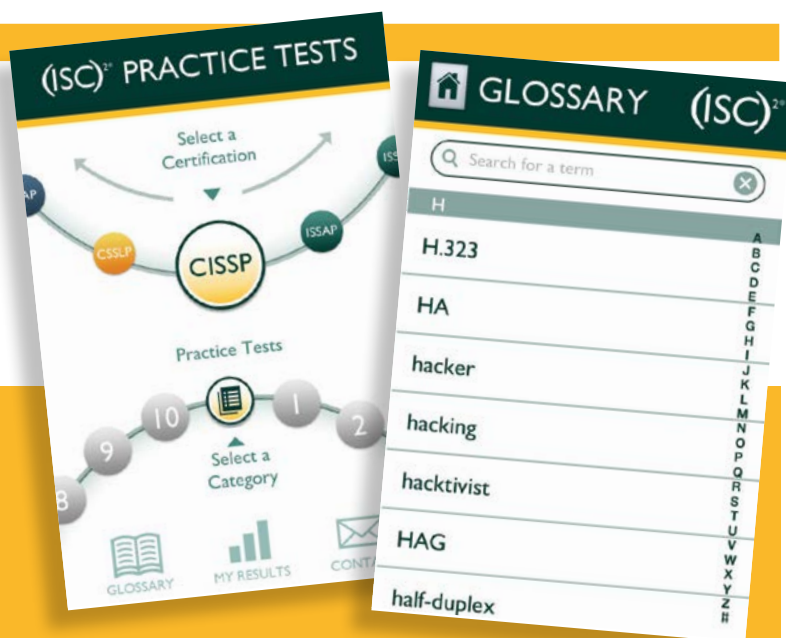
A growing trend will incorporate design and user experience (UX) as components of successful security design.

Access the (ISC)² Glossary of Terms

Download the glossary of terms for **FREE** on the (ISC)² Practice Tests App. Available on iTunes, the app contains a glossary of nearly 5,000 information and software security industry terms. The terms have been pulled together from the (ISC)² Press Library, Auerbach’s glossary definitions and commonly used industry terms and acronyms.

Test your knowledge on-the-go with the in-app practice tests available. Whether you are keeping up your knowledge in the field or studying for an (ISC)² exam, access practice tests for the CISSP, SSCP, CAP and CSSLP for a nominal price.

Download the (ISC)² Practice Tests App at www.isc2.org/practice-tests-app



(ISC)²®

AS TECHNOLOGY CHANGES, SO DOES CASE LAW

Everyone with a CISSP—and many without—already knows that the legal and regulatory foundation for data protection and information security has been out there for a long time, with a wave of formulations that date back to the Computer Fraud and Abuse Act of 1986.

Brightfly's Brandon Dunlap notes that, by depending on the specific mix of device ownership, socialized corporate security policy and technology, companies could run afoul of that early law. A complete remote wipe of the content of an employee's personal mobile device, a tactic to prevent theft of valuable proprietary data, could violate the Computer Fraud and Abuse Act if it "knowingly...exceed[ed] authorized access," on what is deemed a "protected computer."

New wage concerns regarding hourly workers exist specifically where BYOD policies enable employees to use their personal devices for company work and access to company data and communications. If they respond to a work email sent to their device outside of

company hours, is the employer subject to ceiling-less hourly charges? The solution has been to limit BYOD to salaried employees only.

But as mobile technologies reach more employees' hands, case law, policy solutions, and important debates will emerge that reinterpret existing frameworks into workable legal architecture. In early 2014, the White House issued more guidelines on data privacy. This followed an initial effort in 2012, bringing U.S. standards perhaps more into alignment with EU data privacy principles that already impact many U.S.-based global corporations.

And as individuals and governments demand more privacy controls, (witness the EU court's ruling calling for Google to remove personal information on demand), increased vigilance against exploiters, hackers, and cyber criminals will be needed. ●

MICHELE KRIEGMAN, CISSP, is a New Jersey-based IT risk and security professional supporting mobile and social media, business operations and marketing.

Concentrate Your CISSP® Wherever you may happen to be...



with (ISC)²® Live OnLine Training

Join Today!

MOBILE MALWARE

OLD TRICKS ON NEW PLATFORMS BY CRYSTAL BEDELL



W

ITH ANY INNOVATION, once the next new thing takes hold, the criminals are right there, finding ways to exploit it for their own ends. The current target: the ubiquitous mobile device.

Ask three malware researchers what poses the biggest threat to mobile device users and you'll get three different answers. But while they might not agree on what constitutes the biggest threat or the rate of mobile malware growth, they can agree on two things: Android is the favored target, and mobile malware is increasing.

In 2011-2012 we had around 100,000 malicious samples in our database. Now we are approaching one million,” says Filip Chytrý, malware analyst and operator at AVAST Software, based in Prague, Czech Republic.

MORE MOBILITY = MORE VULNERABILITY

The growth of mobile malware shouldn't be a surprise, given the boom in mobile device use.

According to “Worldwide Mobile Phone Users: H1 2014 Forecast and Comparative Estimates,” a report by the digital research firm eMarketer, the global smartphone audience surpassed the 1 billion mark in 2012. This year, it will total 1.75 billion. In addition, 48.9 percent of mobile phone users will go online via their mobile phone at least once a month in 2014. Security professionals know: Cyber criminals go where users go.

“As mobile devices become more prolific, malware writers will continue to shift [their efforts from desktops to mobile devices].”

—TYLER SHIELDS, senior analyst for mobile security and application security, Forrester Research

“As mobile devices become more prolific, malware writers will continue to shift [their efforts from desktops to mobile devices],” says Tyler Shields, senior analyst for mobile security and application security, Forrester Research, Cambridge, Mass. U.S.A. “While I don't always agree with all of the numbers that AV vendors put out about quantity of malware, I do agree that the trend is upward going. ... It's not a matter of if it will hit critical point, more of a matter of when.”

A growing user base is one of the reasons why, experts say, malware writers are targeting the Android platform.

“We're seeing a much larger increase in malware in the Android world versus Apple iOS,” says Paul Martini, co-founder and CEO of iboss Network Security, San Diego, Calif., U.S.A. “It might be due to Android

becoming more popular. Apple [also] tends to control more of the iOS platform. They have much stricter guidelines. Google has the Android Play Store and it's vetted, but the platform is open.”

THE COST OF OPENNESS

SMS is the primary attack vector today, according to Julian Evans, mobile security specialist and co-founder of ID Theft Protect, based in Peterborough, UK. Automated SMS phishing and geographic SMS phishing are being carried out on Android devices.

“It's difficult to do on iOS if the device is not jail broken,” he explains. “The Android platform being slightly more open means that it's more vulnerable to [phishing] attacks. Even if the device isn't rooted, there's still a chance to deliver a drive-by download.”

Phishing and drive-by downloads are just two examples of malware writers adapting familiar techniques for mobile devices—a trend that is likely to continue.

“Anything that's ever worked on desktops in terms of malware and threats is probably going to make its way to tablets,” warns Roger Thompson, chief emerging threats researcher at Verizon's ICSA Labs, Mechanicsburgh, Penn., U.S.A. “The biggest example is ransomware. We have also seen fake AV software already on Android devices, which is another big money-maker for the Windows world.”

The difference lies in how these threats are executed. On a Windows desktop, Thompson explains, the threats exploit a vulnerability or leverage social engineering to convince the user to take some type of action. In the Android world, however, Thompson points out that cybercriminals are primarily using social engineering. CryptoLocker-type malware, or ransomware, is an example.

“If you're unlucky enough to run CryptoLocker-style malware, it encrypts everything on your machine, and locks it up, and tells you that such-and-such police department has found illegal content on your machine, and you are hereby ordered to pay a fine of \$350,” explains Thompson.

He adds that the message is customized to reflect the user's currency and local law enforcement. “It looks like you've been caught and have to pay a fine to get your phone back. [This type of malware] has been lucrative on PCs, and it's made its way to Android.”



MORE NOVELTY NEEDED



“THE BIGGEST PROBLEM facing vendors is that malware analysis is going to need improving,” cautions Julian Evans from ID Theft Protect. “We’re looking at both the client and the carrier, embracing machine-to-machine learning, [and] how to trigger malware and develop a dynamic detection capability.”

According to Tyler Shields, a senior analyst at Forrester Research, machine learning enables analysis within context, and

therefore enables the detection of malicious behavior, like a malicious application piggybacking off legitimate permissions.

“The cutting-edge technology that allows you to detect malicious behavior is along the lines of machine learning,” he says. For example, running an application in a sandbox, looking at the behavior and using machine learning to classify whether it is potentially malicious.

“There are some vendors that do application reputation systems that are doing a good job of finding malware before it attacks your system,” he continues. “The other option is to get down into the secure network gateway layer and apply machine learning to network traffic.”

Martini says iboss Network Security’s Secure Web Gateway uses behavioral data profiling to

establish a baseline of how much data an application or system sends out, and to trigger alerts when the amount of data exceeds a threshold.

Thresholds can also be configured by country. So, for example, an administrator can be alerted if outbound data to Russia exceeds five megabytes.

This is similar to the contextual and risk-based mobile security management Shields says enterprises can expect to see from vendors in the future: “Vendors will look to do more machine learning and behavioral analytics on the network, operating system and application tiers to quantify the risk rating of each tier.”

This will enable organizations to apply security controls based on the risk level and keep the malware infiltrators at bay. ●

—Crystal Bedell

UNWANTED “BONUS” AT THE APP STORE

One of the easiest ways that malware writers infect mobile devices comes not from the desktop world, but from a concept born out of the mobile world.

“Malware writers recognize that embedding one piece of functionality in an app is the easiest way to get massive infections,” says Shields.

“A popular game gets thousands of downloads and can impact a lot of users.” Malware writers download a popular app, break it apart, insert malware, repack the app and place it in a third-party app store, he explains.

When installing a mobile app, users are prompted to give the app permission to access data, like contacts, email, GPS location, etc., on the device. An attacker may modify the application to access data for malicious purposes, say, to track user activity or steal passwords to bank accounts.

“Users just want to fling birds at pigs. They don’t care about permissions, and that’s a big part of the

problem,” says Shields. “That security control model is ineffective because people just don’t pay attention to it. Once you give permission to the app, the app can do whatever you gave it permission to do.”

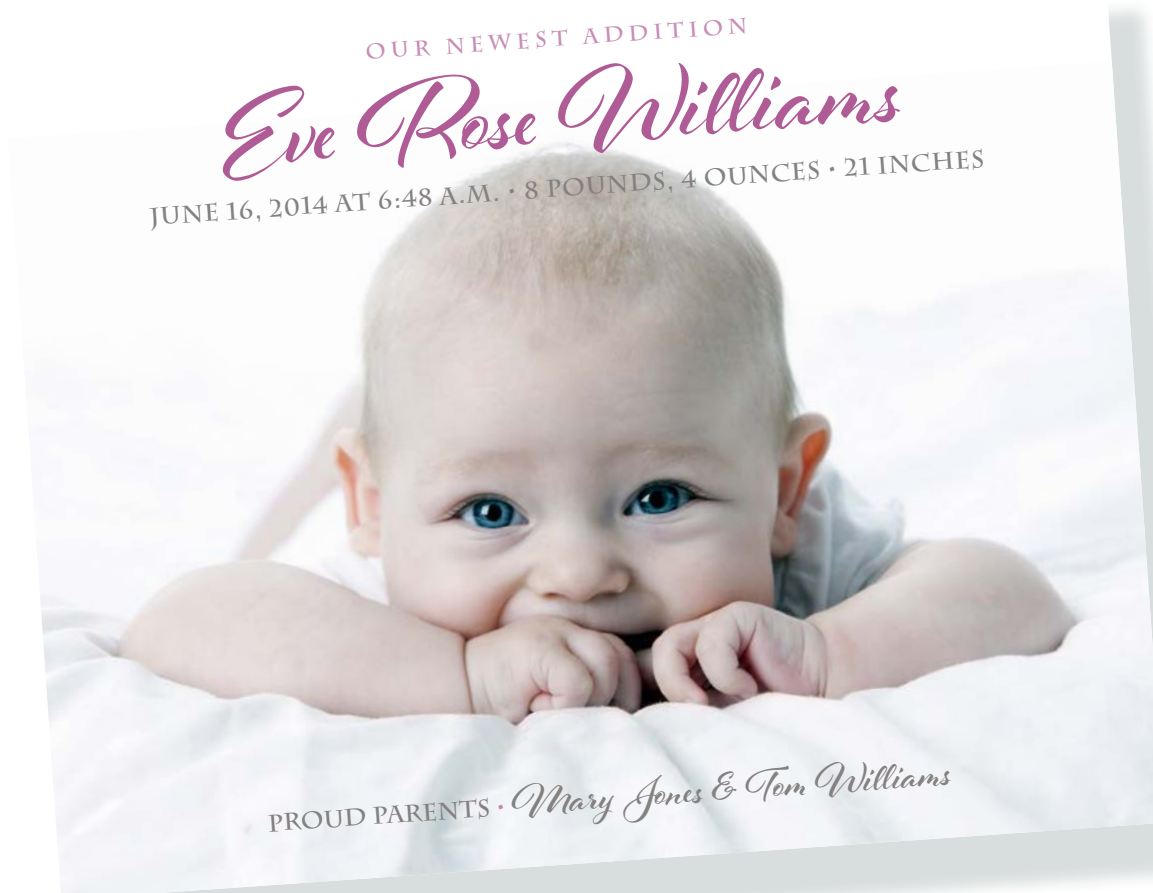
This could mean providing full access to whatever is on the device. “Mobile devices are like personal diaries—location, web search, social media—all this data is like a treasure if you know where to sell and [how to] misuse them,” advises Chytrý.

But preventing mobile malware in this case is not as simple as denying an application permissions, Shields explains. Some apps, like a voice recorder, may have a legitimate need to send the user’s data to a remote server or access the user’s contacts.

“Contextually, that might make sense because maybe I want to email the recording,” he says. ●

CRYSTAL BEDELL is a Spokane, Wash.-based technology writer and regular contributor to InfoSecurity Professional magazine.

WATCH AND SEE



A CYBER CIVIL RIGHTS ADVOCATE SHOWS HOW WE'VE CREATED A GENERATION OF AT-RISK YOUTH BY RAJ GOEL

TECHNOLOGY HAS ALWAYS existed at the intersection of hope and fear. At the dawn of the Internet age, we dreamt of a world without borders or boundaries for information routed around censorship. Several decades later, we now live in a world that closely resembles the United States television series "Person of Interest," in which we are constantly under surveillance by governments, corporations, law enforcement, our neighbors, and even our family members.

Not only does this erode our expectations (and rights!) to a certain level of privacy, but the vast amounts of data gathered in the course of such omni-

present surveillance also puts us at a much higher risk of fraud and identity theft.

But some of the outrage needs to be directed inward as we, the consumers, continue to aid and abet cybercriminals through personal data paraded on social media and handily offered to mobile apps, just to name two popular practices.

So what about a child born in 2014, who enters this world without much to trace? What information do we need to conduct ID theft or potentially ruin their reputations before they've even said their first word?

Not much.

WAYS PARENTS AND FAMILY MEMBERS GIVE UP THE GOODS

At a minimum, we need five identifiers to impersonate someone else online or over the phone:

- Mother's maiden name
- Date of birth
- City of birth
- Name
- Phone

Long before a child is born, his parents may have married and announced their nuptials a number of ways, from a formal wedding announcement in the local newspaper (with an accompanying website) to an online site that advertises an engaged couple's wedding plans, including the couple's full names, date of the marriage and location of the wedding. This is how we acquire a mother's maiden name, provided she changed it after getting married; it is not uncommon now in many countries for women to retain their maiden names for personal or professional reasons.

More and more, prospective parents are sharing "Save the Date" or "We're Expecting" announcements. This does not give us a date of birth, but an ID thief now knows around what time to monitor a feed or local newspaper for the official announcement of the arrival. And, of course, social media plays its part by having both major and minor life events (from engagements and births to posts about how a couple first met) advertised on Facebook, Google+, and other sites where stricter privacy settings are often ignored.

As soon as the baby is born, you can expect proud parents or grandparents to send out the "Welcome our Little One" cards, posts, tweets, etc. And even in the age of HIPAA, hospitals across the United States and other nations proudly share the newborn's name, date of birth, parents' names, and in some cases, names of siblings and health care practitioners involved in the delivery.

This is how we acquire the child's full name and city of birth.

Finding a household's phone number that the child eventually "inherits" is just a Google search away, thanks to the many "people finder" services that search engine algorithms seem to love.

HOME IS WHERE THE HEART HACK IS

So, is our baby safe in his/her home?

Not really. More and more, parents are turning to technology to help manage their baby's care. And most consumer-grade equipment was never designed with security in mind.

Just ask Heather and Adam Schreck of Cincinnati, Ohio, U.S.A., who were woken at midnight to a man shouting, "Wake up, baby! Wake up!" in their 10-month-old daughter's room.

Adam ran to the bedroom and found the shouts coming from a Foscam IP Camera aimed at the crib. The camera turned to face the startled father. "Then it screamed at me," Adam told a local television reporter. "Some bad things, some obscenities. So I unplugged the camera."

Most baby cams, baby monitoring systems, and other consumer devices come with either no passwords, default passwords that are never changed, or vendor-coded back doors that can never be secured.

And not every hacker makes his secret presence obvious by screaming at the occupants.

SCHOOL DAZE

School shootings worldwide have led more communities to implement student monitoring systems at public and private campuses to record who comes and goes from buildings or who approaches students on school grounds. Rarely, if ever, do parents balk at the increased safety measures.

But it's a different story when it comes to technologies like InBloom, a database initiative largely funded by the Bill & Melinda Gates Foundation and built by Rupert Murdoch's News Corp. The technology, which as of last year was adopted in nine states, creates a centralized database where student records, from attendance to disciplinary to special needs, are stored. New York City parents, including the current mayor, expressed outrage upon learning that the data could be sold to private companies.

Civil rights groups took immediate legal action to try and prevent the practice of disseminating student data—a practice that also had been taking place in Colorado, Delaware, Georgia, Illinois, Kentucky, North Carolina, Massachusetts, and Louisiana by the time the New York uproar began.

In April 2014, InBloom announced it would shut down.

WORD OF MOUTH

Marketers know that children and teenagers are a financial goldmine. They are easily influenced by advertising that can lead to lifelong brand loyalty. And they love to tell their friends, providing the kind of peer pressure corporations—and data mining dynasties like Facebook, Google, and Twitter—love. Their choices, and choice words, leave a lasting impression—which some come to regret.

That's one reason more and more (ISC)² members are volunteering for the (ISC)² Foundation's Safe and Secure Online program. Companies are not necessarily going to do right by our children, so we must teach them how to protect themselves when they use Web services and interact online and across public airwaves.

Because, as we adults all know, the Internet never forgets.

To paraphrase the U.S. Justice system's Miranda rights: Everything you say can and will be used against you, by anybody, now or decades into the future.

THE TRACKERS ARE ORGANIZED


So far, we've seen how we've put our children at risk just by being social, friendly, and even caring. But the child of 2014 will inherit governments that have the ability and perhaps the desire to conduct ubiquitous surveillance that could increasingly endanger privacy rights.

It's not just the NSA-funded programs that capture emails, chats, videos, photos, file transfers, login activity, social media profiles from a variety of entities including Microsoft, Facebook, Skype, Google, PalTalk, AOL, Yahoo, YouTube, Apple, AT&T, Verizon, Sprint, etc.

There are provisions in the United States Electronic Communications Privacy Act of 1985 that allow law enforcement to acquire email older than 180 days as well as certain online data with minimal judicial effort. These efforts were augmented by the post-9/11 U.S. Patriot Act. Civil and privacy rights advocates are continually challenging this latitude on the part of the government, but the children born in 2014 will have to learn to protect themselves.

And it's not just the U.S. federal government; law enforcement agencies in cities and towns across the country are beginning to invest in "StingRay"—a

Ways We Put Our Children at Risk for Fraud/ID Theft



The graphic features a series of black silhouettes representing a child's growth from infancy to adolescence. The silhouettes are arranged in a line, with the first being a crawling baby, followed by a sitting baby, a toddler with a ball, a young child, a pre-teen, and finally a teenager. The text 'infancy to teen' is written in a large, light green, sans-serif font across the bottom of the silhouettes.

| | | |
|---|---|--|
| ✗ Birth announcement in the local newspaper | ✗ Unsecured webcams/baby monitors | ✗ Social media monitoring/impersonations |
| ✗ Birth announcement on social media | ✗ School announcements in local newspaper or websites | ✗ GPS on mobileware |
| ✗ Online "people finders" to pin down addresses, family details | ✗ Parents' blogs | ✗ POS technology for target marketing |
| ✗ Posts on social networks | ✗ School databases used for marketing and research | |

technology that can mimic a cell phone tower, thereby intercepting mobile phone numbers. Warrants are not required because the device is collecting numbers, not actual conversations. And police departments are keeping mum about having the technology.

The car you drive and loan to your child is no longer just a vehicle in a stream of traffic. License plate readers, traffic cameras, and other community video functions are capturing license plate data every minute. That data is collected not only by police agencies, but by data collection firms (for sale) and auto repossession companies.

CELL ME SOMETHING I DIDN'T KNOW

It could be said that the cell phone is the best spying tool ever invented, and as users, we enable it and our children are learning to do it as well. GPS tracks our every move (and our children's). Cell phone logs show who we talk to and for how long. Our kids take pictures and share them with their friends on Instagram. Our phones can record what we say. There are apps, like CrowdPilot, that will broadcast our every word.

The cell phone quickly became part of our lives, and it'll be part of the lives of children in 2014 in ways we never even considered.

WHAT'S THE GAME?

So why are we being spied on, and creating a world constantly under surveillance for the children of 2014?

Some will claim "safety": The advantage of knowing where our children are, avoiding getting lost, keeping track of the bad guys, etc. But for most, it's about money.

Those ubiquitous shopping mall cameras track your every move, and point of sale technology notes your every purchase, whether it's cash, debit or credit. The value to the retailer is immense: by knowing your shopping preferences and those of your children, you can be easily targeted on birthdays, anniversaries, sales of your favorite items...all because of the data you've willingly shared.

Consider this true story from Charles Duhigg's best-seller, *The Power of Habit*: retail giant Target used its proprietary data profiling service to determine that a teenaged customer in New Jersey was pregnant,

based primarily on her purchase history. They began to mail her coupons for baby products and other materials for expectant mothers. The young woman's father called the store manager to complain that the mailings were inappropriate because his daughter wasn't pregnant. The store manager apologized profusely, believing the technology had malfunctioned. But a few months later, it was the father who was apologizing. Unbeknownst to him, his daughter was indeed pregnant and later gave birth.

That incident took place several years ago. What are we to make of the technological advances since? Everything poses a threat, from drones hovering over neighborhoods to our neighbors hovering over their own Web cams.

THE WATCHERS ARE EVERYWHERE

In London, our child will be photographed by the largest collection of government surveillance cameras in the world. In Russia, his/her telephone and email metadata content, as well as all Internet Wi-Fi, and social media traffic may be monitored by law enforcement.

Whether our children are at home or abroad, they are being watched—but not in the way a parent would prefer. On every continent, we live under the watchful eyes of governments, corporations, and other private entities. It is up to us as parents, citizens, and information security practitioners to help protect the most vulnerable segment of society: our children.

We cannot always compete technologically, but we can certainly do our part to spread awareness and to speak out, as parents in New York City did, when that technology goes too far and places our children in harm's way.

It's important that each of us, as information security practitioners and private citizens, teach the children and adults in our lives that no privacy rights exist on the Internet—not in Canada, the U.K., Russia, China, or even the international space station.

Welcome to the life of a child in 2014. ●

RAJ GOEL, CISSP, is a cyber civil rights advocate, author, and speaker who will speak about global surveillance architecture at this year's (ISC)² Security Congress September 29 - October 2 in Atlanta.

Giving Corner

FOSTERING GOODWILL,
EDUCATION, AND
RESEARCH INITIATIVES

MANY HAPPY RETURNS

Two Hong Kong CISSPs share their volunteering experiences. BY **JULIE PEELER**

SINCE 2006, the (ISC)² Safe and Secure Online program has helped professional volunteers sharpen their presentation skills, communicate effectively with a challenging user audience, gain front-line insight into developing behavior in cyberspace, and raise the profile of their chosen profession and the companies that employ them.

Those are a lot of rewards for the (ISC)² members who volunteer in the program.

We at the (ISC)² Foundation want to share the experiences of two Hong Kong-based volunteers, Carol Lo, CISSP, and Henry Lai, CISSP, to show the ways volunteering enhances career skills and raises professional profiles.

Carol's given two Safe and Secure Online presentations in recent months to 300-plus students in both primary and secondary schools.

"The biggest challenge [for me] was how to convey complicated IT concepts to people who might know nothing about the subject, especially when there are only 30 minutes to an hour to cover several cyber-related subjects," she said. "Putting myself in their shoes helped me think of a way to make the presentation relevant and interesting to the audiences.

"Being an inexperienced public speaker, I felt accomplished when students actively raised their hands to answer my questions. I knew it was impossible for them to memorize all the information on the slides. But, hopefully, they are now more aware of the cyber risks in the world and will take precautions against cyber crimes in their daily encounters.

"I enjoy this volunteer work so much and it's definitely provided me with a 'golden chance' to practice my public speaking."

Henry Lai gives weekly technology briefings to customers, so public speaking comes a bit more naturally. His biggest concern after deciding to be a Safe and Secure Online volunteer was how best to deliver content to 10- to 12-year-olds.

"The public speaking in this volunteer work didn't make me uneasy," he said. "On the other hand, I learned a lot from the audience. From their reactions and responses, I came to better understand the way teenagers—the future masters of our society—truly think about cybersecurity and better understand online behavior and the influencing power of peers. This really opened my eyes."

He continued: "It is my honor to participate in the Safe and Secure Online program as a volunteer speaker. I wish more and more members would contribute their valuable knowledge and time to this extremely meaningful project in the near future. Not only can you educate our community, you also can raise your professional profile."

He credits local (ISC)² representatives Kitty Chung and Nico Chan with making presentations go more smoothly.

"Without their background support, I couldn't complete my volunteer work in such an easy way."

Are you ready to devote some time to helping keep our children safe in the online world? Then visit us at <https://www.isc2cares.org/> to learn how you can bring or enhance the Safe and Secure Online program in your area. ●



Carol Lo



Henry Lai



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



2020 Vision

A ROUNDUP OF MEMBERS'
AND INDUSTRY EXPERTS'
PREDICTIONS

EDITED BY ANNE SAITA



THE FUTURE OF MOBILE SECURITY

We asked (ISC)² members to predict the biggest threats to mobile users by the year 2020



“AS MOBILE devices continue to proliferate, they will be increasingly used for managing day-to-day activities (heating the house, starting the car, monitoring health care). That is a huge risk. Mobile devices can be so easily lost. There will continue to be issues downloading apps—there will be new technologies to hack.”

—Karen Kabel, CISSP, CISA, CISM,
President, (ISC)² Manitoba/Saskatchewan Chapter, Winnipeg, Canada

“CHILD EXPLOITATION via mobile and wearable devices—I see this continuing to be a problem until parents realize how serious it is to give young children uncontrolled mobile devices. We need to educate parents about the dangers online and allowing our children to be ‘connected’ without understanding enough of the technologies to keep our children ‘protected.’ Criminals are quick to adopt and utilize technology, which allows them to jump between borders, disrupting local

law enforcement efforts. I see wearable mobile technology as the next way for criminals to exploit honest people, but when used for good it is possible we might be able to turn the tide on cyber threat actors.”

—Paul Cardelli, CISSP, CEH, CHFI, CCNA Security, JNCIA-Junos, Washington, U.S.A.

“WHEN IT comes to threats in the mobile space, I think we will continue to face a world that is far more focused on ‘time-to-market’ for delivering and receiving new devices and applications, rather than ensuring good security controls and best practices are in place. We will continue to see rapid proliferation of devices and applications which are adopted by an uneducated public by growth-driven markets faster than they can be evaluated from a risk/threat perspective by trained professionals. Until we can institutionalize information security awareness, these threats will continue to rise at an exponential rate.

“Perhaps the next big threat in mobile is one where we become so reliant on these devices to survive, that a global outage results in massive economic impact.”

—Forrest Foster, CISSP, President, (ISC)² Austin Chapter, Texas, U.S.A.

“THE BIGGEST threat with mobile has almost arrived by now, I think.

“It stems from the uniqueness of using smart phones for everything, for accessing banking accounts, for paying simply by passing the cashier desk, for handling our smart homes, smart cars, smart everything.

“If a malicious code is able to attack one of these applications, which is the most vulnerable among the many present in the phone, AND it is able to cross the boundaries between applications, then losing one service might endanger all the others.

“It is similar to attacking the hypervisor or other middleware in a cloud. We can log the activity in ‘our’ operating system, but will not see what is below it.”

—Kati Szenes, CISSP, President, (ISC)² Budapest Chapter, Budapest, Hungary

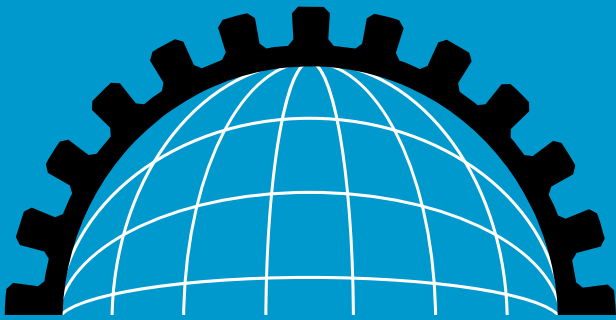
“INTERNET/CLOUD of Things, embedded and wearable technology—all offer new, efficient and effective ways to take control. As these become ubiquitous, so do the risks. Adequate attention needs to be given to privacy and security of these—policies, standards, regulatory frameworks and laws need to play catch-up, and fast too.”

—Wunmi Faiga, Lagos, Nigeria

➤ **NEXT ISSUE** What are the biggest risks with Big Data? Will future security standards for protecting data derived from the “Internet of Things” come primarily from the industry or from government legislation/regulation? Send your thoughts in a paragraph or two to asaita@isc2.org by August 15, 2014.

SECURITY CONGRESS

2 0 1 4



Sept 29 – Oct 2
Atlanta, GA

Georgia World Congress Center

Colocated with



SECURITY CONGRESS

EMEA

2 0 1 4



Dec 9 - 10
London, UK

Bloomsbury Hotel, London

In Partnership
with



STRENGTHENING CYBERSECURITY DEFENDERS

(ISC)² Security Congress 2014 offers attendees education sessions led by industry known speakers, designed to transcend all industry sectors, focus on current and emerging issues, best practices, and challenges facing cybersecurity leaders. As cyber threats and attacks continue to rise, the goal of (ISC)² Security Congress is to **strengthen cybersecurity defenders** by arming them with the knowledge, tools, and expertise to protect their organizations.

(ISC)² Member Benefits:

- Earn CPEs
- Conference Pass Discounts
- Networking Opportunities
- Meet with (ISC)² Executive Staff

Register Now

www.isc2.org/security-congress