

GET SOME SLEEP ■ 5 MINUTES WITH CARLOS CAÑOTO

InfoSecurity PROFESSIONAL

A Publication for the (ISC)²® Membership

JULY/AUGUST 2017

UNLOCKING
A COMMON
CRYPTO ISSUE

10 WAYS
TO IMPROVE
CUSTOMER SERVICE
RELATIONSHIPS

RISING TO THE TOP

CISOs explain how they reached the C-suite

Realogy SVP and CISO
Nashira Layade



After 11 consecutive years of success in the Americas and Asia-Pacific,

The Information Security Leadership Awards are coming to the EMEA!



The (ISC)² EMEA ISLA are a unique opportunity for you to nominate fellow information security and management professionals that go the extra mile to enhance security throughout the private and public sectors across Europe, the Middle East and Africa.

Why not show your appreciation for achievement that has impressed you?

Nomination Categories:

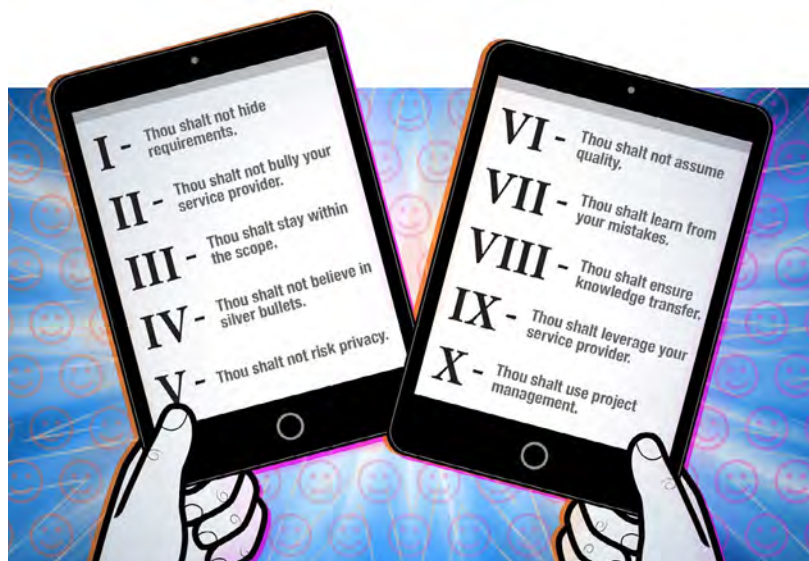
- » Senior Information Security Professional
- » Information Security Practitioner
- » Up-and-Coming Information Security Professional
- » Woman Information Security Professional

Submit Your Nomination Today: Open until 12th July, midnight
www.isc2.org/emea-isla



contents

VOLUME 10 • ISSUE 4



It isn't on there, but if there were an 11th commandment, it would be to read this article. PAGE 26

features

LEADERSHIP

16

View from the C-Suite

Four CISOs and RISOs share what it takes to reach the top level of cybersecurity—and stay there.

BY MICHELE KRIEGMAN, CISSP

ENCRYPTION

22

Key Management

Now's a good time to consider updating cryptography policies and procedures so you know who is—and isn't—keeper of the keys.

BY YVAN ROLLAND-CHATILA, CISSP

SWISS ARMY KNIFE

26

10 Commandments for a Good Security Customer Experience

Before you lash out at a service provider or hire another third party, consider these 10 tips sure to improve customer relations.

BY MARTIN PEREZ, CISSP

departments

4 EDITOR'S NOTE

Endless Summers

BY ANNE SAITA

6 EXECUTIVE LETTER

What's New for Latin America Members

BY GINA VAN DIJK

8 FIELD NOTES

USA Security Congress goes deep in the heart of Texas; new (ISC)² chapters announced; a look at women in cybersecurity from this year's Global Information Security Workforce Study and much more.

12 NEXT CHAPTER

Alberta Chapter spotlighted.

15 MEMBERS' CORNER

Post-quantum Crypto: It's Here!

BY ALEKSANDAR VALJAREVIC, CISSP

30 CENTER POINTS

Finding the Funds for Safe and Secure Online

BY PAT CRAVEN

32 5 MINUTES WITH...

Carlos Cañoto

This Venezuela native now living and working in the Netherlands is interested in securing all "things."

4 AD INDEX

Cover photograph: MATT GREENSLADE. Image (above): ENRICO VARRASSO

InfoSecurity Professional is produced by Twirling Tiger Media, 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. ©2017 (ISC)² Incorporated. All rights reserved.

editor's note

► BY ANNE SAITA

Endless Summers

What keeps you up at night?

I **LIVE IN A PART** of the United States known for its “endless summers” because there’s little variation in seasonal daytime temperatures. It means we work hard and play hard all year long. The true endless summers, though, occurred when I lived near the Arctic Circle and never saw the sun fully set for several months.

Long hours of sunlight can generate more bursts of energy, but long days on end can really mess with circadian rhythms that help dictate ample sleep. And chronic sleep deficits and insomnia don’t just impair your focus and judgment; over time they reduce your health and even lower life expectancy.

Inadequate sleep also has a huge impact on job performance. You can only manage with copious doses of caffeine for so long. (In fact, that stimulant, especially if taken beyond a certain time of day, is a likely source of fitful sleep. So are certain medications or herbal supplements, or exercise done too close to bedtime.)

In the short term, poor sleep habits affect our moods, memory and ability to learn. At work, chronic sleep loss reduces productivity and raises the risks of errors or accidents. I don’t need to remind you of what mistakes might mean if you oversee or manage a SOC or work within one.



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

Like eating and breathing, sleeping is a vital part of our well-being. Just why we need it to survive is still a medical mystery. But sleep plays a factor in our career development. Those who master sleep have more stamina and mental sharpness to troubleshoot, to lead and to innovate.

That’s why one of the “skills” upwardly mobile professionals master is sleep. They eat a healthful diet and reenergize with daily breaks (including outdoors in good weather) to stay alert. They establish a bedtime routine and wake at the same time most days. They find healthy ways to manage stress, especially if it’s caused by unresolved issues or unexpected changes.

So don’t discount the role sleep plays in your life and your career. Instead, devote the time and energy needed to give the mind a much-needed break. Both your brain and your body will thank you later. ■

advertiser index

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

| | | | |
|---|----|---------------------------|----|
| (ISC) ² EMEA..... | 2 | (ISC) ² | 25 |
| (ISC) ² Security Congress..... | 5 | Booz Allen Hamilton..... | 29 |
| (ISC) ² Ultimate Guide..... | 7 | TechTarget..... | 31 |
| Alibaba JAQ Security..... | 14 | Twirling Tiger Media..... | 33 |
| (ISC) ² Vulnerability Central..... | 21 | | |

InfoSecurity PROFESSIONAL

(ISC)²® MANAGEMENT TEAM

SENIOR MANAGER,
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

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

PROOFREADER
Ken Krause



Twirling Tiger Media 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.
www.twirlingtigermedia.com

Join us for the 7th annual

(ISC)²



SECURITY
CONGRESS

2017

Sept. 25-27 • Austin, TX • JW Marriott Austin

Keynote Panel



Moderator:



Gary Beach
Author: The U.S.
Technology
Skills Gap

Panelists:



David Shearer
CEO, (ISC)²



Brandon Dunlap
Managing Director,
Brightfly



Don Freese
Deputy Assistant
Director, F.B.I

Help Wanted! – Addressing the Cybersecurity Skills Shortage

A 1.8 million worker shortage in cybersecurity gives the old adage “Good help is hard to find” a whole new meaning. With the dearth of qualified cybersecurity professionals and our networks under attack from all angles every day, the demand and competition for talent is fierce. One hiring manager remarked “real candidates are fought over like Thunderdome.” Join (ISC)² as they discuss the state of job market, why there’s a skill shortage and how organizations can position themselves to find and attract the best candidates.

(ISC)²
Members
Save \$300

Register Today

Early Bird Pricing through **JULY 31**

Congress.isc2.org • #ISC2Congress

Earn up to
46 CPEs!

Latin America Members Have More Training, Networking Options

THIS IS AN EXCITING TIME for (ISC)² in Latin America. We recently hosted Security Congress Latin America in Brazil, expanded our regional member activities and have some very promising partnerships in the works.

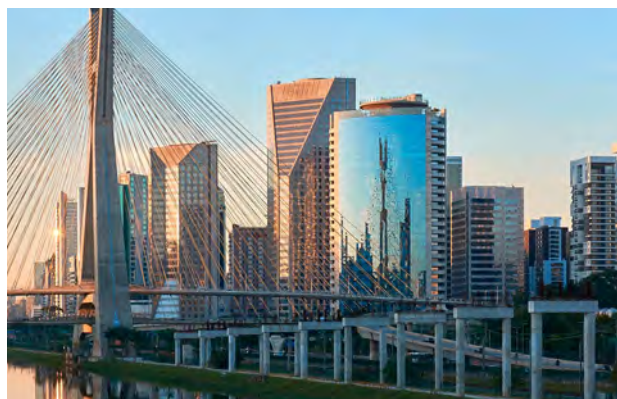
We began preparations for Security Congress more than a year ago, and this year included a job fair to help organizations and qualified information security professionals meet.

Among other developments this year that we're proud to provide are Secure events in Chile and Colombia and a presence at industry events in Argentina, Brazil and Mexico. We're also more involved in our Latin America Advisory Council (LAAC) and providing more support for (ISC)² chapters in our region. Additionally, we're excited by a budding partnership with WorldSkills Brazil, Latin America—part of the nonprofit and politically neutral

WorldSkills International, which promotes vocational education and training for member organizations and nations. Working together, we can help train both today's and tomorrow's information security workers.

These programs and partnerships are designed to help cybersecurity professionals face challenges that should ring familiar with (ISC)² members across the globe: the lack of skilled cyber professionals to fill a growing workforce shortage. In Latin America, that gap is expected to reach 185,000 unfilled job openings by 2022.

Such a shortage means employed members often work with inadequate headcounts,



which strain resources and lead to work-life imbalances that can carry a steep personal and professional toll. And, of course, it has an impact on organizations' and government agencies' ability to ward off cyberattacks and data breaches.

Simply put, the global cybersecurity workforce shortage is not sustainable. There are promising signs that the pipeline of qualified professionals is becoming robust, but much more is needed to keep it that way.

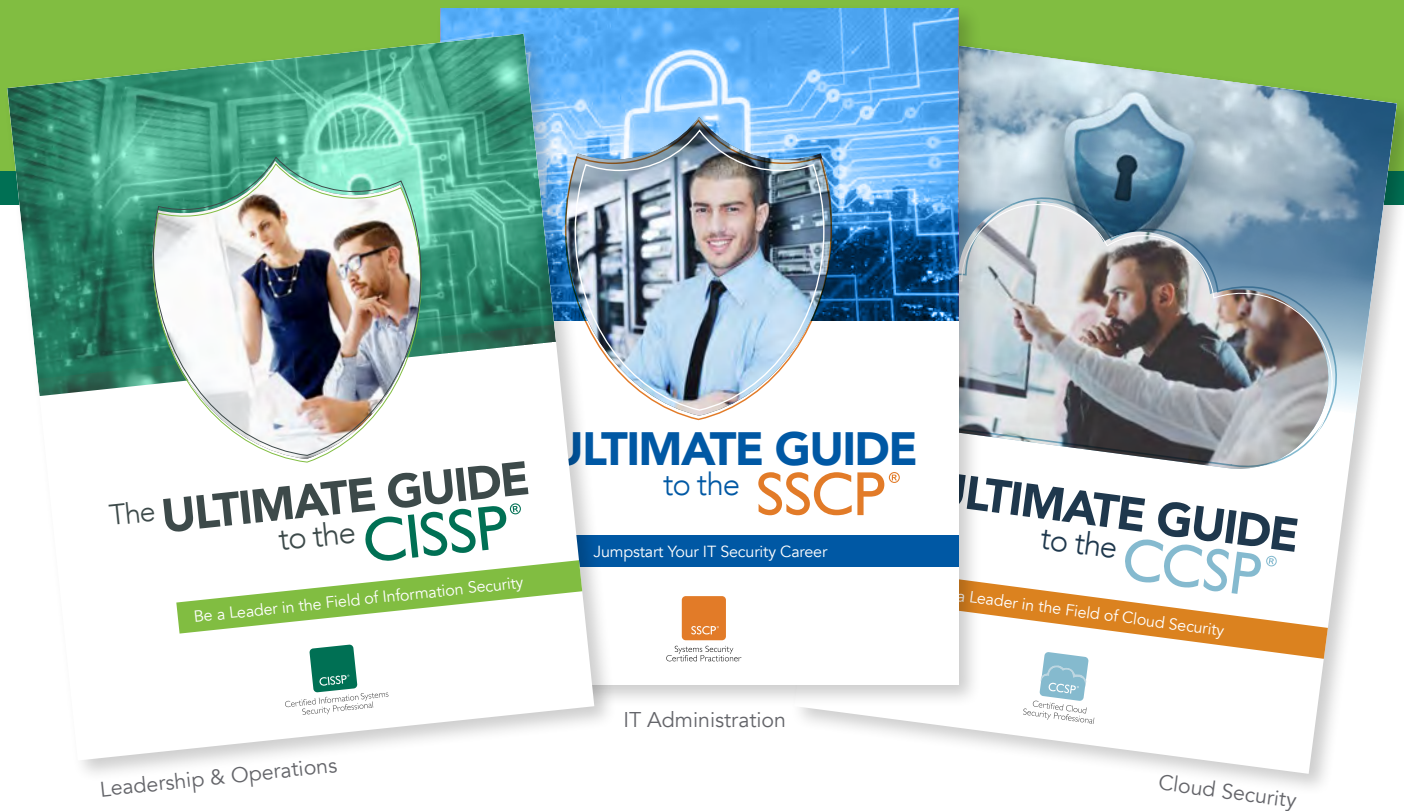
This mission to create a safer cyber world is one reason the (ISC)² Latin America office was created in September 2014. Like many working today in cybersecurity, my own career path is a bit unconventional. I was born in Nigeria, studied in the Netherlands and moved to Brazil in 2001 to realize my dream of working with Brazilian street children and others. Along the way, I was chosen to lead the (ISC)² Latin America office and now have an expanded mission: In addition to helping children in need, I hope to help the world's information security professionals gain the skills it will take to keep the world cyber safe. ■



Gina Van Dijk is the (ISC)² regional director for Latin America. She can be reached at gvandijk@isc2.org.

To gain more understanding of the Latin America cybersecurity landscape, be sure to read the [micro report on the region](#) from the 2017 Global Information Security Workforce Study.

The **ULTIMATE GUIDES** to the Ultimate Cybersecurity **CERTIFICATIONS**



Validate your expertise and show your boss you have what it takes to protect your organization with a globally recognized (ISC)² certification.

Choose which certification is right for you and download The Ultimate Guide for tips, tools, and more.

[Get Your Ultimate Guide >](#)

These guides include:

- ✓ Fast facts of the certification
- ✓ An overview of the exam
- ✓ Benefits of the certification
- ✓ Setting yourself up for success
- ✓ Steps to getting certified



field notes

A ROUNDUP OF WHAT'S HAPPENING IN (ISC)² COMMUNITIES

EDITED BY DEBORAH JOHNSON

Saddle Up and Hit the Road for Texas!

(ISC)² Security Congress 2017 promises to be a rootin' tootin' time.



The 7th annual (ISC)² Security Congress sets up shop Sept. 25-27 at the JW Marriott in Austin.

With a full complement of speakers, presentations and workshops, there will be exciting opportunities to learn, discover and share. Among the highlights:

- 100+ sessions
- Deep-dive workshops
- Birds of a Feather sessions
- Career Center for resume reviews and professional development opportunities

Note that this year's Security Congress will feature five preconference training sessions on Sept. 23 and 24 to maximize your learning and CPE opportunities.

In addition, look for special events at this year's Congress:

- Cloud Security Alliance Summit
- Executive Women's Forum workshops
- (ISC)² Town Hall meeting with the Board of Directors and management team
- Seventh annual Americas Information Security Leadership Awards (AM-ISLA®)

Congress will wrap up Wednesday night in true Texas style with an attendee party at the popular Austin venue and nightclub Speakeasy.

(ISC)² CEO David Shearer looks forward to a Congress that will leave its mark on all who attend. "We hope to provide plenty of inspiration for a safe and secure cyber world. We look forward to seeing you in Austin in September. It's going to be a great event!"

For more information and registration, go to <http://congress.isc2.org/>. ■

"We hope to provide plenty of inspiration for a safe and secure cyber world."

—DAVID SHEARER, CEO, (ISC)²

NEW (ISC)² CHARTERING CHAPTERS APPROVED

The first round of new chapter petitions has been reviewed and scored. (ISC)² is pleased to announce the approval of several new chartering chapter petitioners to proceed through the chartering process and ultimately become official chapters.

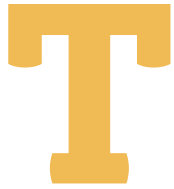
In the North America Region (NAR):

- ✓ North Central West Virginia, including Clarksburg and Fairmont
- ✓ Wichita, Kansas, including South Central region
- ✓ Pennsylvania Highlands region, including State College
- ✓ Albuquerque, New Mexico, including Los Alamos and Santa Fe
- ✓ Northern Virginia region, including Loudon and Fairfax counties
- ✓ Waterloo, Ontario, Canada, including Kitchener and Cambridge

In the Europe, Middle East and Africa region (EMEA):

- ✓ Belux, including Belgium and Luxembourg
- ✓ Saudi Arabia, central location Riyadh
- ✓ Spain, central location Barcelona
- ✓ Qatar, central location Doha
- ✓ United Arab Emirates, central location Dubai ■

GISLA® Winners Announced



THE WINNERS OF its 14th annual U.S. Government Information Security Leadership Awards (GISLA) program were announced during a springtime gala in Washington, D.C.

A judging committee of senior cybersecurity experts from (ISC)²'s U.S. Government Advisory Council reviewed all of the nominees and selected the following recipients in seven distinct categories:

Technology Improvement - Individual: Daniel Holmes, senior information technician operations engineer, U.S. Army

Process/Policy Improvement - Individual: Matt Shabat, director of performance management, Department of Homeland Security (DHS)

Workforce Improvement - Individual: Barbara Smith, information security director, Pacific District, Department of Veterans Affairs

Up-and-Coming Information Security Professional - Individual: Michael Rocha, IT specialist, DHS

Community Awareness - Team: Hemant Baidwan, branch chief, Executive Business Management, DHS

Most Valuable Industry Partner (MVIP) - Team: Parham Eftekhari and James Scott, co-founders and senior fellows, Institute for Critical Infrastructure Technology

F. Lynn McNulty Tribute Award: Brig. Gen. (ret.) Gregory Touhill, CISSP, former federal Chief Information Security Officer

For more information on the GISLA program, please visit www.isc2.org/gisla. ■

Exclusive (ISC)² Member Offer from 451 Alliance

(ISC)² is excited to offer a complimentary membership to the 451 Alliance. The 451 Global Digital Infrastructure Alliance is an exclusive, worldwide network of IT executives and experienced technology professionals coming together to give up-to-date information from an end user perspective. This member-driven think tank tracks changes in corporate IT and digital infrastructure technologies well in advance of other sources. Members gain access to research and best practices in their core areas of expertise.

Please note you must be an (ISC)² member for this offer. For more information: https://www.451alliance.com/cv/cgi-bin/memberdll.dll/open-page?wpr=MembershipApp_web_isc2.htm&sponsorcd=4010016. ■



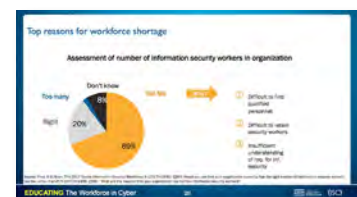
2016 - A BANNER YEAR FOR (ISC)²

(ISC)² CEO David Shearer calls 2016 "a phenomenal year," and urges members to review achievements in the 2016 (ISC)² Annual Report, available online at [https://www.isc2.org/uploadedFiles/\(ISC\)2_Public_Content/About_ISC2/Management/2016AnnualReport.pdf](https://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/About_ISC2/Management/2016AnnualReport.pdf).



In addition to the year's highlights, the report includes the organization's audited financials, which, Shearer says, is "a cornerstone of our pledge of transparency." Shearer looks forward to continued success. "I know that 2017 will be another exciting year for (ISC)², and we will accomplish great things together. Thank you for all your support and for all that you do to inspire a safe and secure cyber world." ■

U.S. GOVERNMENT RESULTS NOW AVAILABLE ONLINE



The newest Global Information Security Workforce Study micro report, on U.S. government and released at May's CyberSecureGov, is now available online at <https://iamcybersafe.org/wp-content/uploads/2017/05/2017-US-Govt-GISWS-Report.pdf>. ■

► RECOMMENDED READING

Suggested by Larry Marks, CISSP, CISA, CISM, CFE, PMP, CRVPM, CRISC, CGEIT, ITIL

How to Measure Anything in CyberSecurity Risk

By Douglas W. Hubbard and Richard Seiersen
(Wiley Publishing, 2016)

HERE IS A FRESH approach to analyzing the impact of a data breach or attack, using data analytics to measure and report how data security incidents and risks impact a business.

Douglas W. Hubbard is the inventor of applied information economics (AIE) and an internationally recognized expert in measurement and quantitative decision analysis. Richard Seiersen is former general manager of Cyber Security & Privacy at GE Healthcare. By integrating applied mathematics, data mining and measurement along with security, governance and risk, the authors aim to improve the methods for managing and insuring cybersecurity risk.

These techniques, programmed in Excel, are used to quantify, to the best degree possible, the impact of an incident such as a data security breach. Using the 2014 Target breach as an example, the authors present key questions that the analyst can ask regarding probability and frequency to quantitatively compute the potential dollar value of an incident based on the data records being exposed. The formulas, though, do not take into account the residual risks that remain after the issue is mitigated.

While I would have preferred more examples in the use of their techniques, I found the book to be a great read and informative. Caution is also warranted: Due to the significance of cybersecurity risks, a high level of care must be taken in applying their metrics and evaluation. Bravo, Hubbard and Seiersen! ■

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



Tech Industry Turnover

WHY PEOPLE LEAVE THEIR JOBS

| | |
|-----|-------------------------------------|
| 37% | Unfairness/mistreatment |
| 35% | Seeking better opportunity |
| 25% | Not satisfied with work environment |
| 22% | Not satisfied with job duties |
| 19% | Recruited away |

Source: Tech Leavers Study – Kapor Center for Social Impact & Harris Poll, April 2017
<http://www.kaporcenter.org/tech-leavers/>

PREDICTION
22.5 BILLION
IoT devices in 2021
(up from 6.6 billion in 2016)

Source: *Business Insider* prediction based on a survey of 500 global executives in a wide range of industries. *The Internet of Things 2017 Report*, January 2017

Top three cloud security concerns

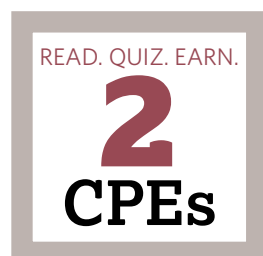
| | |
|-----|------------------------------|
| 57% | Protecting against data loss |
| 49% | Threats to data privacy |
| 47% | Breaches of confidentiality |

Source: *Cybersecurity Trends-2017 Spotlight Report*, an online survey of 1,900 cybersecurity professionals sponsored by (ISC)²

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.

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&PCAT=7777&CAT=10647



2017 GLOBAL INFORMATION SECURITY WORKFORCE STUDY

WOMEN IN CYBERSECURITY

The needle hasn't moved much for women seeking work in cybersecurity.
But more efforts could yield more diversity.

GENDER MAKEUP OF GLOBAL WORKFORCE

11%

of the global cybersecurity workforce are women



REGIONAL BREAKOUTS

| | |
|---------------|-----|
| North America | 14% |
| Asia-Pacific | 10% |
| Africa | 9% |
| Latin America | 8% |
| Europe | 7% |
| Middle East | 5% |

GENDER WAGE GAP

Women earn less than their male counterparts

| JOB LEVEL | AMOUNT/YEAR |
|----------------|-------------|
| Director | \$4,540 |
| Manager | \$4,640 |
| Non-managerial | \$5,000 |

“What is clear is that enterprise and government efforts to attract and retain more women in the global cybersecurity profession have not made a meaningful impact.”

—2017 Global Information Security Workforce Study

EDUCATION LEVEL

Entering cybersecurity workforce with a master's degree

| GENDER | PERCENT |
|--------|---------|
| Women | 51% |
| Men | 46% |



JOB SATISFACTION

Train me!

61%

of women who feel valued say their organization provides training and leadership development

Value me!

47%

of women who feel undervalued say their organization does not provide adequate training

52% of women surveyed under age 29 have computer science degrees.

#nextchapter

EDITED BY DEBORAH JOHNSON

(ISC)² ALBERTA CHAPTER

Success in Calgary: (ISC)² Alberta Chapter's Inaugural Cybersecurity Congress

NASA, Cisco, NATO and FedEx were just a few of the presenters in Calgary at the April Cybersecurity Congress hosted by the (ISC)² Alberta Chapter. The three-year-old chapter offered professionals a daylong opportunity to hear from security specialists from leading enterprises and to network with colleagues and vendors.

More than 200 security professionals from around the world attended. Among the featured top-notch industry speakers:

- Jerry Thomas, CIO of NASA Ames Research Center
- Chris Pogue, CISO of Nuix and a member of the U.S. Secret Service Electronic Crimes Task Force
- Manisha Parmar, NATO Communications and Information Agency
- Steve Biswanger, (ISC)² Alberta's membership director
- Dan Waddell, managing director, North America Region at (ISC)²

The Congress featured a series of keynote presentations and panel discussions on a variety of topics

(ISC)² ALBERTA CHAPTER CONTACT INFORMATION

Chapter President: Michael Primeau

Email: president@isc2chapter-alberta.org

Website: <http://isc2chapter-alberta.org>



(Left) **Cybersecurity Congress Calgary, April 2017.**

(Below) **Michael Primeau, President, (ISC)² Alberta Chapter.**

“I was honored to act as master of ceremonies and got a chance to meet several chapter members and other fascinating professionals who are part of the growing Calgary cybersecurity landscape.”

—DAN WADDELL, managing director, North America Region, (ISC)²

including IoT risks, cyberspace as a domain, zero-trust architecture and future cybercrime defenders.

Waddell, CISSP, CAP, PMP, says the Congress was evidence of the professional growth in Calgary. “The Alberta Chapter is a thriving chapter. ... I was honored to act as master of ceremonies and got a chance to meet several chapter members and other



fascinating professionals who are part of the growing Calgary cybersecurity landscape.”

The success of the Alberta Congress helps guarantee the chapter's activities in the region, says (ISC)² Alberta Chapter President Michael Primeau. “The profits generated from this event will go towards funding our Safe and Secure Online Program and help develop other focus areas such as our mentorship program.”

Plans are already underway for next year's Congress in Calgary. ■

Q&A ► NALO IFIELD

Getting a First-ever Congress off the Ground

For this inaugural Congress, what were the goals?

The conference was about advancing leaders in cybersecurity. As we built the vision goals, it became how do we bring in relevant and interesting messaging? A lot of feedback we had with membership [in group meetings]—the comment was always, “That was great, but can you bring us someone we don’t know already, someone that we just can’t walk down the street and have coffee with?”

Given that this was a brand new endeavor for the chapter, how did you line up the variety of speakers the membership was asking for?

I went out and leveraged contacts I had made over the last year. We were able to attract organizations such as NASA Ames Research, FedEx, NATO—really talented speakers. We wanted to make sure the messaging wasn’t something that they [the members] heard before. Research is crucial. If we got a name, we scoured YouTube for video, LinkedIn posts, blogs, anything.

It really is a balancing act. You’ve got to pay for this, so sponsorship is huge. Sponsors want to bring in their own speakers and you’re leery of that because those speakers might have a sales pitch. So you coach them about the messaging being education.

My caution is to really do the research about the people you want.

You’re already planning for next year?

We are. We already have two big speakers who said they’d like to come back, as well as several of the sponsors, and the feedback from the attendees that they saw the value in the day. Now that we have a year and the experience, we’ll be able to build an even bigger and better Congress for next year. ■



“You’ve got to pay for this, so sponsorship is huge. Sponsors want to bring in their own speakers and you’re leery of that because those speakers might have a sales pitch. So you coach them about the messaging being education.”

—NALO IFIELD, (ISC)² Alberta Chapter director at large, events chair, (ISC)² Calgary Congress Director



ELSEWHERE IN THE
CHAPTER WORLD

(ISC)² SHANGHAI CHAPTER

CHINA’S FIRST (ISC)² CHAPTER CONNECTS WITH SHANGHAI’S CYBER COMMUNITY

The (ISC)² Shanghai Chapter, founded in 2014, was the first chapter formed in China. Since its inception, the chapter has grown from 20 to 260 members. The chapter maintains a close relationship with the Shanghai Cybersecurity Association, Cloud Security Alliance, OWASP and other well-known international organizations. Last year, the chapter supported the Enterprise Information Security Summit in Shanghai and provided 80 percent of conference speakers at the event.

To encourage communication and interaction among peers, the chapter holds an interactive networking game called “Lucky Match” where veteran members are paired with newcomers so that they can meet and chat. A “salon” on hacker industry chain is a new attempt for the chapter. The Shanghai Chapter will always uphold the principle of openness, mutual trust and constantly bridging the local and regional professionals, and business community.

(ISC)² SHANGHAI CHAPTER CONTACT INFORMATION

Chapter Chairperson: Shi Yong

Email:
shiyong@sjtu.edu.cn or 5301289@qq.com

Chapter official WeChat: ISC2SH

#nextchapter

(ISC)² CENTRAL FLORIDA CHAPTER

BREAKFAST WITH A SIDE OF CYBERSECURITY

Seeking a new way to network with information security professionals, the (ISC)² Central Florida Chapter decided breakfast was the way to go. The chapter's inaugural Breakfast Brief included members and guests and featured, in addition to a continental breakfast, a presentation by Dr. Lee Mangold, a member of the chapter, CEO of GoldSky Security and a winner of the (ISC)² ISLA[®] Community Service Star award in 2013.

This first session was held in a downtown Orlando location and future Breakfast Briefs are scheduled for other locations in the city. The goal is to get information security professionals together at the start of the day



for about 90 minutes, with time to register new members, network, hear a timely presentation and, of course, have some breakfast.

(ISC)² CENTRAL FLORIDA CHAPTER CONTACT INFORMATION

Chapter Contact: James McQuiggan

Email: info@isc2chapter-centralflorida.org

Website: <http://isc2chapter-centralflorida.org>

Photograph: James McQuiggan

The Security Engine Protecting 1 Billion End-devices



Alibaba JAQ Security debuts internet information security solutions in terms of business value-centric for SMB and Enterprises as well. We offer solutions covering Mobile Security, Anti-fraud Solution, Content Security and ID Authentication. Over 1 billion mobile devices and thousand companies are secured by our security capability and protection solutions for their business.



Mobile Security

- . Vulnerability scan
- . APP Hardening
- . Security Suite
- . APP Monitoring
- . Anti-virus



Anti-fraud Solution

- . Risk Identification
- . Security Verification



Content Security

- . OCR Identification
- . iText Filter
- . iPic Filter



ID Authentication

- . ID Counterfeit
- . ID Authentication

Website: <https://intl.aliyun.com/product/mobile-security>

<http://jaq.alibaba.com/>

E-mail: mobilesecurity@service.alibaba.com

Post-quantum Crypto: Ready, Set, Go!

NIST [defines quantum computers](#) as machines that exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for conventional computers. Once available on a large scale, these could bring significant benefits, through faster processes in medical research, financial analysis and other areas.

These computers could also exploit weaknesses in public key infrastructure (PKI), symmetric algorithms and hash functions and introduce changes to algorithms and mechanisms that today represent the basis for cryptography and information security. This will in turn change the solutions we build, from data encryption to authentication and SSL.

Cryptography is dead, long live cryptography!

The world of information security and specifically cryptography will change, but it is not the end of the world when it does. Some of the algorithms we use today, such as RSA and Diffie-Hellman, will be “dead” and others will require longer keys, but this does not mean death of cryptography, it means a new life. We will use new algorithms

and adapt some existing ones to continue providing confidentiality and integrity of data.

My colleague at LAWtrust, solutions director Maeson Maherry, tells us that in this case, change is constant and inevitable and that the cryptographic solutions that are brought to market must be flexible and adaptable to ensure smooth transition. If we wait for standardization and start adapting only then, we will be too late. Maherry clarifies that he is not saying to implement new algorithms now, but rather to get ready to do it when needed.

Should we be getting ready for these changes? A 2016 research paper by Microsoft (“Hybrid quantum-classical approach to correlated materials,” Bauer et al.) says that we

could have functional large quantum computers as close as a decade from now. Institutions such as NIST, ETSI and IETF have taken note of these developments and are taking action. NIST [called for submissions](#) for quantum-resistant public-key cryptographic algorithm candidates late last year and the process of standardization will take an estimated five to 10 years.

We will use new algorithms and adapt some existing ones to continue providing confidentiality and integrity of data.

Cryptography-based solutions rely on standardization and interoperability. Therefore, the information security community must work intensively over the next decade to be ready to adopt new algorithms, mechanisms and standards, through technological and process changes in both new and existing products and solutions.

Jon Geater, CTO at Thales e-Security and a pioneer of practical PKI systems, warns that the process of introducing post-quantum crypto might not be without difficulties. He cautions that in using new or less-examined algorithms—quantum resistant ones included—there is a risk that defects will be found as they gain popularity and that in the meantime, we must start using quantum-resistant algorithms and diversifying in general.


Jumping in wholesale and too early could make the real security position even worse, so to counteract this problem, he advises the deployment of relatively untested quantum resistant algorithms be introduced carefully while continuing to use the best mechanisms currently known, possibly in parallel.

Get ready for the change, plan for it, prepare and act. The new world of cryptography is coming. Post-quantum crypto is knocking on your door. ■



Dr. Aleksandar Valjarevic, CISSP, PMP, is a professional services consultant at LAWtrust in South Africa. He specializes in information security and management, especially authentication, encryption, digital signatures and PKI.

VIEW FROM THE C-SUITE



Realogy SVP and CISO
Nashira Layade

Advice from CISOs and RISOs who've risen to the top on how to join them—and stay there.

BY MICHELE KRIEGMAN, CISSP

PHOTOGRAPH BY MATT GREENSLADE

ONE RUNS MARATHONS. Another writes young adult sci-fi. Still another embraces efforts to end homelessness, and a fourth splices in college teaching while managing an eight-country digital asset portfolio. All arrived at the C-suite by divergent paths. Yet in frank conversations about the future of the job and trends for the information security field, some common themes emerged.

THE CHANGED ROLE OF THE CISO

The CISO's role has been transformed by the changing nature of cyber espionage in industry and the military and the headline-grabbing advanced persistent threats (APTs) by foreign nation states. Janet Levesque, chief information security officer at RSA and a board member of the Internet Security Alliance (ISA), summed up the regulatory impact: "In the past five years the regulatory environment has been catching up to be more pervasive."

A second impact to the role is the acceleration of attacks: "There have been so many incidents in the past five years we have a little 'breach fatigue' ... so it's much more top of

mind for people around the world. A CISO has to keep the organizational focus on protect/detect/defend goals and give solutions that deliver to these goals, despite 'breach fatigue' or statements like 'it's not if, but when [you're breached].'"



"In the past five years the regulatory environment has been catching up to be more pervasive."

—JANET LEVESQUE, chief information security officer, RSA, and a board member of the Internet Security Alliance (ISA)

The third shift globally is the elevation of the office of CISO. In 2016, the holding company Realogy, known for its real estate brands Sotheby's International and Coldwell Banker, elevated the CISO role from vice president to senior vice president with the departure of the previous CISO.

"A part of it was in order to recruit the talent they wanted," says new Realogy SVP and CISO Nashira Layade, and "to ensure that information security is elevated across the organization."

RSA's Levesque summed up the transformation with, "These aren't just IT issues; we're seeing *executive* issues. The CISO historically reported to a CIO or CTO, but across industries we need to bring it up a level so we have a seat at the table with other C-level executives."

THE ROOM WHERE IT HAPPENS: BOARDROOM, EXECUTIVE SUITE OR SOC

Over the years, the broad issue that faces CISOs continues to be: How to get the board to listen. Sometimes it's a conversation about metrics, which ones should be reported and to what detail. But before a CISO or RISO (regional

information security officer who typically oversees the information security of several country offices for a global corporation) can get to this quantitative approach, there has to be a qualitative shift.

Michal Niezurawski, who has held multiple RISO roles



"[The] IT security [executive] often comes in with similar goals [as the legal executive] to the board, but can easily fall into the trap of sounding too technical: protect databases, networks, etc."

—MICHAL NIEZURAWSKI, RISO in Europe, the Middle East and Africa for healthcare and life insurance companies

in Europe, the Middle East and Africa for healthcare and life insurance companies, observes that a board typically "wants to reduce IT operating costs, especially [those] seen as repeatable tasks. These IT operational costs are viewed as undesirable. This approach also includes IT security. However, at the highest organizational levels, IT security costs could and should be viewed as a constant investment in the brand."

"From my perspective, it's easier for legal to start a conversation about what they need to protect or invest," he continued. "The board has better understanding of such costs, especially if they are justified by legal action or PR procedures. [The] IT security [executive] often comes in with similar goals [as the legal executive] to the board, but can easily fall into the trap of sounding too technical: protect databases, networks, etc. These terms can, in some cases,



"CISOs need to get over the fact that boards are 'digital immigrants.' You need to learn their language."

—LARRY CLINTON, *president and CEO, ISA*

be taken as intimidating by board members. Links to the business value are not immediately obvious. It is hard to justify why long-term funding is required in such situations."

What is the magic dashboard that will give a meaningful report to the board?

A who's who of CISOs tackled this very issue in a handbook titled *Cyber-Risk Oversight* produced as part of the Director's Handbook series of the National Association of Corporate Directors (NACD) that covers the nuts and bolts of metrics and communication. (See sidebar on p. 19 for a list of board-level cybersecurity metrics.)

It was edited by the president and CEO of the ISA, Larry Clinton, who has addressed the issue at industry events and in U.S. Senate testimony. He summarized the challenge this way: "CISOs need to get over the fact that boards are 'digital immigrants.' You need to learn their language. When you learn their language, integrate and contextualize your discipline into their frame of reference, you'll be much more able to work with them and influence—they talk about mergers and acquisitions, product innovation and strategic partnerships. We need to integrate cybersecurity at the front end of the business process and not at the back end of the IT process. I see a dialogue that starts with, 'Oh, you're doing an acquisition? Here are the questions you need ask.'"

Niezurawski concurred, "Translating IT risks into monetary terms that are used in the board room is difficult. I face this weekly."

Clinton also noted, "Everyone knows about the Target attack. Few people remember that around the same time eBay was attacked because eBay managed their public relations at that time that mitigated the reputation risk."

"As a CISO, to paraphrase the screenwriters of *Forrest Gump*, every day is a box of chocolates," says Levesque. For her, the room where it happens isn't just the boardroom or the security operations center (SOC), but also an executive

team room. "One of the things we've built here is a management incident response triage team at RSA. The collaboration and solving as a team is one of the most worthwhile aspects. Having this incident triage team corrals all the right people in a room—legal, operations, monitoring, IT—and together breaking down a problem."

WHAT THEY LOSE SLEEP OVER

Whether you are already a CISO, report to one or aspire to be one, it makes sense to be aware of what keeps CISOs up at night. *InfoSecurity Professional* magazine turned to Marcelo Olguin, who has served as RISO for MetLife since 2004 with Chile, Mexico, Brazil, Argentina, Colombia, Ecuador, Panama and the Caribbean in his portfolio.

"It's a nightmare the rate that the threats change," he says. "Two areas: [one,] the increasing sophistication of attacks. They're really smart guys, and can even repurpose the same attacks in new ways. One example happened at multiple companies, including



"It's a nightmare the rate that the threats change."

—MARCELO OLGUIN, *RISO, MetLife in Chile, Mexico, Brazil, Argentina, Colombia, Ecuador, Panama and the Caribbean*

Amazon, where the bad guys took advantage of new legit tools for cyberattacks via IoT. We need good quality people and good intel. We aren't a cyber intel business ourselves, so we need good partners with that focus."

The other area he identifies is third-party risk management, particularly the cloud, where data is "not completely under our control in terms of human weaknesses."

RSA's Levesque breaks it down into two more components. Like Olguin, she includes the IoT and due diligence around third-party outsourcing, but also warns that "ransomware is an issue especially for healthcare, but each industry has challenges."

The other component is "phishing and spear phishing [which is an email phish that targets specific executives], and the human component of how you train people to

9 Questions to Gauge Your Board-level Cybersecurity Metrics

These questions are excerpted from the 42-page *Cyber-Risk Oversight* handbook, part of the Director's Handbook Series from the National Association of Corporate Directors, in conjunction with the Internet Security Alliance (ISA).

They provide a starting point for the metrics a CISO might be expected to deliver to the board. The metrics were prepared by Larry Clinton, president and CEO of the ISA, a multi-sector international trade association focused on cybersecurity. In 2015, the National Association of Corporate Directors named Clinton to its "Corporate 100" list of the most influential people in the field of corporate governance. He serves on the CyberSecurity Advisory Panel of the Center for Audit Quality and is the past chair and a current executive committee member of the IT Sector Coordinating Council.

1. What is our cyber-risk appetite?

This fundamental question is one that the chief information security officer (CISO) should tackle with the chief risk officer (CRO) function. This type of collaboration can produce qualitative and quantitative data points for presentation to the board that provide context around cyber-risk appetite.

2. What metrics do we have that indicate risk to the company?

One organization has implemented a cybersecurity risk "index," which incorporates several individual metrics covering enterprise, supply chain and consumer-facing risk.

3. How much of our IT budget is being spent on cybersecurity-related activities? How does this compare to our competitors/peers, and/or to other outside benchmarks?

These metrics will support conversations about how management determines "how much spending is enough," and whether increasing investments will drive down the organization's residual risk. Additional follow-up questions include:

- What initiatives were not funded in this year's budget? Why?
- What trade-offs were made?
- Do we have the right resources, including staff and systems, and are they being deployed effectively?

4. How do we measure the effectiveness of our organization's cybersecurity program and how it compares to those of other companies?

Board-level metrics should highlight changes, trends and patterns over time, show relative performance and indicate impact. External penetration-test companies and third-party experts may be able to provide an apples-to-apples comparison within industry sectors.

5. How many data incidents (e.g., exposed sensitive data) has the organization experienced in the last reporting period?

This metric will inform conversations about trends, patterns and root causes.

6. Value chain relationships typically pose increased risk for companies given the degree of system interconnectivity and data-sharing that is now part of everyday business operations. How do we assess the cyber-risk position of our suppliers, vendors, JV partners and customers? How do we conduct ongoing monitoring of their risk posture? How many external vendors connect to our network or receive sensitive data from us?

This is a borderline operational metric, but it can help support discussions with management about residual risk from third parties. There are service providers within the cybersecurity marketplace that provide passive and continuous monitoring of companies' cybersecurity postures. A growing number of firms use these services to assess their high-risk third-party relationships as well as their own state of cybersecurity.

7. What operational metrics are routinely tracked and monitored by our security team?

While operational metrics are the domain of the IT/security team, it would be beneficial for directors to understand the breadth and depth of the company's cybersecurity monitoring activities for the purposes of situational awareness.

8. What metrics do we use to evaluate cybersecurity awareness across the organization?

Data about policy compliance, the implementation and completion of training programs and the like will help to inform conversations about insider risks at various seniority levels and in various regions and divisions.

9. How do we track the individuals or groups that are exempt from major security policies, activity monitoring, etc.?

These measures will indicate areas where the company is exposed to additional risk, opening the way for discussions about risk/return trade-offs in this area. ■

remain security aware while they are multitasking.”

Niezurawski homed in on an immediate threat that CISOs and other senior officers have in common: “Spear-phishing attempts are instances where boards need to listen in order to break the psychological or human element in the kill chain. [Directors] and line employees still fall for the oldest tricks.”

He added that sometimes what keeps him up at night, the diversity of threat vectors, is exactly what makes the CISO role the most interesting to him in information security. He cited a penetration test where one “white hat” hacker with physical access attained global administrator level of a major multinational firm in 48 hours.

PARTNERSHIPS, PARTNERSHIPS, PARTNERSHIPS

Each CISO interviewed spoke about the need to partner with groups within IT, and ones like IT audit or legal outside of it.

Niezurawski recommended, “There’s a similarity to dancing, when sometimes you’re just taking two steps to the side to find a way forward. We should no longer be the ones who only speak purely about risk in terms of IT. We need to take a lead in this dance, constantly negotiate and seek out opportunities for risk mitigation if there’s a valid business need. From a purely managerial perspective, it is possible to say ‘no,’ but if that’s too consistent a voice, it gets ignored.”

RSA’s Levesque gives a similar example. “In my organization I own compliance but not legal ... [and] we’ve come up with a nice cadence [that has delivered] a runbook of provisions for compliance and information security in a legal contract.”

Building that cadence, or mutual history, can be crucial, she continues. “I would say the same for physical security. Whether a joint investigation of addressing piggybacking [when unauthorized people enter a facility by ‘piggybacking’ or passing through a turnstile or door with the aid of a well-meaning colleague who holds a door open or swipes them in] or video surveillance monitoring, collaboration is critical. Relationship building is key to achieving what’s really a shared goal across the organization.”

Pressed for her partnership recipe, Realogy’s Layade also emphasized relationship-building, and gave these additional examples of key partners, “I’ve always had a 50-50 split between privacy and IT security. The two organizations are intrinsically linked. At another organization, physical security and information security worked closely in support of disaster recovery and the business continuity plan. The CISO and systems groups should meet often, not infrequently.”

SYSTEMS GROUPS AND ‘SHADOW IT’

To bring a specialized understanding of a group’s business process to its technology support or to speed implementation, the business may establish systems teams within their own organization. The more common examples include financial systems groups, HR IT or legal IT and collectively they are sometimes called “shadow IT.”

Here, by and large, the consensus among CISOs interviewed for this article was that partnership is still often the answer. “I’ll go back to that partnership conversation and add to that a knowledge of where hand-offs need to occur,” recommends RSA’s Levesque. “When a shadow IT group wants to introduce a new purpose-built tool or technology or change providers, they should be bringing IT security in to evaluate the security risks. The CISO’s office should be building those relationships so security is brought in early and often.”

Niezurawski referred to his metaphor of organizational collaboration as a dance. “This goes back to taking two steps to the side to find that common way forward. In my opinion, CISOs should be open for any collaboration, for understanding security.”

When pressed, he cited specific concerns a CISO should have. “Policy shouldn’t be played by CISOs to become corporate policeman. Firstly, it doesn’t need to if we have the discussion as early as possible to find what meets security needs. Second, what’s really challenging for me are legacy systems—to meet the original purpose, but allow for us to mitigate the risks and update for changed processes. Third, it also invites another threat, luring, especially for shadow IT. On a technology level, we have new types of ‘things’ that are connectivity-active, hard to patch, hard to see inside with no robust supporting community. It’s a contrast to Linux or Windows, with many people who are knowledgeable. These devices don’t have [the equivalent] vendor mitigation. But from the other side, offer a lot of new functionalities that are requested to be immediately available by our business partners.”

THE PATH TO BECOMING A TOP-LEVEL INFORMATION SECURITY OFFICER

Levesque joked that “the CISO role isn’t one someone chases” but did describe some standard “archetypes” for the careers that lead to it. “One is former military with a technical cryptography background. Then there is the technical expert who has worked in networking, patch and change management and needs to work at not getting caught in the weeds. The third path comes from the risk management, audit and compliance side. The whole space is evolving to a risk-based domain in terms of how you identify your high-value assets, then, once identified, protect

the prioritized assets.”

Niezurawski came up through that third path. “IT audit is a very important partner of IT security. I came from audit; it’s not common, but I know several others who’ve followed this route. It’s valuable to have an IT auditor who knows the technology and compliance assessment side.”

STAYING SHARP, GETTING REFUELED

Layade offered both introverted and extroverted advice. On the one hand, this SVP advises, “start to read business trade magazines like *Harvard Business Review*, *The Economist*, *Wall Street Journal* and *The New York Times*. On any given day, they don’t address cybersecurity specifically, but a CISO will come to understand its impact by reading the things they do address.”

On the other hand, she also recommends that CISOs and would-be information security officers seek out “marketing groups that put together CISO forums. We’re all facing similar challenges, so we might hear a different view that’s useful at these. ... As a female CISO, the Executive

Women’s Forum has been empowering: to spend two or three days with women ... if your industry has forums for CISO.... We understand [though] our companies may be competitors, we all face the same issues and threats. It’s good to face them together.”

Olguin echoed the recommendation for reading the *HBR* and emphasized “good studies of successful launches and alignments” because they add to what you get from more strategic technology updates. It’s understanding microeconomics—how the company works unlocks it for IT security.”

Levesque pointed out another avenue. “I rely on people in my network, through conferences and expert blogs. It’s having practitioner-to-practitioner organizations.”

Those of us who are active in (ISC)² chapters might well agree. ■

MICHELE KRIEGMAN, CISSP, ITIL, CISM, is the principal of MK Info Security Consulting and works in English and Japanese.

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.



(ISC)² | 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.



Key Management

WHY IS THIS ASPECT OF CRYPTOGRAPHY SO OFTEN NEGLECTED?

BY YVAN ROLLAND-CHATILA, CISSP

WHEN WE THINK ABOUT CRYPTOGRAPHY, what usually comes to mind are complex sequences, obscure schemes and sometimes movies. After all, isn't cryptography the art of rendering data unreadable?

All too often, cryptography is seen as a discipline only available to the tech-savvy. While this is certainly true when one needs to devise a new implementation of cryptography algorithms, hardware security modules or new security designs, there is a specific discipline of cryptography that should not be left to specialists, and this is *the management of keys*. By this I am referring to the following rules: who keeps keys, who should be accountable for them, when do they expire, which keys should be used—and how to create or terminate them.

In 2012's *Everyday Cryptography*, Keith Martin argues, "If key management is not performed correctly, then there is no point in using cryptography at all." Why should these principles be the exclusive prerogative of geeks, infrastructure gurus and genius mathematicians, rather than the owners of the keys themselves?



As an example, let's look at a bank, with various vaults and safes spread across the premises to protect customers and bank assets. Like cryptography keys, they provide confidentiality and integrity on their content. Access to the safes and vaults involves a specific set of procedures and checks (e.g., having the key and/or the combination, plus some biometric controls) to provide access.

Where would the keys or combinations be stored? Who could have access to them? When do they need to change? Who establishes these procedures?

Do we think this should be the vault manufacturer or the building owner? No. Most likely the bank manager will know or, by delegation, its security service. There will be a clear responsibility pattern.

Why, then, should it be different when it comes to data and cryptography? Why is the management of keys so often neglected?

Little consideration is given to the governance of the keys or long-term maintenance.

DOING VALUE CHECKS ON KEYS

Here is a scary story. A client once asked me to look at renewing a very old master key that protected an entire old production system. This key needed to evolve to newer standards and needed to be changed. It was known on the systems by its "key check value." We needed to have access to the key itself to perform the translation of part of the data.

Our search in the various safes that held keys came back empty-handed. After much tinkering, we found an old document that described the initial setup configuration for the production system. This document sat unprotected at the bottom of a well-forgotten shared folder. Reading through the document, I came across this very odd phrase: "Let's imagine that the master key value is XXXX. Then from it we could derive (...)" and on it went. My first instinct was that this was another setup document, with test value in it, which is usually quite common. But then, on second thought.... I frantically scrambled to calculate the check value of this "imaginary" key XXXX and—lo and behold!—it matched the production system key check value.

The only "protection" for this key was obscurity through

a misleading phraseology. Surely, this is not enough. And, of course, there was no ownership, procedures, rules, etc., governing this key that was so central.

'CRYPTO CREEP'

There are many similar stories out there, where companies see encryption as a necessary evil, and will do what is needed to "make it work" without any consideration for the security of their keys.

Then over time, there is a clutter effect: keys pile up everywhere, they are added with the only objective of making the immediate project work. Little consideration is given to the governance of the keys or long-term maintenance. Let's call this the "crypto creep," as a reference to the "privilege creep" in access control.

What happens when the key needs to change?

There might be a security policy, or a standard in the industry or the organization asking for a periodic rotation, or the underlying algorithm is found to be broken. Or the key itself has been breached by some clever engineering (technical or social). Then starts the archeological work of trying to find out the key role, and who knows about it in the organization. In certain cases, it is a daunting and time-consuming task, especially the larger (and the older) the organization may be.

Modern key-management devices now take into account these considerations and facilitate logging and traceability. But sometimes they do not cover all of the keys set up in a defined organization, especially on some exotic projects or very old ones.

What about keys held by external parties and their ownership? When your vendor holds some of your customer data or processes transactions on your behalf, who owns the keys? Who decides if, and when, to change or upgrade them?

RISKS OF NOT MANAGING

Then there are the risks. Why trouble oneself if keys are all over the place? After all, everything is encrypted, right? Well, it is not so simple. There are a few risks to consider:

Operational: This occurs when a key is not used for its intended purpose. Let's look at an internal key encrypting a database. If the same key is used over the internet to transport data, then the chances of compromise are much higher. Also, the key setup was probably designed for a limited database access.

Also, when multiple versions are present, it is possible that the wrong version is targeted by a process, giving misleading results.

In addition, what happens when you decide to upgrade your keys (i.e. change the encryption algorithm or key size)? At the start of a new project, a new system is added that does not support your legacy keys, or an algorithm is broken and you decide to upgrade. Do you know how to change and upgrade all of your keys?

Compliance: In large or regulated industries (like the banking, payment or financial sector), security rules and standards (PCI-DSS is one) demand that keys are retired (archived, deactivated or deleted) at the end of their life cycle. The risk then is a breach of compliance that will be found during an audit, with an associated short time to remediate, or even potentially more dire consequences relating to the standard being breached (e.g., loss of accreditation). This will lead to additional costs and overhead that could be avoided.

Fraud risk: If a key is found to be compromised (let's say you find the clear value on some dark web page...) then how quickly and safely can it be rotated? On all instances, on all end-points, where was it set up? If the data leakage is in the press, then the C-level executives' patience for your careful investigation and processing might be quite thin.

Also, what would keep an attacker, with some inside knowledge, from using your own keys against you? Let's say you have a very old key on a legacy system, and it has been dormant for quite a while. An attacker that has inside access can potentially hijack this key to encrypt and exfiltrate some of your data. Chances are, your probes and firewall will most likely not detect this activity, as this encryption process is occurring on one of your internal systems and that old system is not monitored. There might be some variations to this, but I have seen a case where some encrypted traffic left an organization without its knowledge.

IT'S ALL ABOUT KEY MANAGEMENT

Depending on the size of the crypto estate and your estimated crypto creep problem, an individual or a team needs to be set up. It can be managers, not necessarily IT support experts, with organizational knowledge, some good and basic understanding of cryptography.

The first task is to try to get a list of all the keys with the following information in a central place. That of course can be enriched with any standard mandatory information, but at a minimum you will need:

- An identifier for the key
- A check value (KCV, hash ... any method that will show you whether a key is duplicated)
- Key loading or creation date

- Key purpose
- Key owner
- Algorithm used and the key length
- The storage location, and applications accessing it

WHO EXACTLY IS A KEY OWNER?

This is the entity that will decide the fate of the key, in a normal setting or in a compromise scenario. But how, in a large organization, do we decide this?

Well, keys are always set up for a purpose—they protect data, other keys, databases, data transmission, etc. And usually the owner of this data is well identified. The data owner can determine how important that key is, which will lead to the appropriate key algorithm, length and applicable standard. The owner can also decide what his/her risk appetite is. If the key is compromised, then the data protected by it is at risk.

And there are cases where the key owner can decide, in a compromise, not to renew or change a key. For instance, a key protects a database attached to a project that will end in a few days. Upon learning of the compromise, the key owner realizes that the cost to remediate the key is important and the impact is low: most customers have already been moved to the new product. In this instance, forcing the migration of the last customers is less costly than remediating the key itself.

Of course, in his decision-making, the crypto owner is helped by the crypto manager(s) and the various impacted technical teams.

FOCUS ON POLICIES AND PROCEDURES

Each industry will have its own specifics, but there are some points of attention.

A cryptography policy should be aligned to the rest of the cyber defense policies, especially when it comes to incident and response.

But there are country and industry-specific regulations. If you are in France and are a public body, all your customer-facing applications should abide by the "Référentiel Général de Sécurité" (RGS). In the U.S., you must abide by the appropriate Federal Information Processing Standard (FIPS) if you are a federal entity. Payments and the banking industry are ruled by the PCI standards (PCI DSS, PCI PIN, PCI CP).

Most of these standards will encompass strong rules about the type of keys acceptable, as well as the life span of keys.

This last point needs careful attention. Although standards like NIST have some recommendations, it is usually up to the key owner to determine the life span (also called

“crypto period”) of the keys. Several questions might help determine the right crypto period. How exposed is the key? Is it used in an open network or on an internal closed environment? How critical is the data being protected? How difficult is the key rotation process?

DEEPER DIVE

The personal blog of Bruce Schneier, where one would find the latest on threats and cryptography developments.
www.schneier.com

If you are in or will travel through the UK, it's a good opportunity to visit the birthplace of the BOMBE and Colossus cryptography devices.
<https://www.bletchleypark.org.uk>

To find the latest recommended length for your keys, you can filter by the recommending body.
<https://www.keylength.com/>

The right crypto period is a fine balance between risk acceptance and operational key rotation cost.

What about the procedures? Usually, they are quite detailed when taking into account the manipulations on the cryptographic devices themselves (vendors usually cover that part quite well). But they should also encompass other aspects. How do you securely disseminate the keys? Are there any outages on any system required? Is any testing possible or advisable? Sign-off by the key owner is a necessity.

We have managed to discuss at length cryptography, without even mentioning elliptic curve, XORing, collisions and quantum computers. Apart from a basic understanding of the algorithms themselves, the points mentioned above can well be taken up by a seasoned project manager. ■

YVAN ROLLAND-CHATILA, CISSP, is a cryptography expert at Barclaycard in the United Kingdom. This is his first contribution to InfoSecurity Professional.

(ISC)² MEMBERS

Download Your Certificate DIGITALLY

Based on member feedback, you can now download a digital PDF certificate!

Your digital certificate is available under My Profile.

Download my certificate 



10 COMMANDMENTS FOR A GOOD SECURITY CUSTOMER EXPERIENCE

Had trouble working with a service provider?
Look inward before lashing out. BY MARTIN PEREZ, CISSP



Has your organization ever conducted a security engagement with a third party that ended badly? Were there unfinished deliverables, disruptions to business operations, numerous escalations and, ultimately, hostile relations with the service provider?

While you might lay the blame for this traumatic experience at the door of the service provider, you should consider how your own organization contributed to the pain of the

project. I expect your organization strives to deliver world-class service to your customers. But so does your service provider. How you behave as a customer has tremendous influence on the success of your project.

This article is intended to instruct organizations facing the objective to experience a successful third-party security engagement. Please consider these 10 commandments to help you achieve more productive implementations, save you some trouble and potentially prevent any damaging situations for your business.



Thou shalt not hide requirements

Imagine you are sick and you decide to see your doctor, but you don't clearly explain your symptoms—where it hurts and how much. If you mislead your doctor, you will not be prescribed with an effective treatment. By the same token, gathering your true requirements prior to engaging the service provider is paramount.

One of the first important steps to defining requirements is to involve the key stakeholders within your organization. Include the business unit owners. Get their input to understand how the solution maps to their business activities. Will the new solution pose any challenges in terms of usability; will compliance with a security initiative increase workload? You cannot implement a new security solution without their internal buy-in. You need champions.

If you are obligated to comply with any industry standards (e.g., HIPAA, PCI DSS), you should assess how the implementation of your new solution might impact compliance. Confer with your auditors (internal or external) for assistance. The requirement-gathering phase is so important that you might want professional expertise to gather the information with the proper methodology. Depending on the complexity of your project, and your budget, you may consider temporarily hiring a business analyst to help you.

If the quality of your requirements is poor, it will negatively impact the quality of the scoping phase for your service provider, which will jeopardize your likelihood of success.



Thou shalt not bully your service provider

Put yourself in your service provider's shoes. Treat them like a partner, not like the enemy. The reality is that in the technical arena, especially in our IT industry, people tend to disregard the human and emotional side and focus completely on technicalities and facts. Employing an overly aggressive communication style will not help you to get the most from your service provider.

Many studies of emotional intelligence and organizational behavior point to the fact that a motivated and happy individual can achieve the highest productivity levels. Bear in mind that your service provider's organization is comprised of humans with feelings that affect their motivation and productivity. You will get the best from them with positive reinforcement and by nurturing a mutual collaboration environment. True leaders build stronger bonds with others while understanding what

motivates them, which results in higher performance, as maintained by psychologist Dr. Daniel Goleman in his 1995 book *Emotional Intelligence*.

I am not suggesting you hug your partner. You do need to make sure the third party delivers the expected SLA and quality of work. Go ahead and hit, but be the hammer in the pillowcase—soften the blow!



Thou shalt stay within the scope

While the project is being executed, treat the statement of work (SOW) as your constant companion. The whole scope must be executed and it is your responsibility to monitor and ensure that all deliverables are finalized before a signoff is provided to the third party.

Your original requirements should be addressed by deliverables defined in the statement of work. Expect that any new requirements that arise will generate additional work and must be defined and submitted via a change request. When requesting changes, think of the impact of a new technical requirement or design change. Do you need a proof of concept (POC) of the proposed change prior to executing? Does the change undermine the security posture the original design is supposed to deliver? If the size and complexity of new requirements are extreme, they may entail a whole separate engagement. Don't try to squeeze those in the same contract.

Do not try to take advantage of the service provider to get more work done at the same price. Be careful—that approach will surely generate conflict and might affect the quality of your implementation. Respect the contract!



Thou shalt not believe in silver bullets

Security is not a one-time deal. It is a process and a long-term commitment.

Take, for example, a SIEM solution. In a BrightTALK webinar I recently attended, the presenter, Sridhar Karnam, director of product marketing at Artic Wolf Networks in Sunnyvale, Calif., compared SIEM with a bicycle. For the solution to work, multiple processes/tasks around it must be in constant motion. Like a bicycle, you have to pedal! After the SIEM server is in place, major network changes are needed to point log sources to it. Strong correlation rules must be developed and maintained to make SIEM effective. Resources must be in place to take action on the alerts. You may need to create a mini-SOC within your organization just to look after SIEM.

A box is not enough. What about people, the weak-

est security link? You must train them to increase their security awareness. Also, organizations wanting to improve security need a solid roadmap. Isolated implementations might actually weaken your security posture if they are not aligned with a master plan. Consider spending part of your budget on a security assessment. It is worth the money.

What do you say? Ready to embrace security?



Thou shalt not risk privacy

Even though the service provider should be considered a partner, you are letting a stranger into your home. Make sure you have security controls for those indi-

viduals who will have access to critical systems. Monitor access closely (frequency should be dictated by each asset's criticality) and make sure access is removed as soon as the project is complete. ISACA strongly recommends, in its *CISM Review Manual, 14th Edition*, that access is granted on a need-to-know and least-privilege basis. Access must receive the approval of the asset owner.

In terms of documentation and communications, request that any sensitive data is exchanged using a secured file transfer tool. Email creates an exposure.

The contractual documents must include a non-disclosure agreement. You have the responsibility to protect any sensitive proprietary data (e.g., patents) and your customers' information too. Do not take the discretion of your partner for granted. Do your due diligence to get formally protected.



Thou shalt not assume quality

Testing is one of the most important responsibilities you have as a customer. Your organization should create a comprehensive user acceptance test (UAT)

for each phase of the project. The UAT should be as detailed as possible. Include scenarios/test cases, who performs them and the expected outcome. Your service provider might help you build this test plan, but they definitely cannot own that responsibility.

When the solution can indirectly impact systems that are not in scope, check with your business units to ensure that performance and functionality have not suffered any degradation.

For planned changes in your environment, always ask for a detailed MOP (method of procedure) with a rollback plan. To avoid negative impact to your production environment due to defects, consider the following alternatives: conducting a pilot, a proof of concept, or deploying on a segregated test environment, whenever possible.



Thou shalt learn from your mistakes

Conduct a lessons-learned exercise at the conclusion of the project. Look at your organization and how your team

handled the implementation. Look for process gaps or overlooked responsibilities that might have affected the overall quality of the final result.

The goal is to objectively evaluate how the project was handled and identify opportunities for process improvements to make things better on your next engagement.

Although I would not suggest a tight agenda for this session, it would be very helpful to at least identify the main areas of discussion to keep your team discussion focused. Avoid a finger-pointing session. Most importantly, create a list of action items or recommendations relative to the issues. Make sure all voices are heard and that detailed minutes are kept and shared with the whole team.

Finally, it would not hurt to have a follow-up session with your business unit owners a few months after the implementation to evaluate the performance of the new solution, identify any usability or incompatibility issues or to simply assess how the new system has helped your organization to meet the initial objectives. Management might be very interested in hearing about it!



Thou shalt ensure knowledge transfer

The implementation is almost complete. Time for you to ensure the new solution is properly handed over to you as per

the deliverables defined in the SOW. First, you will need to get all the support contract details. If the solution is not managed by the service provider, they should provide the information you need to reach the vendor.

Make best use of walk-throughs or simulations provided by the service provider. Invite the end users to get the hands-on experience. Your service provider can give an initial introduction and then have some of your key users run simulations. In this way, any usability challenges can be addressed. The session should be recorded for others to see and/or revisit.

All user guides and documentation should be saved to a central online repository available to your team members.



Thou shalt leverage your service provider

Keep your eyes and ears open throughout the engagement for any other skills or capabilities your service provider

might have that could benefit your organization. Go to their website and do some research on their core capabilities. Know your partner.

Some organizations like the one-source-responsibility approach to contracting. This way, they deal with one vendor as opposed to several. You may want to develop relationships with sales and delivery teams who become knowledgeable about your environment. This is especially valuable when the service providers deliver good quality of work and demonstrate reliability.



Thou shalt use project management

Many projects fail due to poor communication. A project manager can handle this aspect for you. When it comes to

escalations, for example, there must be a set of ground rules understood by your organization and the service provider. An escalation path/tree is of the essence. You don't want to

escalate to everyone; you want an issue owner and a single communication channel to guide your project back on track. Also, please escalate with a basis. The last thing you want is to create confusion by crying wolf without a good justification.

A project manager also is of valuable assistance to track progress on the execution of your engagement. Especially when there is some complexity involved, formal project management tools should be employed to keep you on track and on budget. The project manager can identify and help to resolve issues that might get in the way of your success.

In conclusion, I cannot dictate what you can or cannot do in a customer role. You may not follow these as commandments, but please consider them strong suggestions. I hope these practical tips help you manage your next implementation more successfully. ■

MARTIN PEREZ, BSc (Eng), MBA, PMP, CISSP, CISA, CCNASec, CISM, is senior project manager for a cybersecurity company in Toronto.

Booz | Allen | Hamilton

ARE YOU READY?

We know that to protect our nation's most sensitive interests against attacks, it's not enough to be a step ahead. We have to be a threat ahead. Together we will secure the future of your organization. Are you ready?

BOOZALLEN.COM

The Cost of Safe and Secure Online

SINCE THE RECENT LAUNCH of Garfield's *Cyber Safety Adventures* and the introduction of Dr. Cybrina, CISSP, we have already reached some 10,000 children in 10 countries. And that was just with Lesson 1: Privacy. In May, we released Lesson 2: Posting, and the positive responses continue to grow as the series itself does. I'm sure our next lesson release—on cyberbullying that is scheduled to be released in October—will also be popular.

Whenever we are at conferences to promote cyber safety, (ISC)² members familiar with the former version of Safe and Secure Online program ask about the cost of new educational materials. I thought I would take this opportunity to explain how your Center for Cyber Safety and Education is funded and why some items are free and some have a small fee.

The Center is legally the charitable trust of (ISC)² but is registered in the United States as a 501(c)(3) charity. This is different than (ISC)², which is also registered as a nonprofit organization but under IRS code 501(c)(6), meaning it is not a charity. Donors or members do not get a charitable

tax deduction for contributions to (ISC)², nor is there a cash dividend paid to shareholders like a for-profit company.

But donors (individuals and corporations) could get tax deductions for financial contributions to the Center. Because of this distinction, the Center operates independent from (ISC)², while still under the umbrella of the (ISC)² Board of Directors. In fact, (ISC)² is the Center's biggest donor, but not its sole supporter. Just a couple of years ago, (ISC)² did provide nearly 95 percent of the Center's operating income; that's now down to about 60 percent. (ISC)² hasn't decreased its

support of our programs; rather, we are gaining support from other sources and companies and are beginning to stand on our own in delivering educational programs around the world.

Since we don't charge dues or membership fees, we must count on donations from individuals and companies to continue our research, scholarships and education programs. This year, we are expanding fundraising opportunities, including May's silent auction at CyberSecureGov; TopGolf outings in Washington, D.C., and Tampa; and a big blowout casino night-themed party at Security Congress in Austin in September. You can learn about all of these events (with more to come) at www.IAmCyberSafe.org/events.

Since we don't charge dues or membership fees, we must count on donations from individuals and companies to continue our research, scholarships and education programs.



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

Those interested in our Safe and Secure Online program can find materials for parents, seniors and children on our website www.SafeAndSecureOnline.org. The only item that has any cost is the additional (and optional) printed materials for the Garfield's Cyber Safety Adventures program. These items, including the very popular Educators Kit, are available by ordering online.

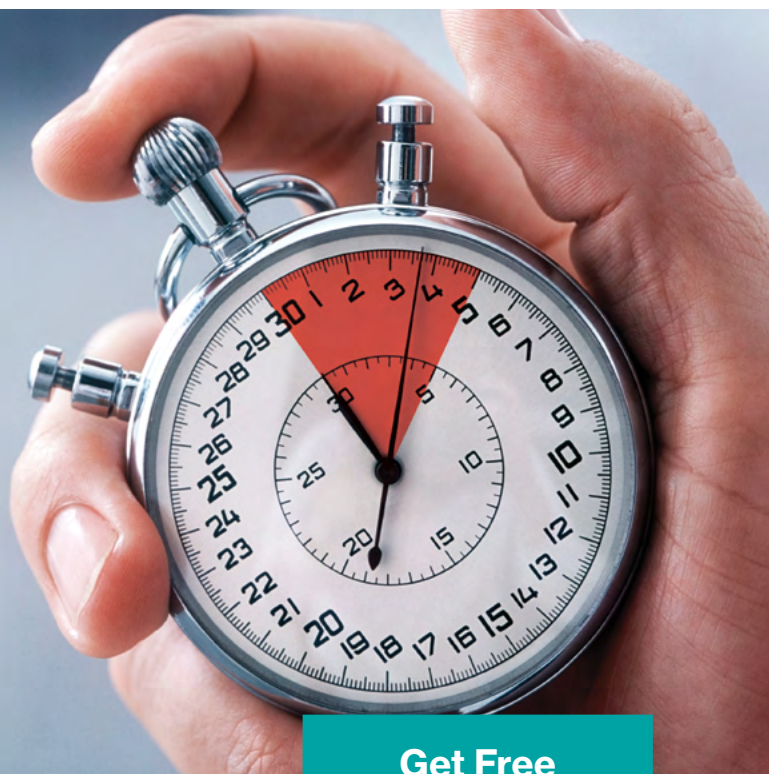
These printed materials are sold at cost—we don't profit from sales, but must raise the funds to cover our own production expenses as we build out a more robust fundraising pipeline. The Center's small but dedicated staff is working hard to make sure that we meet all our goals—and all of (ISC)² members' expectations. ■



SearchSecurity

It takes minutes to compromise a system.

Only seconds to be better prepared.



Get Free Membership

In 93%* of confirmed data breaches, it takes attackers “minutes or less” to compromise a system. It’s critical that you arm yourself with the latest information about the industry.

Take 60 seconds to join SearchSecurity, where professionals turn every day to solve their toughest security challenges. As an (ISC)² member, it’s **FREE** to join, and you’ll gain access to our monthly online **Information Security** magazine, which covers topics like:

- **Malware analysis** beyond the sandbox
- Defending against the **digital invasion**
- Regaining control of **cloud compliance**
- Emerging **security threats** from every which way
- Strategies for **perimeter network security**

Get your free SearchSecurity membership and online magazine at:
www.SearchSecurity.com/ISC2



* 2016 Verizon Data Breach Investigation Report

5

minutes with...

Carlos Cañoto, CISSP

Carlos Cañoto is a virtual systems engineer manager originally from Caracas, Venezuela, and now working in Amsterdam, the Netherlands. He's been an (ISC)² member since 2006.

Did you ever think you'd be working in information security when you were a child?

Not really; my interest in computer science started at the beginning of high school (mid- to late '80s) doing basic programming with "shy attempts" to develop video games, working with databases and information systems. The interest in the security field came as I started to see not only how programs worked, but also how they failed and how you can make them fail. Then after college, networking and security became my main interest.

What do you find most rewarding about what you do?

In my current role, I am not as involved in the day-to-day operations as I used to be (although I try to be as much as possible, as well as continuously learn and develop). But I am working closely with entry-level engineers and what I find rewarding is to support them as they gain the proper skills set and mindset for their future.

You recently moved from South America to the Netherlands. What was that transition like?

As with every change, it was difficult at the beginning: new culture, different ways of doing things, new regulations, new language, etc. But

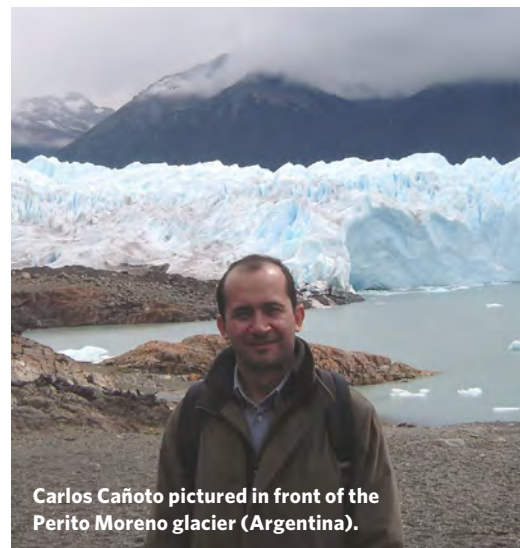
at the same time, it was, and still is, a wonderful experience, both from a professional and personal point of view. You have to learn new things every day. Also, as a father of two small children, I get to see them grow in such a rich, diverse environment. It's amazing how fast they adapt and develop new skills.

What are you working on now that might improve information security in the near future?

At the moment, I think that helping develop a new generation of engineers with the right set of tools and awareness about the field is the most meaningful contribution. Another project in mind for the future is the Center for Cyber Safety and Education's Safe and Secure Online program, which helps kids start with the right foot in cyber education.

What solutions excite you, and why?

There are many, but currently I would like to focus first on the security of "things." We are quickly approaching a point where every common device is connecting to the network, which brings enormous value, but also increases the exposure to risks in a way we have never experienced before. It's very difficult and there are many different approaches to the problem (depending on the kind of device, its criticality and even



Carlos Cañoto pictured in front of the Perito Moreno glacier (Argentina).

vendor), but I think every industry will (and many already are) put a significant effort towards securing their devices.

Where do you believe your peers in the Netherlands are experiencing the greatest threats to cyberattacks?

We live in a highly connected world, so the risks we face in the Netherlands are not very different than those faced in other parts of Europe or the United States. They also can come from anywhere in the world, but in general, I would say that a rapidly expanding attack surface is one big factor (related to the previous question). Now, the ability to consolidate data from many different sources and platforms, and being able to extract useful information on time to react, is more important than ever. ■

An expanded version of this interview will appear in the August issue of *Insights*, a companion e-newsletter for the (ISC)² membership.

A person with a large backpack is standing on a grassy hill, looking out over a landscape at sunset. The sky is a mix of orange, pink, and blue, with clouds catching the low light. The person is in silhouette, wearing a dark t-shirt, shorts, and hiking boots. The backpack is large and blue with orange accents. The overall mood is contemplative and adventurous.

**E-BOOKS
ARTICLES
BLOG POSTS
INFOGRAPHICS
CASE STUDIES
NEWSLETTERS
SUCCESS STORIES**

**A NEW PERSPECTIVE ON
YOUR BRAND'S NARRATIVE**

Using words and images that are unique to your branding, Twirling Tiger Media can help you tell your company's story cohesively across multiple content marketing solutions.

**TWIRLING
TIGER** *media*

*creators of content you
can sink your teeth into*

Contact info@twirlingtigermedia.com