A Look at Today's ICS Threats

COLLEGE REQUIRED
Is it time to reconsider a four-year degree for some government posts?

RMF
A member's rocky road to implementation

Stephen A. Ridley, CTO and founder of enterprise security provider Senrio
Everything You Need For Your Enterprise Cybersecurity Certification and Training

(ISC)² Enterprise Solutions

It takes a fully trained team to keep your organization secure.

Each organization has its own unique training and certification needs. We understand that there’s no cookie-cutter solution, which is why we offer tailored training solutions centered around your organization’s budget, schedule, and cybersecurity certification requirements.

Learn about our new Enterprise Solutions

(ISC)² Direct
(ISC)² Official@Work
(ISC)² Investment
features

CRITICAL INFRASTRUCTURE

20 Power On
As nations like the U.S. expand energy operations, threats to the systems controlling them create new challenges.
BY SHAWNA McALEARNEY

PROFESSIONAL DEVELOPMENT

24 Making the Grade
Hiring the best and the brightest to defend national cybersecurity requires box-bending thinking.
BY ANDY COHEN and MARVIN MARIN, CISSP-ISSMP

GOVERNANCE, REGULATION AND COMPLIANCE

27 A New Frame of Mind
An (ISC)² member shares lessons learned from establishing RMF at his organization.
BY JASON MCDOWELL, CISSP

departments

4 EDITOR’S NOTE
Reducing Downtime During a Disaster
BY ANNE SAITA

6 EXECUTIVE LETTER
More Ways for EMEA Members to Learn—In Person and Online
BY ADRIAN DAVIS

8 FIELD NOTES
New EMEA member benefits; new board members; North America region’s new managing director; GDPR myths debunked; workforce stats around the world.

17 NEXT CHAPTER
Chapter of the Year

18 MEMBERS’ CORNER
The Importance of CISSP Vetting
BY NORMAN MUELLEMAN, CISSP

31 CENTER POINTS
More Than $1.1 Million Awarded in Scholarships
BY PAT CRAVEN

32 5 MINUTES WITH...
Ronald Ricohermoso, SSCP
A security analyst in the Philippines discusses what a workforce shortage means there.

Cover photograph: BRIAN SMALE. Image (above): DANIEL HERTZBERG
Reducing Downtime During a Disaster

As the year comes to a close, communities worldwide continue to clean up from natural disasters that are inevitable given population growth in high-risk regions and violent weather. From hurricanes and typhoons to heat waves and wildfires, not to mention blizzards, earthquakes, tornadoes and landslides, each event is a harsh reminder to always prepare for the worst.

We tend to focus on the basics following a catastrophic event—food, shelter and clothing. Within IT there is the urgency to generate power, filter water, safely handle waste and keep transit options and communications channels open. Such network reliability and application assurance is further challenged by the fact bad actors like to strike when a system is most vulnerable.

That’s why it’s incumbent upon every SOC within every organization to plan in advance for such an emergency. This means developing strong change management practices, regularly reviewing written processes and performing drills so everyone is ready when disaster strikes. Remember: the simpler the instructions, the more likely people will remember to follow them.

The advice holds true for manmade incidents too. This issue’s cover story takes a look at the impact the rise of nation-state malware is having on critical infrastructure. A member also shares lessons learned from implementing RMF at his organization. Additionally, two experts weigh in on required four-year degrees for many U.S. government cybersecurity jobs.

As always, I’d love to hear what you think of the issue’s content and what you’d like to see featured in the coming year. As for 2018, let’s hope it’s a safe one for all of us. ■

Anne Saita, editor-in-chief, lives and works in Southern California. She can be reached at asaita@isc2.org.

InfoSecurity Professional  ●  4  ●  November/December 2017

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

(ISC)² Enterprise Solutions  ................................................2
(ISC)² Cyber Risk ..............................................................5
Infosecurity Middle East ....................................................7
(ISC)² Vulnerability Central  ..............................................14
(ISC)² APAC .................................................................19
Twirling Tiger Media .........................................................33

© Rob Andrew Photography

(ISC)² MANAGEMENT TEAM
DIRECTOR, CUSTOMER EXPERIENCE
Jessica Hardy
727-493-3566  |  jhardy@isc2.org
EXECUTIVE PUBLISHER
Timothy Garon
508-529-6103  |  tgaron@isc2.org
SENIOR MANAGER, CORPORATE COMMUNICATIONS
Jarred LeFebvre
727-316-8129  |  jlefebvre@isc2.org
MANAGER, CORPORATE COMMUNICATIONS
Amanda D’Alessandro
727-877-2230  |  adalessandro@isc2.org
COMMUNICATIONS SPECIALIST
Kaity Eagle
727-683-0146  |  keagle@isc2.org
MEDIA SERVICES MANAGER
Michelle Schweitz
727-201-5770  |  mschweitz@isc2.org
EVENT PLANNER
Tammy Muhtadi
727-493-3441  |  tmuhtadi@isc2.org

SALES TEAM
EVENTS SALES MANAGER
Jennifer Hunt
781-685-4667  |  jhunt@isc2.org
REGIONAL SALES MANAGERS
Lisa O’Connell
781-460-2105  |  loconnell@isc2.org
Mike Magno
781-569-6630  |  mmagno@isc2.org

EDITORIAL ADVISORY BOARD
Carlos Cañoto, South America
Kaity Eagle, (ISC)²
Tushar Gokhale, U.S.A.
Jarred LeFebvre, (ISC)²
Javvad Malik, EMEA

TWIRLING TIGER MEDIA
EDITORIAL TEAM
EDITOR-IN-CHIEF
Anne Saita
asaita@isc2.org
ART DIRECTOR & PRODUCTION
Maureen Joyce
mjoyce@isc2.org
MANAGING EDITOR
Deborah Johnson
EDITOR
Paul South
PROOFREADER
Ken Krause

© Rob Andrew Photography

InfoSecurity Professional  ●  4  ●  November/December 2017

© Rob Andrew Photography

(ISC)² is certified as a women’s business enterprise by the Women’s Business Enterprise National Council (WBENC). This partnership reflects (ISC)²’s commitment to supplier diversity.
In today’s connected world, cyber risk is no longer just a technical concern

What Every Business Leader Should Know About Cyber Risk

This whitepaper is the perfect tool to inspire the board and initiate the change today. Release the potential in your organisation with this action plan developed by (ISC)².

We have defined five fundamental focus areas to help cybersecurity professionals open the dialogue with executives and encourage them to take back control of cyber risk:

» Accept cyber risk is a business risk
» Align cyber spend to your risk
» Create a culture that prevents vulnerability
» Get control of data
» Ensure security and privacy are ‘baked in’ to processes

Get your free copy today 🔄
executive letter

BY ADRIAN DAVIS

More Ways for EMEA Members to Learn—In Person and Online

NEVER UNDERESTIMATE the amount of talent within the (ISC)² Europe, Middle East and Africa (EMEA) region. This year we launched the EMEA Information Security Leadership Awards and received a fantastic response; in fact, in our first year we had as many nominations as the Americas ISLA® program, which is more established.

We’ll be announcing the winners during an awards ceremony during the two-day Secure Summit UK that kicks off Dec. 12 in London. (Around the same time next year, we’ll be welcoming the return of the (ISC)² EMEA Security Congress!)

Events like these are one way to connect members from a large and varied region. But we know not everyone can join us in person. That’s why we are expanding our multimedia education opportunities with more EMEA member-focused podcasts and with webinars on our BrightTalk channel. We also are expanding our presence on YouTube with how-to videos, so our cybersecurity professionals gain the most value from their membership.

Speaking of value, we have now launched a Member Perks and Wellness program for EMEA members (see “New Money-saving and Wellness Benefits for (ISC)² EMEA Members,” p. 8). So often we are focused on mastering technologies to halt threats and secure our networks that we forget the toll such dedication can take on other aspects of our lives. That’s why this free two-part program includes a focus on financial and personal well-being. Discounts will be available to U.K. members first, looking to achieve regional coverage in 2018. The personal well-being service is now available to all EMEA members immediately. To access this benefit, members can find exclusive sign-up details on the member area of the website, and access their profile through the LifeWorks app or online.

We want to help our members master more than just information security domains. The perks program provides mechanisms to support members both professionally and personally and provides access to such support. You are not in this alone.

...We are expanding our multimedia education opportunities with more EMEA member-focused podcasts and with webinars on our BrightTalk channel.

If you are a woman working in information security in our region, however, you may indeed feel alone. One of the most disappointing findings in this year’s EMEA regional report from our 2017 Global Information Security Workforce Study was that only 9 percent of our workforce are women. That low percentage was constant across each continent in our region.

Quite frankly, I was shocked at such low participation, particularly since the survey also showed a growing workforce shortage and lack of talent to fill it.

The second surprise for me was almost one-quarter (24 percent) of survey respondents lack an IT or IT-related degree. To me that’s a good sign that we are recruiting from a more diverse talent pool.

If you recruit only those similar to you, you will all approach problems similarly too. As we know, our adversaries do not problem-solve in the same way. They are more agile. We need to be too. So, let’s continue to look outside traditional fields for new talent. And let us know how we can best continue to serve you helping to protect organizations throughout the EMEA region.

Adrian Davis is the director of the EMEA Regional Office. He can be reached at adavis@isc2.org.
THE GULF’S SPECIALIST EVENT FOR SECURING VITAL GOVERNMENT AND BUSINESS DATA AGAINST EVER-GROWING CYBER THREATS.

Discover the latest products and technical solutions, learn best practice through interactive sessions by industry innovators and develop business opportunities to protect critical infrastructure in a borderless cyber-enabled world.

POWERING INNOVATIONS, EMPOWERING COLLABORATIONS FOR A SAFER CONNECTED WORLD
New Money-saving and Wellness Benefits for (ISC)² EMEA Members

(ISC)² EMEA recently launched its LifeWorks program, offering both perks and wellness support to members in the region. You can download the LifeWorks app or access online.

LifeWorks provides free, confidential telephone- and web-based information and support services designed to give members information and support across a range of issues covering their life, health, family, money, and work. LifeWorks is available 24 hours a day as part of your membership. The program includes:

- Counseling, coaching, digital content, and care services
- 24/7 telephone service and toll-free phone number in the U.K.
- Personalized wellbeing content with relevant tips and advice based on your interests
- Access online and through the app

EMEA members can access these programs through the member benefits page on the website. Get more from your membership by logging in today!

In addition, U.K. members can currently access Member Perks to save money through exclusive discounts on a wide variety of products and services. (A similar program was announced earlier for North American members.) Benefits include discounts on:

- Cinema tickets
- Gym memberships
- Travel
- Restaurants
- In-store shopping
- Online fitness and yoga classes

In addition, members can:

- Earn cash back online
- Purchase gift cards
- Access all existing (ISC)² member discounts through the platform

We are looking to extend perks to the rest of EMEA. If you know of a similar program that you would like us to consider please contact member-supportemea@isc2.org.

Four New Directors Elected to the Board

Four security experts will join the (ISC)² governing body to help drive strategic direction of the organization. The new members of the (ISC)² Board of Directors begin their service on January 1, 2018.

- Biljana Cerin
  CISSP, Croatia

- Tony Cole
  CISSP, SSCP, U.S.A.

- Earl Crane
  CISSP, U.S.A.

- Tiffany Jones
  CISSP, U.S.A.

“I am extremely grateful to the outgoing members of our Board of Directors for their volunteer service to (ISC)²,” said David Shearer, CEO. “They are leaders in the industry, as are these new members; and we appreciate having their expertise to help guide the organization. I know they will be fantastic additions to the board.”

The four newly elected professionals will join the ranks of other top cyber, information, software and infrastructure security professionals from around the world representing academia, private organizations, and government agencies. All board members volunteer to provide strategic direction for the organization and are (ISC)²-certified. The 13-member board provides strategy, governance, and oversight, grants certifications to qualifying candidates and enforces adherence to the (ISC)² Code of Ethics.
Brian Correia Named Managing Director for North America Region

BRIAN CORREIA, recently the director of business development for the (ISC)² North America region, is now the region’s managing director. He will oversee North American business operations, including sales and member recruitment, business development, government relations and strategic partnerships.

Prior to joining (ISC)², Correia served as the director of business development and venue planning at SANS Institute. In his 16 years at SANS he was involved in sales, partner relationships, event management, contracts and marketing campaigns. His previous experience includes the trade show industry and as a member of the Starwood Advisory Meetings Board (which consisted of Sheraton, Westin, W Hotels, St. Regis, Four Points and Luxury Collection), where he helped implement new products, marketing and consulting to one of the leading hospitality companies in the industry.

“Cybersecurity professionals are tasked with the pressing challenge of protecting our nation and our economy against a constantly evolving threat landscape with a limited workforce and skill set,” he said. “Few organizations in the world do as much to empower and advance the cybersecurity profession as (ISC)². It’s a privilege to join the organization and lead such an outstanding team of dedicated individuals.”

(ISC)² CEO David Shearer praised Correia’s work with the organization. “Since joining (ISC)², Brian has played an integral role in identifying strategic business opportunities to advance the North America region and its commitment to strengthening and diversifying the information security workforce. He is an exemplary leader furthering our mission.”

Correia has a bachelor’s degree in business administration from James Madison University. (ISC)²’s North America Region Office is located in Alexandria, Va.

GDPR MYTHS DEBUNKED

The European Union’s General Data Protection Regulation (GDPR) will go into effect on May 25, 2018. There are many misconceptions and misunderstandings about the GDPR; here are some of them:

1. GDPR is like Y2K. Some firms are tackling GDPR with the same hysteria prevalent during the Y2K millennium bug, approaching GDPR as a single project with a defined end date. But GDPR is not just a “point in time” activity. Compliance with GDPR should be the default position for legitimate firms.

2. No one will get fined. Targeted enforcement is likely and authorities may go after high-profile companies or companies with particularly egregious data processing faults.

3. Everyone will get fined 4 percent. Fines are set at either 2 percent or 4 percent depending on the type of infraction as well as the company’s history with the GDPR and other factors.

4. All security breaches must be reported within 72 hours. Only personal data breaches will have to be reported and reporting obligations will vary with a firm’s role in handling data. Companies that process personal data will have to notify their controllers of personal data breaches without delay.

5. It will be safest not to report security breaches. Some firms may think that if they conceal security breaches from authorities, they will not get fined. This is untrue; they could be found out anyway and could be fined for failing to report data breaches.

Mark Your 2018 Calendars for These Events

Miss one of our (ISC)² member conferences this year? Plan now to attend one next year. You can find a list of 2018 events, from one-day Secure events to multi-day Security Congresses throughout the world. Go to https://www.isc2.org/News-and-Events/Event-Calendar.
A link to the content is not available.
field notes

**SENIOR INFORMATION SECURITY PROFESSIONAL**

**Jorge Mario Ochoa**

*Project/Initiative – Information Security Culture*

With more than 17 years of experience in information technology, Jorge Ochoa has experience implementing, auditing and certifying ISO 27001:2013 and ISO 22301:2012, information security strategy, information security frameworks, vulnerability assessment, application and network penetration testing (OSSTMM and OWASP), information security awareness programs, consultancy, and as a leader of several regional and global projects.

**Mansur Hasib**

*Project/Initiative – Cybersecurity Technology Degree Program*

2017 Cybersecurity People’s Choice Award winner Dr. Mansur Hasib has 30 years’ experience in leading organizational transformations through digital leadership and cybersecurity strategy in healthcare, biotechnology, education and energy. He currently teaches the art of cybersecurity leadership and is Program Chair of the Cybersecurity Technology program in the Graduate School at University of Maryland University College.

**Bart Lauwers**

As Membership Chair for the Austin Chapter, Bart Lauwers was lauded for creating chapter growth, redeveloping the chapter’s website, encouraging volunteerism within his chapter and promoting this (ISC)²’s Security Congress.

**JULIE FRANZ PEELER “DO IT FOR THE CHILDREN” VOLUNTEER AWARD**

Named for the late Julie Franz Peeler, the first director of the (ISC)² Foundation that is now the Center for Cyber Safety and Education, this award honors her devotion to teaching children how to be safe online. “Her real passion was to build an educational program that would teach parents, seniors and especially children how to be safe and secure when online,” director of the Center for Cyber Safety and Education Patrick Craven recalled. “If you ever had a conversation with Julie about our educational programs she always went right for your heart by reminding you ‘It’s for the children.’”

**James McQuiggan**

2017 Winner

By making inroads in his company, along with his daughters’ schools, his church, and senior citizen groups in his community of Winter Park, Florida, James McQuiggan has helped more than 7,000 children, parents, senior citizens and teachers learn to protect themselves online. 

**PRESIDENT’S AWARDS**

**Glenn Leifheit**

Glenn Leifheit was recognized for his commitment and dedication to (ISC)² and the community at large including his volunteer service on the (ISC)² North America Advisory Council, the (ISC)² Application Security Council and the (ISC)² Chapter Governance Committee.
Announcing the 2017 Scholarship Recipients

**The Center for Cyber Safety and Education** is proud and honored to announce the 2017 (ISC)² and Raytheon scholarship recipients. This year 48 information security students will share some $175,000 in awards. Students come from 17 different countries.

These 2017 scholarship recipients demonstrate a passion, dedication, drive and determination to stand out amongst many deserving applicants. While we wish all applicants could be awarded, we would like to take this opportunity to shine a light on some of the best and brightest.

### (ISC)² Women’s Information Security Scholarship Recipients

<table>
<thead>
<tr>
<th>Name</th>
<th>Country</th>
<th>Institution</th>
<th>Degree(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saleema Adebisi Adejumo</td>
<td>Nigeria</td>
<td>University of Leicester – M.S.</td>
<td>Security and Risk Management</td>
</tr>
<tr>
<td>Jan Shuyler Buitron</td>
<td>U.S.A.</td>
<td>Colorado Technical University – Ph.D.</td>
<td>Computer Science, Information Assurance</td>
</tr>
<tr>
<td>Valerie Chen</td>
<td>U.S.A.</td>
<td>Yale University – B.S.</td>
<td>Computer Science</td>
</tr>
<tr>
<td>Mudita Khurana</td>
<td>India</td>
<td>Carnegie Mellon University – Information Security</td>
<td></td>
</tr>
<tr>
<td>Avanthika Ramesh</td>
<td>U.S.A.</td>
<td>University of California Berkeley – B.S., Electrical Engineering &amp; Computer Science</td>
<td></td>
</tr>
<tr>
<td>Valerie Chen</td>
<td>U.S.A.</td>
<td>Yale University – B.S.</td>
<td>Cybersecurity, Computer Science</td>
</tr>
<tr>
<td>Serita Denise Sargent</td>
<td>U.S.A.</td>
<td>NYU Tandon School of Engineering – B.S., Cybersecurity, Computer Science</td>
<td></td>
</tr>
<tr>
<td>Susan Wanjiru</td>
<td>Kenya</td>
<td>University of Maryland University College – M.S., Cybersecurity Technology</td>
<td></td>
</tr>
</tbody>
</table>

### (ISC)² Undergraduate Information Security Scholarship Recipients

<table>
<thead>
<tr>
<th>Name</th>
<th>Country</th>
<th>Institution</th>
<th>Degree(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacob Tyler Blackburn</td>
<td>U.S.A.</td>
<td>Northern Arizona University – B.S., Management Information Systems</td>
<td></td>
</tr>
<tr>
<td>Amber Borowiec</td>
<td>United Kingdom</td>
<td>University of Oxford – B.S., Mathematics-Computer Science</td>
<td></td>
</tr>
<tr>
<td>Brendan Michael Brown</td>
<td>U.S.A.</td>
<td>Champlain College – B.S., Computer &amp; Digital Forensics</td>
<td></td>
</tr>
<tr>
<td>Olivia Kate Bryant</td>
<td>United Kingdom</td>
<td>Harvard University – B.S., Computer Science</td>
<td></td>
</tr>
</tbody>
</table>

48 students from 17 countries sharing $175,000 in awards
Rebecca Kim
George – South Korea – Indiana University of Pennsylvania – B.S., Computer Science/Information Assurance

Hannah Laila Hellerstein – U.S.A. – Reed College – B.S., Computer Science

Stephanie Bree Jensen – Australia – Central Queensland University – B.S., Network Security

Erwin Karincic – Germany – Virginia Commonwealth University – B.S., Computer Engineering

Nicole Oakley Krantz – U.S.A. – George Mason University – B.S., Cybersecurity Engineering


Bryn Christine Loftness – U.S.A. – Colorado Mesa University – B.S., Computer Science

Catherine Anne McLean – U.S.A. – Northeastern University – B.S., Computer Science/Cyber Operations Concentration

Fonyuy Rose – Cameroon – Century College – A.S. Network Security

L’oreal Smith – U.S.A. – University of Central Florida – B.S., Computer Science

Elijah Michael Staple – U.S.A. – University of Colorado Boulder – B.S., Computer Science

Taylor Marie Whiting – U.S.A. – Embry-Riddle Aeronautical University – Global Conflict/Cybersecurity

(ISC)² Graduate Information Security Scholarship Recipients

Oluwatosin Tope Bello – Nigeria – Johnson & Wales University – M.S., Information Security/Assurance

Alan Michael Brockway – U.S.A. – University of North Carolina at Charlotte – M.S., Computer Science/Information Security and Privacy

Candice Carter – U.S.A. – Kansas State University – M.S., Cybersecurity UAS

Keith Allan Duemling – U.S.A. – Penn State University – M.S., Cybersecurity & Information Assurance

Susheela Erugu – India – University of North America – M.S., Information Systems Security

Will Fair – U.S.A. – Marymount University – Ph.D., Cybersecurity

Jessica Gottsleben – U.S.A. – Salve Regina University – Administration of Justice and Homeland Security, Concentration in Cybersecurity/Intelligence

Moses Ike – Nigeria – Georgia Institute of Technology – Ph.D., Computer Science

Stephane Ikoue Ebanda – Cameroon – Texas State Technical College – M.S., Cybersecurity Engineering

Tameika Nicole Jacquette – Jamaica – Regis University – M.S., Information Assurance

Kelton Kostis – Canada – Bellevue University – Information Systems/Cybersecurity

Casey R. Morganelli – U.S.A. – Capella University – Ph.D., Information Security/Information Assurance

Kwadjo Anobaah Nyante – Ghana – EIT Digital Education Foundation – M.S., Cybersecurity and Privacy

Jessica Lynn Rush – U.S.A. – Capella University – M.S., Information Assurance & Security
field notes

Vita Senyuk – 
Estonia – Pennsylvania State University – 
M.S., Information Security

Andre Shori – 
Malaysia – SANS Institute – M.S., 
Information Security Management

Tiffany Marie Snyder – 
U.S.A. – University of Central Florida – M.S., Digital Forensics

Chooi Shi Teoh – 
Malaysia – Universiti Teknologi Petronas, Malaysia – Ph.D., Information Technology

Ngoc-Tien Doan – 
U.S.A. – University of Maryland, College Park – B.S., Computer Science

Katya Doersam – 
U.S.A. – Towson University – B.S., Computer Science – Security Track

Huda S. Fawzi – 
Iraq – George Washington University – Cybersecurity

Lalla Hasnaa Khalil El Ouadghiri – 
Morocco – Northern Virginia Community College – B.S., Cybersecurity

Andrea Marie Koch – 
U.S.A. – Daytona State College – IT - Cybersecurity & Digital Forensics

Paula Paysan – 
U.S.A. – The University of Texas at Austin – B.S., Computer Science

VULNERABILITY Central

Start tracking the vulnerabilities keeping you up at night.

Get Started

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

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

vulnerability.isc2.org

No new account is required to use Vulnerability Central and it’s free to members; just log in with your (ISC)² member account.
RECOMMENDED READING
Suggested by Larry Marks, CISSP, CISA, CISM, CFE, PMP, CRVPM, CRISC, CGEIT, ITIL

Cybersecurity 101: What you Absolutely Must Know (Vols. 1 & 2)
By James Scott
(self-published, 2016)

Providing to-the-point information about some of today's cybersecurity challenges is the goal of James Scott's two self-published volumes of Cybersecurity 101: What You Absolutely Must Know.

The books are geared to the business professional working in a firm where the current technology or current events raise alarms and risk. Short and direct, these two volumes are designed to give readers the basic means to identify, prevent and protect against assaults like spear phishing, zero-day exploits and “nephophobia”—fears about cloud computing.

Volume 1 focuses on defining and recognizing the threats, while Volume 2 provides tools for thwarting or preventing attacks. The topics are organized by areas of risk, with each opening with a question, such as, “How can attackers use…,” “What happens during this type of exploitation,” and “How can … be prevented.”

These books provide easy insights into the essentials of cybersecurity. Written in plain language, they cover topics of cybersecurity without taking the reader through extensive definitions, and may be just the right kind of information for a business person keen to understand what the information technology area is facing and how it affects his or her business.

The author did not receive financial compensation from this publisher, nor a free copy of this book. All opinions are his alone.

23% of surveyed educational institutions are well prepared to beat cyber risks

Source: 2017 Cyber Risks in Education, Netwrix Blog

310.4 MILLION
Wearable devices predicted to be sold worldwide in 2017

Source: Gartner, Inc., August 2017
http://www.gartner.com/newsroom/id/3790965

$5,302,890,448
U.S. and international exposed dollar loss caused by business email compromise from October 2013 to December 2016

Source: Federal Bureau of Investigation Internet Crime Complaint Center (IC3)

Earn CPEs for Reading This Issue
Please note that (ISC)² submits CPEs for (ISC)²’s InfoSecurity Professional magazine on your behalf within five business days. This will automatically assign you two Group A CPEs.

2017 GLOBAL INFORMATION SECURITY WORKFORCE STUDY

REGIONAL BREAKOUTS

Here are some highlights from the regional reports generated by study data. The full reports are available at https://iamcybersafe.org/GISWS/.

<table>
<thead>
<tr>
<th>Top Concerns</th>
<th>BY REGION</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>Data exfiltration 35%</td>
</tr>
<tr>
<td>Latin America</td>
<td>Ransomware 44%</td>
</tr>
<tr>
<td>Europe</td>
<td>Ransomware 28%</td>
</tr>
<tr>
<td>Middle East &amp; Africa</td>
<td>Hacking 47%</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>Data exfiltration 37%</td>
</tr>
</tbody>
</table>

*N=19,641*

<table>
<thead>
<tr>
<th>Top Reasons for Worker Shortage</th>
<th>BY REGION</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>Qualified personnel difficult to find 52%</td>
</tr>
<tr>
<td>Latin America</td>
<td>Business conditions can’t support additional personnel 46%</td>
</tr>
<tr>
<td>Europe</td>
<td>Qualified personnel difficult to find 48%</td>
</tr>
<tr>
<td>Middle East &amp; Africa</td>
<td>Requirements not understood by leadership 50%</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>Qualified personnel difficult to find 47%</td>
</tr>
</tbody>
</table>

*N=12,709*

<table>
<thead>
<tr>
<th>Percentage Who Came from Non-IT/Engineering Background (among those who did not start in cybersecurity)</th>
<th>BY REGION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>30%</td>
</tr>
<tr>
<td>North America</td>
<td>35%</td>
</tr>
<tr>
<td>Latin America</td>
<td>18%</td>
</tr>
<tr>
<td>Europe</td>
<td>24%</td>
</tr>
<tr>
<td>Middle East &amp; Africa</td>
<td>29%</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>22%</td>
</tr>
</tbody>
</table>

*N=16,210*

Overall, 70% of hiring managers will increase their workforce this year; 30% wish to expand by 20% or more.” —2017 Global Information Security Workforce Study
Kansas City Named (ISC)² Chapter of the Year

The Kansas City Chapter received the (ISC)² Outstanding Chapter Award (North America) at September’s Security Congress in Austin. The award is given to the North America region chapter that best promotes the (ISC)² vision and mission of inspiring a safe and secure cyber world. In presenting the award, chapter leaders were commended for demonstrating a well-rounded offering of activities and services to benefit its members and affiliates, as well as making a significant contribution to the profession and local community through the core focus areas of the (ISC)² Chapter Program of connect, educate, inspire and secure.

Finalists for Chapter of the Year:
• (ISC)² Tampa Bay
• (ISC)² Alberta

(ISC)² KANSAS CITY CHAPTER CONTACT INFORMATION
Contact: Derin Beechner
Email: membership@isc2kcchapter.org
Website: http://isc2kcchapter.org

(ISC)² Chapter Appreciation Award

From left to right: David Shearer, Dylan Cornelius (Director of Marketing), Tabitha Greiner (Director of Sponsorships and Community Outreach), Bart Lauwers (Membership Chair and Director of Technology Services), Jim Kaiser (Secretary), Bill Thompson (CPE Coordinator) and Steven Hernandez.

The Austin Chapter was given special recognition during Security Congress with the (ISC)² Chapter Appreciation Award for chapter members’ time, dedicated resources, and demonstrated loyalty and service to the organization or its local community. (ISC)² recognizes the efforts of the team of volunteers who help achieve or exemplify the corporate vision of inspiring a safe and secure cyber world.

Number of (ISC)² Chapters worldwide.
The Importance of CISSP Vetting

WEEKLY, IF NOT DAILY, news agencies report the discovery of a new cyberattack or breach. Usually these stories mention the lack of cybersecurity professionals to deal with the ongoing threats.

Studies earlier this year, including the (ISC)² Global Information Security Workforce Study, predict a global shortage of up to 2 million cybersecurity professionals by 2019. There are now more people wanting to fill that cybersecurity void. That means more information security professionals seeking to be accredited. Are we as an industry prepared for the influx of personnel? What are we doing to ensure these new personnel are trustworthy and ethically grounded?

(ISC)²’s CISSP is a fantastic certification. Those who earn that credential must not only pass a rigorous exam, they must be vetted by other CISSP credential holders. In the (ISC)² application process, new applicants must have a sponsor, namely a CISSP in good standing, to review the potential new member’s resumé and ensure all requirements are met, including five years’ experience.

How far should a sponsor go to ensure an applicant fulfills the requirements? (ISC)² recommends that work history is checked to ensure the work experience cited matches the specific domain within the CISSP realm. For example, as a former police officer, I had a lot of experience with physical security aspects from a crime prevention standpoint. I was able to leverage this experience to the physical security domain requirements of the CISSP certification requirement. I provided my sponsor with my modified resumé, showing work history and how it equated to CISSP domain requirements. My sponsor also requested contact information for each position so that he could verify my work history.

These are sound vetting practices, but I would argue more vetting is needed to ensure the integrity of hard-earned certifications. To keep our coveted certification at the top of the list, it is our duty as CISSPs to do more than just check boxes for those we sponsor.

First, take a good look at an applicant’s resumé to ensure that he or she has the required experience for at least two of the domains. Request that the applicant provide documentation to show how their work experience meets the domain requirements. Then have the applicant provide a contact you call to verify their self-submitted work history. Ideally, it’s someone in the field, not someone from human resources who is more limited in what he or she can release.

We owe it to the industry, and our certification body, to uphold the integrity of the process. That means a full vetting of our applicants. If you can’t reach a source via phone, try to get an email response. If you can’t get in touch with the provided reference, have the applicant provide an alternate. Usually a person can provide at least two or three professional references.

Take 30 minutes, verify the validity of the information, and know that you are doing your part in ensuring the integrity of our certification process.

Norm Muelleman is a senior cybersecurity professional at a St. Louis-based IT security firm. After a 20-year career in law enforcement, he eventually entered the IT field, starting with computer networking. He has a passion for auditing and compliance review and obtained his CISSP certification in 2014. He is a former president of the (ISC)² St. Louis/Scott AFB Chapter.
APAC Secure Webinars
(ISC)² Security Briefings
Watch Free Webinars Live/On-Demand
Anytime, Anywhere

프로파일링 기반의 이상 행위 분석을 통한 보안 전략
특권アカウント乗っ取り事件の事例とその真相
利用大数据实现积极且
具有高度关联性的安全防御
Adding Intelligence to Investigations
Protecting Privileged Accounts in the Cloud
DDoS Threats of Past, Present and Future

Subscribe Now!

Earn 1 CPE per Webinar*
*will automatically be added to the (ISC)² members’ profiles.

To Speak. To Sponsor. Contact mpark@isc2.org
CRITICAL INFRASTRUCTURE

FOR YEARS, information security professionals have said that it’s not a question of if, but of when we’ll see a major cyberattack from an enemy targeting a nation’s electrical systems, its airports, or even space stations. And we have seen successful attacks on both the power grid and an airport in Ukraine to serve as a warning for larger and more widespread attacks.

“The old-guard security vendors are trying to retrofit that ‘walled garden’ paradigm to this new interconnected world.”
—Stephen A. Ridley
CTO and founder, Senrio

Power On

As nations like the U.S. expand energy operations, threats to the systems controlling them create danger.

BY SHAWNA McALEARNEY

FOR YEARS, information security professionals have said that it’s not a question of if, but of when we’ll see a major cyberattack from an enemy targeting a nation’s electrical systems, its airports, or even space stations. And we have seen successful attacks on both the power grid and an airport in Ukraine to serve as a warning for larger and more widespread attacks.
Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems have long been known to be vulnerable to malware like Duqu, PlugX, Stuxnet, Flame, Havex and Black Energy. More recently, solar power grids have been shown to be at risk, reflecting a new threat dimension, given they are not aging systems like some other critical infrastructure.

While malware is still a dominant attack tool, more government-sponsored hacktivists are manipulating social media users to create chaos and sow the seeds of destruction. This makes it that much harder for cybersecurity professionals to protect their systems.

“We’re a huge, fat target that appears to be really stupid about defensive computer security,” says Marcus J. Ranum, an independent security consultant, referring to ICS security. “It’s certainly the case that governments bankrolling the development of attack tools have brought a ‘sky is the limit’ approach to the capability of malware.”

Experts have said that when enough vulnerabilities are found by an adversary to cause a major outage, we could lose power for months and have a major event rivaling the Sept. 11, 2001, U.S. terrorist attacks in New York City and Washington, D.C.

It’s certainly the case that governments bankrolling the development of attack tools have brought a ‘sky is the limit’ approach to the capability of malware.”

—MARCUS J. RANUM, independent security consultant

Recently, a new attack vector came to light. Dutch security researcher William Westerhof identified 21 vulnerabilities present in solar panels, specifically photovoltaic panels sold by SMA. These security weaknesses could enable attackers to shut down a majority of power grids in Europe.

LIFARS, a digital forensics and cybersecurity intelligence firm, says that since Westerhof reported these details to SMA, he has been working with the company, power grid regulators and government officials to address the issues. SMA also issued patches to help harden systems.

Ranum notes: “Power grids have an interesting trust problem: They have to accept inputs that are not necessarily owned by the company that is managing the grid—there’s a certain assumption that anyone who’s in the power business is going to play by certain rules, but you’re still potentially going to have control inputs taking place based on what someone else is doing.”

“The power grid collapse that resulted in blackouts back in 2003 was not a result of hostile action,” adds Ranum. “It was the grid’s response to a failure at a single station.”

In a 2013 interview with Scientific American, electrical engineer Jeff Dagle, a member of the U.S.-Canada Power System Outage Task Force and a specialist in power grid resilience at Pacific Northwest National Laboratory, talked about the massive power outage on Aug. 14, 2003, that impacted 50 million people in the U.S. and Canada.

In that case, trees and a software failure caused three power lines to fail in Ohio. Dagle says, “The grid isn’t designed for that level of redundancy” and it triggered “the largest blackout in North American history and crippled much of the northeastern U.S. for two days… with an estimated economic impact of $10 billion.”

Imagine then the ramifications of a deliberate attack on a weakened critical infrastructure.

“With a few exceptions, the general state of security across the industrial control systems networks that power critical infrastructure is poor at best,” says Galina Antova, a leading ICS expert and co-founder of Claroty. “It is difficult to pinpoint one segment or another of critical infrastructure and call it the most concerning or most vulnerable. Adversaries of different types will have different motives and target sectors accordingly.”

MOTIVATION IS EVERYTHING

While some attackers are in it for the money or the notoriety, most nation-states have much different motives, and are also far better funded than many cyber syndicates. Government-sponsored attacks are often about gathering intelligence, information to predict events or to sway public perception, according to U.S.-based business risk assessment firm Flashpoint.

The company assesses risk and notes shifts in the cyber and geopolitical threat environments, such as the continued political influence attempts emanating from Russia; “the dormancy and then re-emergence of The Shadow Brokers (TSB), most notably with their release of stolen National Security Agency (NSA) exploits utilized in major attacks; the continued drop in Chinese APT activity against the West; and how tensions in the Korean Peninsula impact both the cyber and physical security landscape.

In its Midyear 2017 Business Risk Intelligence Decision Report, Flashpoint analyzed the current nation-state threat
landscape and called out countries based on cyber activity:

**Russia:** In addition to being named in the 2015 Ukraine power grid shutdown, Russia has been linked to efforts to influence various elections in the United States and, more recently, Western Europe, including France and Germany. The manipulation stems from “compromising political opposition groups and engaging in disinformation campaigns.”

**China:** So far this year, the Chinese government has been linked to a handful of attacks against Western and Eastern Asia targets. Flashpoint cites a U.S. Department of Homeland Security report detailing recent activity that involved spear-phishing attempts “against commercial entities in the financial, retail and technology sectors.”

In another case, Flashpoint says the suspected Chinese advanced persistent threat group (APT10) was linked to a campaign targeting the U.S.-based National Foreign Trade Council at a time that coincided with a U.S.-Chinese summit in early April. It also referenced a PricewaterhouseCoopers and BAE Systems report that detailed APT10 activity against unnamed international managed service providers and a number of Japanese entities.

Then, threat intelligence provider FireEye reported that its researchers had observed Chinese threat actors attempting to compromise an organization associated with the deployment of the Terminal High Altitude Area Defense (THAAD) anti-ballistic missile system in South Korea. Therefore, Flashpoint believes “China remains a potent force both technically capable and intent on compromising foreign targets in support of its national objectives.”

**Iran:** Flashpoint’s report says Iran “is believed to have invested much in cyber weapons as a means both of countering the U.S.’s conventional military clout and of projecting power regionally…. One notable aspect of Iran’s cyber strategy is the overwhelming focus on exploiting vulnerabilities in critical infrastructure systems, largely due to such targeting’s ability to cause widespread damage and disruption, even for more classically powerful adversaries, such as the U.S.” Though Iran has been responsible for little cyber activity recently, Flashpoint warns that any major revisions to the Iranian nuclear accord with the U.S., which U.S. President Donald Trump has called a “bad deal,” could spur “renewed Iranian efforts in the cyber domain.”

**North Korea:** Widely believed to still be a potent threat in cyberspace through its proven capability “to strike foreign targets both in the United States and South Korea in particular with significant effect,” North Korea’s cyber capabilities are believed to be heavily contingent on Chinese infrastructure and, Flashpoint believes, tacit political support from Beijing. Current sanctions supported by China and increasing tensions over North Korea’s recent nuclear missile testing appear to have dampened that support, but the likelihood for North Korean-backed cyber activity remains high. In a recent interview with NBC’s “Meet the Press,” former U.S. Homeland Security Secretary John Kelly said a cyber threat from North Korea is much more likely than a kinetic threat.

Antova believes we are more likely to see attacks against critical infrastructure and critical industry used as a form of economic warfare than we are to see these attacks as an element of traditional warfare—at least in the near term.

The NotPetya ransomware campaign, which recently spilled over into production environments, gave us a warning of what is likely to come—$600 million in losses are already being reported from those non-targeted attacks.”

—GALINA ANTOVA,
ICS expert, co-founder of Claroty

“The NotPetya ransomware campaign, which recently spilled over into production environments, gave us a warning of what is likely to come—$600 million in losses are already being reported from those non-targeted attacks,” says Antova. “If an adversary were to custom-craft ransomware to attack ICS domains and target specific companies that represent major players in the U.S. and global economy, they can easily inflict massive losses in an effort to propel their own agendas.”

**The Five Eyes.** Flashpoint report author Jon Condra, director of East Asian Research and Analysis, also examined cyber threat capabilities of the U.S., U.K., Australia, New Zealand and Canada, collectively referred to as “The Five Eyes,” and determined that they “together represent the pinnacle of cyber capabilities of all actors in cyberspace.” He concluded, “Their broad reach, unparalleled levels of
technical sophistication and high levels of coordination make them formidable adversaries for those who are targeted for either the purposes of intelligence collection, disruption or destruction during wartime.”

While Flashpoint indicated that the Five Eyes do not carry out highly disruptive or destructive attacks against allied or Western systems, especially during peacetime, it should be noted that the U.S. has recently been targeted by a mysterious online group dubbed the “Shadow Brokers.” The group has repeatedly released alleged U.S. National Security Agency (NSA) hacking “data,” such as the EquationDrug files and the Lost in Translation dump that details SWIFT and Windows OS-based exploits and payloads. According to Flashpoint, the Shadow Brokers also released “evidence pointing to an ostensible NSA-backed campaign targeting financial institutions, particularly those located in the Middle East.” Also, the EternalBlue exploit, discovered by the NSA and subsequently leaked, was discovered in the global ransomware worm WannaCry.

“Then there’s really ham-fisted stuff like the U.S. government trying to pin WannaCry on North Korea, in order to get everyone to forget that the exploit WannaCry was built on was a CIA exploit that was leaked, probably, by the Russians,” says Ranum. “It’s totally North Korea’s fault that we built a weapon and someone used it, right?”

CHALLENGES REMAIN

Industrial control systems are built around a longer lifecycle than other IT systems; because they have to be continually available and are in place for years, they can be challenging to update.

“This is an opportunity for attackers,” says Mark Nunnikhoven, vice president of cloud research at Trend Micro. “The threat landscape is always changing and this creates openings for attackers to gain control or disrupt ICS. Add to that the higher value of assets connected to ICS, and you get a very attractive target environment for attackers.”

Experts agree that ICS and SCADA security lag significantly behind other IT security and have for years, but overcoming the history of less-than-stellar security doesn’t happen overnight.

“With ICS/SCADA equipment, the replacement timelines are much longer than laptops and smartphones and the security issues last much longer, which means mitigations are needed to address the concerns immediately,” says Nunnikhoven. “You’re forced to live with a ‘temporary’ fix until the root cause can be addressed in the next version or equipment can be replaced.”

“We know from experience that bolting-on security is far less effective than building it in from the start,” he continues. “It’s going to take a while to get the security standards of these devices up to current standards.”

“Traditional ICS/SCADA designs called for the isolation or air-gapping of the equipment to address most of the security concerns,” Nunnikhoven adds. “As networks expand and more modern systems require connectivity, this isolation is no longer a given. Stronger defenses need to be deployed as attackers attempt to breach these systems.”

And other traditional security measures aren’t working for these ICS systems. For example, network access control will break things and intrusion detection systems will look for signatures of shellcode or spyware that aren’t used to attack ICS, says Stephen A. Ridley, CTO and founder of enterprise security provider Senrio.

“The traditional security approaches of ‘walled gardens’ or ‘building moats and castles’ is clearly not effective—Stuxnet was public proof that air-gapping itself is invalid,” Ridley says. “Increasingly, the devices inside networks often need to communicate with devices outside networks. So the old-guard security vendors are trying to retrofit that ‘walled garden’ paradigm to this new interconnected world.”

Ridley suggests thinking of the issue as a public health analogy in which many of the world’s illnesses are preventable with basic hygiene and sanitation. Sure, vaccines and advanced healthcare are important, but what’s needed first—and what solves the majority of issues—are things as simple as potable water and hand washing.

He says security of embedded devices (IoT, ICS, SCADA, etc.) is lacking basic hygiene, both in the devices and on the networks that use them.

ICS AND SCADA MITIGATIONS

Old, out-of-date systems—many unpatched against current threats for a variety of reasons—make attractive targets. This is nothing new. But experts believe security is improving.

“We’ve seen a lot of positive movement in the ICS and SCADA space when it comes to security,” says Trend Micro’s Nunnikhoven. “In the meantime, third-party security controls are required to properly protect these systems. That takes resources. A substantial and continuing investment in products and people is needed now—that will help swing the advantage back to defenders.”

“The defender/attack dynamic is a constant cycle,” adds Nunnikhoven. “Improvements made on either side force the other to change. Fortunately, there’s enough high-profile attention on the defense of these systems that we’re seeing renewed interest and investment.”

SHAWNA McALEARNEY is a Las Vegas-based freelance writer.
Making the grade

Hiring the best and the brightest to defend national cybersecurity requires box-bending thinking.

BY ANDY COHEN AND MARVIN MARIN, CISSP-ISSMP


These three technology giants have changed our lives by understanding software development, coding and technology, and applying them in new ways. Yet if they applied for a cybersecurity position in the U.S. government, they would likely be rejected. Why? Because these three multibillionaires never graduated from college and thus lack a mandatory cybersecurity requirement: a four-year college degree.
It’s time we ask ourselves: Is a four-year college degree a good indicator of the ability to perform well in a cybersecurity role? And, does the federal government have the right expectations, hiring and development programs in place to get the right people into the right jobs?

The answer to these two questions is maybe, and this ambiguity addresses the root of a growing problem that weakens cyber defense. The four-year degree requirement for many cybersecurity jobs, along with the demanding nature of the job and the need for savvy technicians, illustrates a key gap: engaging the right talent at the right time and continually investing in that talent.

It's understandable that the U.S. Office of Personnel Management (OPM) mandated college degrees for a number of government positions because a degree assures an employer that the candidate has some baseline knowledge or skills in the subject area. But there are concerns and limitations with requiring a college degree. One such consequence is producing an overabundance of cyber graduates who are strong at policy and theory, but lack the applicable technical skills that are most in demand now.

Challenging the assumption of a mandatory four-year college degree leads to a number of applicable solutions for enhancing the quality of the cyber graduate in order to create a greater number of “cyber ninjas.” Alan Paller of SANS defines a cyber ninja as “the person who can do the threat-hunting that eludes the AI [artificial intelligence] tools. She/he is the person who fights back against cyber weapons with rapid adjustments to defenses.”

Let’s explore what those needs are.

THE NEED FOR SPEED – AND EXPERIENCE

Cybersecurity is an expanding field and in constant flux, requiring creative on-demand solutions. Unlike many other jobs where new employees can mature into their positions over time, a cybersecurity analyst is often required to provide value immediately in real-world situations that require decisions affecting millions of dollars and possibly the safety of U.S. citizens. We need more cyber ninjas who can quickly assess a threat and take action to resolve it.

For example, during the WannaCry ransomware attack of the National Healthcare System in the United Kingdom, “response time” to restore critical services was of the highest priority. Some patients were not able to get treatment fast enough. Other patients couldn’t be discharged or referred to other doctors. Many patients were diverted to different hospitals as emergency rooms weren’t able to accommodate new patients. In other words, a lifesaving system was shut down.

Cyber ninjas engaged in solving this attack or others like it need to be able to assess the risks, understand the attack in context, recommend actions to respond to the attack and carry out those recommendations. This means the analysts need training, experience under pressure, good communication skills and knowledge of policy, tools and methods. It's exceptionally rare to find someone with a number of certifications or a recent graduate who has that combination of skills. Those are developed over time, responding to real-world attacks.

Currently, many college degrees in information security prepare people to develop frameworks and policy, rather than provide the ability and experience to do technical cybersecurity work as practitioners. Recent college graduates may have only weeks of coursework in cyber and even less in practical skills. Cybersecurity is heavily dependent on vocational-type skills and a traditional undergraduate degree program does not adequately prepare graduates for an entry-level position. Conversely, many people who initially obtain cybersecurity certifications may not have deep networking or technical experience. Their knowledge may be limited to one issue, one challenge or to passing the examination. They may be unable to operate in a more complex, interconnected systems environment.

Cyber and information security demand a non-traditional approach to assessing, vetting and training the cyber workforce. We know that the military, government agencies and civilian contractors struggle to find enough people to fill their cybersecurity roles. Yet we evaluate talent in terms of “degrees and certifications.” This is limiting our thinking and may exclude very capable candidates. It is also short-sighted, because the best teacher in a cybersecurity setting is real-world experience that is currently not captured in all cyber certifications of today.

RETHINKING CYBER TALENT DEVELOPMENT

If the notion of a mandatory degree or certification isn’t a good, or even a complete, requirement for a cybersecurity role, what is the solution for getting new cybersecurity practitioners up to speed faster and more effectively? Here are four options to consider:

1. **Cyber range:** The demand for real-world experience for cybersecurity analysts suggests that a simulated “live-fire” cyber range would help improve skills, improve readiness and provide more balance to the training and development of the cyber workforce. Evaluating candidates in a simulated live-fire environment and putting them under pressure in the same way that a Marine recruit is tested during the Crucible. This follows a Marine Corps maxim: Train as you fight.

   For example, if we wanted to test a candidate’s skill at managing a firewall, we may put them in a virtualized...
Due to the difficulty in recruiting cyber talent, companies have begun internal training programs to move motivated IT employees into security roles.

space where they are given direction to make some modifications to the firewall correctly and to avoid negatively impacting operations or security posture. This type of real-world assessment could help a hiring manager determine if a candidate has the appropriate knowledge, skills and ability to do the job.

2. Segment talent: Certification provides evidence of knowledge in a particular area or specialty, similar to the degree a doctor receives. But it doesn’t, and can’t, indicate how that doctor will be with patients, respond during an emergency or stay on top of the latest technologies. The technical certification, too, cannot predict the other criteria that are equally important in ensuring the right person for a cybersecurity job. Are they a team player? What are their problem-solving skills? Do they possess some of the soft skills required to work well with others?

Hiring managers and organizations should consider ranking skills to a benchmark similar to the Skills Framework for the Information Age (SFIA). This type of ranking would better determine skills related to an entry-level journeyman to a lead practitioner; it would help to understand the “box” that a person should be in and avoid putting people into the wrong position.

Additionally, third-party trusted vendors or organizations can vouch that a candidate is certified at a certain level so that hiring managers can use that as a shortcut. For example, in order to be a Full Member of the Institute of Information Security Professionals (U.K.), an interview and assessment against the SFIA in 35 competencies by industry peers is required.

3. Parallel learning: Cybersecurity is a 24/7 job. But as one chief security officer pointed out, his people work 9 a.m. to 6 p.m. and not on weekends, due to budget constraints. This means that people have time to do other things, such as taking online classes that round out their education. If a college degree is that important, then perhaps the criteria should be reversed: that practitioners get their intensive, real-life training in the first two years through programs in a vocational or community college environment, then are allowed to supplement that education as working professionals over the next four years.

4. Inner drive: When reviewing candidates, it’s sometimes easy to discard some because of several biases: they don’t come from the right school, have the right degree or a combination of factors important to the hiring manager. But that approach could eliminate some very promising candidates. Take, for example, a candidate being inter-viewed for a position as a cyber analyst, which requires a strong understanding of data relationships, manipulation and processing. The candidate under consideration had a BFA (sculpture) from the College of William & Mary, and the interviewer was curious as to how the candidate went from fine arts to a complex field within cyber. “I want to eat” was the humorous response, but it also demonstrated this candidate’s commitment and motivation to the job.

Due to the difficulty in recruiting cyber talent, companies have begun internal training programs to move motivated IT employees into security roles. Additionally, workers outside of STEM roles are being considered if they possess the inclination and drive. In this way, organizations can look to career changers to develop an internal cadre of non-traditional cyber personnel.

HIRING IN THE NEAR FUTURE

As U.S. government agencies face a staffing shortage for cybersecurity analysts, we must provide the best means to hire, prepare and train the individuals who will protect the nation’s systems and data. This means we must challenge traditional criteria to identify good candidates and hire effectively. Most importantly we need to create programs that fully vet and prepare cybersecurity professionals for the conditions they will face on the job.

Unless the government rethinks the way it hires future cyber analysts and defenders of the nation, we will never “graduate” to securing the next generation of cyber ninjas to help build a stronger level of defense. We must consider new methods of identifying, validating and training the future cybersecurity workforce.

ANDY COHEN is a cybersecurity thought leader, TEDx and Google Talks speaker and published author. His new book, Challenge Your Assumptions, Change Your World, will be reviewed in the upcoming Army Cyber Defense Review in which Cohen is also a contributing columnist.

MARVIN MARIN, CISSP-ISSMP, is a technical program manager for NetCentrics and was recognized as a 2016 finalist for EC-Council Foundation’s Chief Information Security Officer of the Year. He currently supports the U.S. Coast Guard Cyber Command.
Sometimes the hardest part of adopting a new framework is getting started. There is just so much information to digest and then just so many hours to take those guidelines and incorporate them into an organization’s infrastructure, policies and culture. Such is the case with my efforts to introduce the Risk Management Framework (RMF) at my organization.

It wasn’t easy. And it won’t be for any other (ISC)^2 members trying to become RMF compliant. But perhaps by me sharing my journey (to date), the process can be less stressful and more successful for others—whether it’s this framework or another better suited for your organization.

First, though, let’s start with why RMF, and why now.
THE NEW STANDARD FOR SYSTEMS DEVELOPMENT

The Risk Management Framework (RMF), a collaborative project managed by the National Institutes of Standards and Technology (NIST), is becoming the de facto standard for all Department of Defense (DoD) and DoD supporting systems. The predecessor to RMF, the Defense Information Assurance Certification and Accreditation Process (DIACAP), remains only as a grandfathered process for those systems that are still working toward RMF authorization.

RMF was designed to promote consistency and standardization among all federal agencies, as well as bring federal agencies more in line with the private sector’s approach to risk management. The RMF authorization six-step process is quite an involved undertaking and is very documentation-heavy; getting an early start on the process is sound advice.

The framework was created with the intent of applying it at the earliest phases of system development; however, many systems under the RMF requirement have been deployed and are operational in the field. This was the case in my current company and most likely with the majority of DoD systems in the wild.

Although the migration from DIACAP to RMF presents some major challenges, it also offers some benefits. These benefits become apparent as one works through the authorization process. DIACAP has been criticized for being rigid and focused on a “check box” mentality, whereas RMF offers more flexibility through baseline overlays and tailoring of controls. There is also significant opportunity to offer justification as to why one option or control was chosen over another.

Additionally, RMF relies on risk as its guiding principle, which allows those most familiar with their systems to propose risk levels they deem most appropriate given the function of the system and what type of environment in which it operates.

Notwithstanding deadlines and due dates, pursuing RMF authorization is a worthy goal for any company and security professional. Due to migration from the more militaristic nature of DIACAP, I believe most security professionals today will quickly appreciate the flexibility that RMF offers.

Additionally, those from the private sector will find that their current skill sets are well suited to assist federal agencies in the RMF authorization process. Through my own journey through the RMF process, I have learned a few lessons I’d like to share with you before you embark on your own RMF efforts.

TRAINING

There are quite a few boot camps and training camps available for RMF. A quick search on the web will yield a substantial number of available courses. Most of these courses are marketed as a complete solution, providing all that is needed to fully complete an RMF authorization. To be fair, there is much value in a boot camp’s ability to review the fundamentals at a very fast pace, but the reality is that RMF expertise comes from pairing experience with previously gained knowledge.

A notable challenge to gaining a full understanding of what is required for an RMF authorization is sifting through vast amounts of available documentation and online resources. To help save time, I’ve recommended those core publications that worked best for me (see “Must Reads” on p. 29).

Most training resources for RMF will give you the basics, which are undoubtedly important. However, to truly understand RMF, one must dive deeper. You also must be willing to make small mistakes along the way, as I have found mistakes to be my greatest teacher during this process.

Keep an open mind regarding how things get accomplished. As you work your way through the authorization process, be willing to consider alternate routes and methods to getting your system authorized. Not only is this a great way to learn different approaches, many times it leads to discovering far more efficient methodologies.

THIS REQUIRES A TEAM EFFORT

Due to the amount of work involved in an RMF authorization, and the collaboration needed with different members of a team, it’s best to let go of any professional ego.

The RMF process incorporates many different facets of a system, all the way from initial development to continuous
monitoring of system changes during its normal lifecycle. That said, to complete an RMF authorization with maximum efficiency, you should include team members familiar with the system and others who have completed other authorizations. This allows the whole team to leverage the experience of its more seasoned members and dodge some of the inevitable obstacles that arise in any labor-intensive project like this.

From my own experience, I would recommend first looking within your own company for RMF-experienced team members. It is quite possible, depending on the size of your company, that there are other information security professionals who’ve completed an RMF authorization and would be happy to help.

Also, don’t be afraid to reach out to your Authorizing Official’s team. The AO will evaluate your efforts to achieving full RMF compliance. They may have some organization-specific guidance and templates that can save you and your team many hours of wasted effort.

**NOT ALL STEPS ARE EQUAL**

Of the six steps to achieving RMF authorization, I found the very first step of system categorization to be most critical and in need of some explanation.

System categorization sets the stage and tempo for the rest of your authorization effort. If your system is categorized incorrectly trouble will soon follow. The general flow of system categorization is to follow the guidance of FIPS 199 and to identify the information types processed by the system by referencing SP800-60, Volume 2, Revision 1. Essentially each information type maps to a specific impact level that, in turn, aligns with classic security objectives: confidentiality, integrity and availability.

Here are a couple of DoD tidbits I learned along the way:

First, if your system is considered a national security system (NSS) or is a system used by or in support of the DoD, then you will not be using the high-water mark concept as specified in FIPS 199.
Second, if you are an NSS or DoD designate, you will be using CNSSI 1253 to identify applicable controls, as opposed to using SP800-53. You will still be referencing SP800-53 for control descriptions; however, your baselines will be from CNSSI 1253.

Now, back to the potentially troublesome part: Assuming your system is legitimately low risk, if your system is incorrectly categorized as, say, a moderate or high impact level, using the high-water mark concept, you will be dealing with an exponentially higher amount of potential controls and control enhancements. A lower impact level dramatically reduces your workload, so it pays to be precise when categorizing your system. Additionally, a low-impact system incorrectly categorized as moderate or high may not even satisfy the requirements of the controls without additional (and superfluous) technical additions to the system.

Bottom line: No matter what, get your system categorized accurately. This is a make-or-break step in the RMF authorization process.

No matter where you are in your organization’s hierarchy, do your best to get to know your AO.

GET TO KNOW YOUR AO AND SUPPORT STAFF

The gatekeeper to achieving your RMF authorization is known as the Authorizing Official, or AO for short. There are many additional roles that may possibly be involved (see SP800-37r1), but the AO is your judge and jury on whether or not your system(s) is up to snuff, so to speak.

No matter where you are in your organization’s hierarchy, do your best to get to know your AO. For example, I was able to find a bio of our current AO, which gave me some insight on our AO’s technical background and past organization experience. By understanding what “style” of security professional you are dealing with, you can get some insight into what the AO may or may not accept.

Let’s say you have a control or set of controls that you believe you simply cannot meet based on the normal operational requirements of the system you are attempting to authorize. Your understanding of the AO’s motivations and program experience may help you contour your rationale or justification to be something the AO will not only understand, but also relate to on a different level. You must keep in mind that the AO likely has a large number of authorization packages to comb through monthly, so it’s up to you to make your system and documentation easy to understand, and easy to authorize. In addition to the AO, make a firm effort to get to know his or her “minions.” The AO usually has a cadre of ISSOs and security specialists working for them. Get names, call them up, send emails. These actions fall under age-old advice: get to know the executive assistant if you want an interview with the boss. AOs rely heavily on their security teams to do the legwork on most authorizations. Building strong working relationships with the AO’s support staff is beneficial.

RESEARCH AND READ

RMF authorization is, without a doubt, a daunting task. Even more so if you are not willing to research and read about how best to accomplish this major goal. As a NIST-managed program, it is essential that you take the time needed to read and understand the RMF-related publications. This advice applies to the 800 series publications, as well as applicable FIPS publications.

I have been guilty of jumping into a process without fully understanding where I’m going or what map I’m using to get there. I’ve seen many a professional take on projects with a bazooka and a pot of coffee, when all that was needed was a sling shot and cup of tea.

With RMF it is imperative that you get the fundamental reading under your belt before moving forward. Take advantage of all the free tools and documentation templates from supporting agencies. If your gut is telling you there should be an easier way, there probably is; take the time to research online so you find it.

IN THE END, IT’S WORTH IT

The Risk Management Framework is an admirable attempt to migrate away from the “check box” mentality that has long characterized government-related security and privacy mandates. We’ve graduated from a mechanical, non-intuitive process to a more refined, risk-based one that relies on the expertise of security professionals like us.

RMF and the community surrounding it are still growing and evolving, and therefore open to feedback from those working through this mammoth process. By following NIST’s guidance, and helping our AOs and managing agencies do the same, we can essentially shape the program’s future. Admittedly, the process isn’t perfect, but we cannot wait for perfection to take action.

JASON McDOWELL, CISSP, works as an information systems security manager at Vandenberg AFB in California.
More Than $1.1 Million Awarded in Scholarships

YES, YOU READ THAT headline correctly. Your Center for Cyber Safety and Education, since we began in 2011, has awarded US$1,125,000 in financial support to future information security professionals. This comes about from the generous donations made by (ISC)², Raytheon and members like you.

This is an exciting milestone for the Center as we work to alleviate the projected shortage of 1.8 million pros that this year’s Global Information Security Workforce Study identified. This year, 48 information security students will share some US$175,000 in awards to support them along their cybersecurity career path, including tuition support, certification prep courses, materials, exams and more.

One of the great things about the Center’s scholarship program is that it is truly international, with this year’s recipients coming from 17 different countries. You can see a complete list of the winners in the Field Notes section.

The first year we offered scholarships, we had 28 applicants. In 2017, we had more than 1,000! Altogether, over the past seven years, we have supported more than 400 students and veterans in their pursuit of a cybersecurity education.

None of this would happen without the 175 members and (ISC)² chapter officers who’ve served on the scholarships selection panels. In the beginning, it didn’t take much to read and judge 28 applications, but reading, reviewing and scoring materials from 1,000-plus highly talented and deserving applicants is another story. This past year, our panelists and judges volunteered an estimated 5,000 hours of their valuable time. There is no way we could do this without their support or the hard work of Carole Boniface on our staff, who coordinates the entire program.

As you can imagine, we get a lot of thank-you letters from scholarship recipients. One that I felt really summed it up best was from one of this year’s recipients, Bryn Loftness: “It means the world to me to know that there are professionals out there that make an innumerable and immeasurable effort to support, inspire, and cultivate the futures of incoming and current undergraduate students such as myself, tantamount to which this scholarship program does so generously.”

“My eternal gratitude goes to the Center for Cyber Safety and Education for freeing me of my financial shackles and making it effortless for me to pursue my passion for cybersecurity and privacy.”

—KWADJO ANOBAAH NYANTE, Ghana

Truly, (ISC)² members are inspiring the next generation of professionals through their unselfish support. So, what about the future? Oh, it gets even better. We are excited to announce that we will not only continue offering the traditional scholarships with the support of (ISC)² and its members, but Raytheon has also signed on again to provide US$8,000 toward six Women’s Scholarships. And we are collaborating with Engility to introduce a new program called the Engility Cyber Warrior Program, which will assist returning U.S. servicemen and women by providing them with the opportunity to earn their (ISC)² credentials and jumpstart their new career in information security. You can learn more about this new Engility program and see the schedule for applying for the (ISC)² and Raytheon Scholarships on our website at www.IAmCyberSafe.org/scholarships.

We are always looking for more support to maintain and even grow the program. If you can assist in some way, or your company would be interested in sponsoring a scholarship in the future, please contact me, and we can develop a program that helps everyone.

Pat Craven is the director of the Center for Cyber Safety and Education and can be reached at pcraven@isc2.org.
RONALD RICOHERMOSO

Ronald Ricohermoso, SSCP, is an information security operations analyst at Ingram Micro in the Philippines, which is experiencing the same workforce shortage as everywhere else. He’s been an (ISC)^2 member for the past four years.

You began specializing in networking. What made you decide to focus on information security?

I got interested in this field because I think there is no dull moment in information security. Every day there are new threats that change the ballgame, as they say. It is a very exciting field where you are required to learn new things and solve different issues all the time.

What made you decide to pursue the SSCP?

I first passed Security+ and was satisfied with what I learned. It gave me the essential knowledge to do my job in information security. I was also interested in getting the CISSP, but I lacked the five-year minimum experience qualification. So, I decided to take the SSCP exam.

You have a B.S. in computer science. How has it helped you in your current position as a security analyst at Ingram Micro?

My college degree provided me the basic knowledge to work as an IT professional. I think I discovered how to “learn by myself” by getting available information from as many sources as possible and using it to solve problems.

Is there a cybersecurity workforce shortage in the Philippines?

Yes, there is. I should say there is a shortage not only in our country but in the industry globally. In other countries like in the United States, there are college degrees focused on information security. Here, we don’t have such degrees. But lately I can see a change in the curriculum for a B.S. in IT and in computer science where schools are adding information security subjects. So, we’re slowly adding more professionals to fill that workforce shortage.

What impact does it have on analysts like you?

It’s hard considering all the work that needs to be done daily and the lack of people doing it. It’s easy getting data from vulnerability scanners, but you need to also ensure that vulnerabilities get remediated in time. It’s easy to get info and alerts from your SIEM or IDS, but you also need people to make sure it works properly. Your responsibility is not only to be compliant, but also to ensure you rise above standards. We need trained people to do that.

What is unique about working in information security in the Philippines?

Information security is an emerging industry in our country. This is due to the BPO (business process outsourcing) industry that encouraged companies to invest here. Before, if you wanted to get into cybersecurity, you had to work in local banks or, more generally, the financial industry. Now companies invest in our country to set up their own Global SOC or MSSPs.

What is unique here is working on a global scale. You get to learn different laws and cultures and support different time zones. Maybe I’m referring to my specific work setup, but working in infosec here will get you assigned to different time zones. Also, you experience working remotely with security solution vendors on places where you would implement that solution.

What did you want for a career when you were 10? And how did you end up where you are now?

When I was a kid I wanted to be an astronaut and liked studying science and technology in grade school. I like to break things and figure out how to put them back together. I guess I got to this field because I’ve always wanted to work with technology.

An expanded version of this interview will appear in the December issue of Insights, a companion e-newsletter for the (ISC)^2 membership.
You need to fill every stage of your buyer’s journey with engaging content that’s worth reading, but you’re short on time and in-house talent.

Get top-notch results by partnering with our team of content experts.

Using words and images unique to your brand, Twirling Tiger Media can help you create engaging and nurturing content for every stage of your buyer’s journey—on time and on budget.

Advertisements
Articles
Blog Posts
Case Studies
E-books
Magazines
Newsletters
Press Releases
Social Media
Success Stories
Web Content
White Papers and more!

Download our guide outlining steps to create content marketing that will bring in business.

info@twirlingtigermedia.com