EXECUTIVE LETTER › **GETTING GOVERNMENT'S EAR**

# InfoSecurity PROFESSIONAL

MARCH/APRIL 2015

*A Publication for the (ISC)²® Membership*

## Stop It Right There

### MANAGING PRIVILEGED IDENTITY

**Latest on Insider Threats**

**4 Ways to Reduce Stress**

**5 Minutes with Jefferson Gutierrez**

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

# Contents VOLUME 8 • ISSUE 2

As attack vectors grow, so do the threats posed by those who undermine security measures. *PAGE 21*

## FEATURES

## DEPARTMENTS

Cover Image by ©iStock
Illustration *(above)* by
©ENRICO VARRASSO

*InfoSecurity Professional* is published by Twirling Tiger Press Incorporated, 7 Jeffrey Road, Franklin, MA 02038. Contact by email: asaita@isc2.org. The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)² on the issues discussed as of the date of publication.

## Editor's Note

# BOWING TO THE BAD DAYS

**I AM WRITING THIS** column without the use of my left hand, which I broke recently in two places following an unspectacular fall. I'm also staring into our kitchen after the ceiling collapsed at 3 a.m. from a water pipe leak. I have broken bones before and had my share of home disasters, but my reactions to both differed from previous setbacks.

I'm learning, slowly but surely, to change how I respond to run-of-the-mill stress—even freak accidents. I was inspired by a talk on mindfulness at last year's Security Congress in Atlanta and have put some of the presenters' suggestions into practice. So far, I've met my deadlines despite my temporary disability and haven't hit a wall (or worse) as the water damage spreads.

In this issue, I share some general information on four specific recommendations—meditation, yoga, tai chi, and qigong—should you, too, feel you need a new way to cope with stress. These come compliments of Mike Rothman and (ISC)$^2$ board member Jennifer Minella. You may have your own outlet to help you relax and react more positively to the challenges we all face at work and home. I'd love to hear what they are.

We also tackle an always timely topic: privileged identity and access management and, somewhat related, the insider threat employees and contractors pose, intentionally or not. With the rise in widely publicized data breaches, this may be a good time to revisit your organization's policies and practices.

I'm also delighted to introduce another active member of the (ISC)$^2$ global community: Jefferson Gutierrez in Bogota, Colombia. Like the previous "5 Minutes with…" featuring Javvad Malik, you can read an excerpt of our interview on page 31 and the full Q&A in the next issue of our companion e-newsletter, *Insights*. Look for it in your inbox early next month.

› **ANNE SAITA** asaita@isc2.org

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

©Rob Andrew Photography

InfoSecurity PROFESSIONAL

**(ISC)$^2$ MANAGEMENT TEAM**

EXECUTIVE PUBLISHER
**Erich Kron, CISSP-ISSAP, HCISPP**
727-785-0189 x4070
ekron@isc2.org

DIRECTOR, MEMBERSHIP RELATIONS AND SERVICES
**Erich Kron, CISSP-ISSAP, HCISPP**
727-785-0189 x4070
ekron@isc2.org

SENIOR MANAGER OF MEMBERSHIP MARKETING AND MEDIA SERVICES
**Jessica Smith**
727-785-0189 x4063
jsmith@isc2.org

PUBLISHER
**Timothy Garon**
508-529-6103
tgaron@isc2.org

MANAGER, GLOBAL COMMUNICATIONS
**Amanda D'Alessandro**
727-785-0189 x4021
adalessandro@isc2.org

MEMBERSHIP MEDIA SERVICES ASSISTANT
**Michelle Fuhrmann**
727-785-0189 x4055
mfuhrmann@isc2.org

**SALES TEAM**

EVENTS SALES MANAGER
**Jennifer Hunt**
781-685-4667 jhunt@isc2.org

REGIONAL SALES MANAGER
**Lisa O'Connell**
781-460-2105
loconnell@isc2.org

**EDITORIAL ADVISORY BOARD**

**Elise Yacobellis** *(ISC)$^2$*
**Erich Kron** *(ISC)$^2$*
**Javvad Malik** *EMEA*
**J.J. Thompson** *U.S.A.*
**Carlos Canoto** *South America*
**Dr. Meng-Chow Kang** *Asia*

**TWIRLING TIGER PRESS INC. EDITORIAL TEAM**

EDITOR-IN-CHIEF
**Anne Saita** asaita@isc2.org

ART DIRECTOR & PRODUCTION
**Maureen Joyce** mjoyce@isc2.org

MANAGING EDITORS
**Deborah Johnson**
**Lee Polevoi**

Twirling Tiger Press Inc. 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.twirlingtigerpress.com

RETURN TO CONTENTS

(ISC)²®

CYBER SECURE GOV

2015

# REGISTRATION IS NOW OPEN!

(ISC)² Member Discount
Earn 16 CPEs

REGISTER NOW

May 14th and 15th, 2015
Ronald Reagan Building and International Trade Center in Washington, D.C.

## From Zero to 60, (ISC)² CyberSecureGov is Advancing the Cybersecurity Workforce.

Join us for an insightful two days as cybersecurity experts from government, industry, and academia share on how to maximize resources in order to keep pace with cyber threats. Attendees will gain an in-depth knowledge on what new threats —and solutions— are emerging, the future legislative and political landscape, funding new initiatives in a post-sequestration reality, effectively adopting federal security initiatives and guidance, how best to recruit, retain, and educate the future cyber workforce, and more.

- Keynotes from leading government cyber security professionals
- Panels with industry leaders
- Three dedicated tracks
- Networking with experts and cyber security professionals

cybercecuregov.isc2.org | #CybersecureGov

THE LATEST FROM (ISC)²'S LEADERSHIP

**EXECUTIVE LETTER › DAN WADDELL**

# STRENGTHENING OUR GOVERNMENT ROLES

**WHEN I ASSUMED** the role of (ISC)² Director of U.S. Government Affairs a year ago, I was surprised to discover how little the U.S. government managers and executives I visited knew about the organization. This is despite the fact there are currently more than 12,000 (ISC)² members living within a 50-mile radius of Washington, D.C., most of whom are federal government employees, contractors, or consultants.

If you look within the Beltway—the geographic area that represents the seat of the federal government—a lot of IT security leaders are CISSPs, but they may not necessarily know we have other credentials and training programs, or that our Foundation helps provide scholarships and vouchers to those entering our career field.

**Dan Waddell**, CISSP, CAP, is the (ISC)² Director of U.S. Government Affairs. He can be reached at dwaddell@isc2.org.

As a longtime member and volunteer, I have long known how (ISC)² can enhance careers and strengthen enterprises. I started my IT career in 1993 as a systems administrator for a major federal contractor before embarking on an information security specialty after the 9/11 terrorist attacks. I became a CISSP in 2004 and earned my CAP in 2007.

Soon, I became more involved with the organization through the Safe and Secure Online program. Eventually, I was asked to join the (ISC)² North American Advisory Board, and last year assumed my current role.

In the past year, I've stepped up our communications and outreach to help spread the word about what we do beyond security certifications. That initiative is going to continue. We are a global organization that wants to provide a safe and secure world for *everybody*. That's something that plays well in Washington.

In addition, we are still going to spread the message that our certifications help strengthen the government cybersecurity workforce. We've made great strides in the past year in this regard, participating in efforts such as the National Initiative for Cybersecurity Education (NICE) and working with the Department of Homeland Security to make sure our offerings are located in their National Initiative for Cybersecurity Careers and Studies (NICCS) training portal.

In short, there's definitely a need to educate government leaders about how we can help them, especially given the growing cyber threat and shortage of cybersecurity professionals within the U.S. government.

After 9/11, I decided to do my part and step up my game to help improve our government's cybersecurity posture. I am not alone. There are many more like me who are drawn to a compelling mission and choose to work in the public sector.

I look forward to meeting with more of these men and women in the coming year at Chapter events and our upcoming CyberSecureGov conference May 14-15 in D.C. Together, we can share ideas and knowledge, help each other grow, and work together to make the cyber world a safer place for all. ●

RETURN TO CONTENTS

0%*
This is the unemployment rate in the field of cyber security.

## Answer the Call for Cyber Security Experts With an IT Degree From Walden.

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

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

## Get Credit for Your Professional Certifications.

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

**Recognized Quality**

Accredited ABET Computing Accreditation Commission

Global Accreditation Center for Project Management — Accredited Program

Committee on National Security Systems — CNSS — Systems Security for the 21st Century

## Explore our programs at WaldenU.edu/cybersecurity.

*Source: International Information Systems Security Certification Consortium, 2013 Global Information Security Workforce Study. Available online at https://www.isc2.org/GISWSRSA2013.

**Walden University**

*A higher degree. A higher purpose.*

## COMING IN APRIL:

# CISSP® AND SSCP® CREDENTIAL ENHANCEMENTS

BY DAVID SHEARER, CISSP, PMP, EXECUTIVE DIRECTOR

DURING OUR 26-YEAR HISTORY, (ISC)² has earned a reputation for providing gold standard information security credentials. Maintaining the relevancy of those credentials amidst the changes in technology and the evolving threat landscape is a core strategy upon which this organization was built.

As a result of a rigorous, methodical process that (ISC)² follows to routinely update its credential exams, I'm pleased to announce enhancements to both the Certified Information Systems Security Professional (CISSP) and Systems Security Certified Practitioner (SSCP) credentials, beginning April 15.

Both credentials reflect knowledge of information security best practices but from different facets. SSCPs are typically more involved in hands-on technical, day-to-day operational security tasks. Core competencies for SSCPs include implementing, monitoring and administering IT infrastructure in accordance with information security policies, procedures and requirements that ensure data confidentiality, integrity, and availability. CISSPs, while also technically competent, typically design, engineer, implement and manage the overarching enterprise security program.

SSCPs and CISSPs speak the same information security language with unique perspectives that complement each other across various IT departments and business lines.

We have refreshed the content of the official (ISC)² SSCP CBK to reflect the most pertinent issues that security practitioners currently face, along with the best practices for mitigating those issues. The result is an exam that most accurately reflects the technical

## SSCP DOMAINS

*Effective April 15, 2015*

1. Access Controls
2. Security Operations and Administration
3. Risk Identification, Monitoring, and Analysis
4. Incident Response and Recovery
5. Cryptography
6. Networks and Communications Security
7. Systems and Application Security

## CISSP DOMAINS

*Effective April 15, 2015*

1. Security and Risk Management (Security, Risk, Compliance, Law, Regulations, Business Continuity)
2. Asset Security (Protecting Security of Assets)
3. Security Engineering (Engineering and Management of Security)
4. Communications and Network Security (Designing and Protecting Network Security)
5. Identity and Access Management (Controlling Access and Managing Identity)
6. Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing)
7. Security Operations (Foundational Concepts, Investigations, Incident Management, Disaster Recovery)
8. Software Development Security (Understanding, Applying, and Enforcing Software Security)

RETURN TO CONTENTS

and practical security knowledge that is required for the daily job functions of today's frontline information security practitioner.

Some candidates may be wondering how these updates affect training materials for the CISSP and SSCP. As part of the organization's comprehensive education strategy and certifying body best practices, (ISC)$^2$ training materials do not teach directly to its credential examinations. Rather, (ISC)$^2$ Education is focused on teaching the core competencies relevant to the roles and responsibilities of today's practicing information security professional. It is designed to refresh and enhance the knowledge of experienced industry professionals.

> **"The result is an exam that most accurately reflects the technical and practical security knowledge that is required for the daily job functions of today's frontline information security practitioner."**

If candidates have recently participated in or plan to participate in an (ISC)$^2$ training course for the CISSP or SSCP soon, we encourage them to go ahead and schedule their examination at a Pearson VUE testing center for a date prior to April 15, 2015. If candidates are currently enrolled in a training course or are unable to sit for the CISSP or SSCP credential examination prior to April 15, 2015, I believe that an (ISC)$^2$ training course is still a beneficial step in their study plan.

For more information, please refer to the FAQs on our Website. And as always, our global Member Services Department is available to answer any additional questions at membersupport@isc2.org. ●

## AND THE NOMINEES ARE...

(ISC)$^2$ is proud to be named a finalist in three categories for the 16th annual *SC Magazine* Awards U.S. They are:

- Best Cybersecurity Higher Education Program – **(ISC)$^2$ Global Academic Program**
- Best Professional Certification Program – **CISSP and CSSLP** *(separate nominations)*
- Best IT Security-Related Training Program – **(ISC)$^2$ Education/Training Program**

Award recipients will be announced on April 21 at the InterContinental San Francisco. ●

## (ISC)$^2$ VALUES YOUR FEEDBACK!

WE INVITE YOU to take 10 minutes to respond to the (ISC)$^2$ Member Benefit Survey. Let your member voice be heard as it relates to member benefits and the experience you are looking for as an (ISC)$^2$ Member. This will help (ISC)$^2$ shape the future as we work to provide you with benefits that matter to you.

Niamh V. Muldoon *(in red gown, above)*, celebrates an evening at *Information Age*'s Women in IT Awards.

# IRELAND'S MULDOON A 'SECURITY CHAMPION'

SHE MAY NOT have ultimately earned the title Security Champion of the Year, but finalist Niamh V. Muldoon still feels like a winner just for making the shortlist.

She writes in an email after the ceremony. "I was the only female in Ireland to make the [shortlist], and what a great achievement to be nominated in the security category."

I was happy that I was nominated as it is also a recognition, to all the people who gave me their time and support to get me to where I am in my career today," she says. "But the one person I really wanted to recognize was my champion—my mother, Violet Muldoon. Not only did she support me with my security career, she paved the way for women in leadership in all aspects of her life career, parenting and sporting perspective."

Muldoon, who is the EMEA technology risk and compliance program manager at Workday, a leader in enterprise cloud applications for Finance and HR, was among five other female finalists for the award, which is part of *Information Age*'s Women in IT Awards. Prior to the ceremony, the magazine featured Muldoon in an article she wrote about her career.

Setting a precedent is not new to Muldoon, who became Ireland's youngest female CISSP in 2004. By then she'd earned undergraduate degrees in economics and geography and had completed a postgraduate information technology program for the Irish Financial Institute as a software engineer, later specializing in information security

She credits others for being a guiding force, especially her son Crean and fellow (ISC)² member Richard Nealon. "I call this man Ireland's information security godfather, and he still continues to encourage me. I have yet to meet anyone still as passionate and committed to the profession. Passion and support are key components to having a successful career in this industry." ●

**CPEs**

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

https://live.blueskybroadcast.com/bsb/client/CL_DEFAULT.asp?Client=411114&P-CAT=7777&CAT=9432

## ANNOUNCING THE 2015 (ISC)² BOARD OFFICERS

Effective January 24, 2015, the following individuals assumed Board officer positions:

*Chairperson:*
**Prof. Corey Schou**
Ph.D., Fellow of (ISC)2, CSSLP (U.S.A.)

*Vice Chairperson:*
**Flemming Faber**
CISSP (Denmark)

*Treasurer:*
**Diana-Lynn Contesti**
CISSP-ISSAP, ISSMP, CSSLP, SSCP (Canada)

*Secretary:*
**Jennifer Minella**
CISSP (U.S.A.)

The 2015 (ISC)2 Board of Directors met January at the organization's Clearwater, Fla., headquarters. *Pictured above, top row, left to right:* Freddy Tan, Prof. Hiroshi Yasuda, Prof. Howard Schmidt, Allison Miller, Dave Lewis, Richard Nealon, Greg Mazzone, Steven Hernandez. *Bottom row, left to right:* Board Treasurer Diana-Lynn Contesti, Board Vice Chairperson Flemming Faber, Board Secretary Jennifer Minella, Board Chairperson Prof. Corey Schou, Dr. Meng-Chow Kang.

RETURN TO CONTENTS

GLOBAL SPOTLIGHT:
**(ISC)² SACRAMENTO, CALIFORNIA CHAPTER**

# COMMUNITY OUTREACH IS A WIN-WIN PROPOSITION

THE (ISC)² SACRAMENTO CHAPTER has reached more than 1,800 students, teachers, parents, and seniors through the (ISC)² Foundation's Safe and Secure Online program. As the first chapter to reach this level, it's a milestone worth noting and a measure of the Chapter's commitment to its community.

Chapter co-founder and chairman Tony Vargas, CISSP-ISSAP, CSSLP, says he realized after looking at his market that (ISC)² Sacramento had a specific calling. "We found a real gap around community outreach."

> **"Chapter members are working with area community colleges on Cyber Patriot, presenting at area conferences and a high school science fair."**

Part of that gap, Vargas admits, was "that a lot of people don't know what cyber security is." Outreach is an opportunity to spread the word about cyber security and change perceptions in both camps. Vargas recalls a conversation with an attendee at a presentation: "We started talking to people, and they would say, 'Wow, you're a normal person.'"

Since the Chapter's beginnings in 2012, it has assisted in the formation of other chapters, expanded its board to include representatives from a variety of area businesses and organizations, and received U.S. federal and state 501(c)3 non-profit status. Chapter members are working with area community colleges on Cyber Patriot, presenting at area conferences and a high school science fair.

Tony Vargas (l), and Steven Hershman

› **(ISC)² SACRAMENTO CHAPTER INFORMATION**
CONTACT: Tony Vargas, Chapter President
EMAIL: president@isc2chapter-sacramento.org
WEBSITE: http://www.isc2-sacramento-chapter.org

The Sacramento Chapter is also charting new territory in raising sponsorship dollars. The Chapter does not levy dues (and has no plans to do so) but has garnered more than $10,000 in donations from businesses and foundations, some of which has been donated back to the (ISC)² Foundation. How did they do it? "Number one: Just ask," Vargas advises. "Companies have foundations and want to give back." Also, look for mutually beneficial scenarios, such as market-wide industry gatherings where potential sponsors will get the additional reward of heightened visibility.

The Sacramento area-wide security industry conference is something Tony Vargas wants to institutionalize. Rather than members having to "go from meeting to meeting to meeting" for their various groups and, perhaps ultimately, having to pick just one organization, Vargas envisions a joint event that benefits all. Each group can have its own meeting and then share in panels, presentations, and (hopefully) sponsorship money. He's currently talking with Sacramento security groups to propose just that.

Ultimately, Vargas believes, the sense of community is vital to the Sacramento group: "There are going to be times when, to really move things, you have to work with other people. That's what really highlights this chapter." ●

*—Deborah Johnson*

RETURN TO CONTENTS

TEACHABLE
MOMENTS FROM
(ISC)² SECURE
WEBINARS
AND EVENTS

**MODERATOR'S CORNER › BRANDON DUNLAP**

# THE FIRST 90 DAYS

**AS THE NEW YEAR** begins to settle down, I look back over the past 90 days and wonder if I have accomplished as much as I could have in 2014.

Since leaving the world of consulting last fall to become the global CISO for a fast-growing multi-national corporation, I am beginning to find the natural organizational rhythm to be far different from what I am accustomed to.

I am continually checking in with my leadership team and asking, "Am I trying to move too quickly?" or "Why do things seem to move so slowly?" Their usual response is, "It's moving at the pace we expected," while reminding me that I am once again the "insider'" looking out, as opposed to the "outsider" looking in.

**Brandon Dunlap** moderates (ISC)² webinars and other educational programs. He can be reached at bsdunlap@brightfly.com.

According to my leadership team, one of the things they are eager to tap into is my professional network—the community of practitioners with whom I spend so much time. They see tremendous value in the time I spend with all of you, exploring the various facets of our profession. And now I am starting to look back and see just how much ground we have covered over the years, how it has informed who I am as an information security professional, and, indeed, how truly valuable this community is.

In these first few months on the job, I have found myself digging into the archives of our ThinkT@nk roundtables, e-Symposiums, and Security Briefings, looking for answers to questions I didn't ask at the time.

As I settle further into my new role, I start to see that my questions are likely not that different from yours, and that the archives are often just as relevant now as when we first recorded the sessions. It is rapidly becoming a go-to resource for me—one that pays dividends beyond the CPEs. It continues to inform and shape my thoughts around the tactics and strategies of our collective profession.

> **"According to my leadership team, one of the things they are eager to tap into is my professional network—the community of practitioners with whom I spend so much time."**

This new organization I joined recognizes what perhaps some of us take for granted: how this forum, and many others like it, nurture our professional lives and gives us new insights and understanding. It is through their generosity that I will be able to continue to play host and moderator to the many new conversations well into the future.

Now, though, I'll do so sharing the same perspective as all of you—on the frontlines and in the trenches. ●

RETURN TO CONTENTS

# BEATING THE BREACHES

## UNDERSTANDING WHAT PRIVILEGED IDENTITY MANAGEMENT CAN—AND CAN'T—DO IS ONE WAY TO HOLD OFF HACKERS

BY **MICHELE KRIEGMAN**

IMAGE BY ©ISTOCK

QUICK! How is financial information security like Hollywood? You could say both manage digitized assets (once shows and movies stopped being stored on film, they essentially became multimedia digital data). Today, though, the response more likely is they both have had headline-grabbing data breaches. Among the biggest newsmakers in 2014 were revelations about widespread data thefts at financial behemoths like JPMorgan Chase and stolen files leaked to the press on entertainment juggernaut Sony.

The silver lining for the silver screen is that these hacks have brought new appreciation for privileged identity management (PIM), which is used to handle an enterprise's most powerful accounts and prevent internal data theft. The term also is sometimes referred to as privileged user management, privileged account management (PAM), privileged identity and access management (privileged IAM), or simply PxM. In fact, notes Russell Miller, a director in the Identity and Access Management practice at CA Technologies, “Almost

RETURN TO CONTENTS

every breach involves targeting a privileged account so [hackers] can get back into the system and expand their control of the network over time."

## TRENDS TO WATCH

In the wake of these attention-grabbing, brand-breaking headlines, information security experts have identified several trends gaining traction. They include alliances and bundling of services by vendors, automation of identity access management, PIM analytics, multiple mobile and cloud identity plays, and IAM application programming interfaces (APIs).

### › *Alliances and bundling*

Until recently, there generally were few solutions available to solve identity and access challenges, recounts Bryan Wiese, practice director for identity and access management at Kansas-based FishNet Security, which was recently acquired by Blackstone Group and merged with Accuvant.

"Information security teams had limited options when it came to building product integrations between products offering different IAM functionality in order to address end-to-end business challenges and needs. They would often build these product-to-product integrations in-house or hire third-party professional services organizations rather than bring in a vendor, who sometimes pushed an oversimplified integration message of 'You can slap on what we offer as a top layer over what you've already got.'"

Soon, however, Wiese predicts the landscape will include more service agreements and bundling between vendors. "Best-of-breed vendors are already starting to focus their product engineering and management teams on their core strengths while building product alliances that can serve the customer better than a vendor who, in the past, tried to be all things to all clients.

"These alliances are starting to align cross-vendor teams without always requiring the presence of an OEM agreement and are starting to branch out from proprietary integrations into emerging standards like the system for cross-platform identity management (SCIM). They are better than trying to customize or build product integrations in-house, especially if IAM is not your core business."

### › *Automated IAM*

Another developing trend includes associating passwords, authorizations, and privileges with an individual user in a way that goes beyond the current federation of access management and single sign-on services. It may enable seamless access where a user may not even know the password to the system they are accessing because it relies on machine authentication based on a user profile.

"Automation is the key. The more you can automate and simplify your processes in IAM, the easier they will be to manage, update, and govern," says Shabbir Bashir, manager of network security for Verizon Wireless in New York, N.Y. Automation could include removal of privileges after separation or internal transfer.

### › *Privileged identity management (PIM) analytics*

CA Technologies' Russell Miller predicts that "PIM analytics will be huge. That gets back to [the fundamental idea of] understanding being so important. You need to understand your people and take action based on what you see. For example, if an admin does something they normally don't do or is out of policy, additional controls such as two-factor authentication, would send a one-time password to their cell phone or require a step-up authentication."

### › *Growth in cloud and mobile*

There will be more growth for all areas in information security around privileged identity management. FishNet's Wiese anticipates that there will be more cloud-based Identity as a Service (IdaaS) vendors with the line between IAM and other security domains blurring as "other traditionally non-IAM vendors like firewall vendors begin to focus on certain aspects of IAM and find ways to combine IAM with cloud and mobility security."

Several experts see more federation into the cloud, with reliance on mobile in the authentication process. However, notes Vice President for IT Security at New York Life Insurance Michael Platoff: "Identity and access management vendors are pushing technologies like containers and multi-factor authentication, using the mobile device as a factor in their IAM suites, but I'm not sure that these technologies need to be as tightly coupled to the IAM suite as IAM vendors are suggesting. MDM [mobile device management]

RETURN TO CONTENTS

## 9 TIPS FOR STARTING A PRIVILEGED IDENTITY MANAGEMENT PROGRAM

BY MICHELE KRIEGMAN

**1.** Don't user hacker-friendly labels for security administration accounts or root files. This was said to be a facilitating vulnerability that the Chinese People's Liberation Army exploited in an attempt to obtain information about U. S. Department of Defense contracts several years ago. One hacked contractor literally named its privileged account for security administrators "SecurAdmin", a sure welcome mat to illicit elevation of network and account privileges.

**2.** Evaluate your assets, advises Javvad Malik of 451 Research. "I'd say number one is knowing your critical assets. What is the secret sauce of the company to help you focus on what to protect?"

**3.** Understand your privileged accounts. Russell Miller of CA Technologies urges you to get a handle on how many there are, who's accessing them, how many have a shared password, and where those are being stored. Then build out privileged identity governance. And, adds New York Insurance's Michael Platoff, by extension, "Get the governance right across the organization."

**4.** Don't bite off more than you can chew. Scope of the program or project has to be clearly defined.

**5.** Use people well. Make your vendors into partners. Find a mentor to help guide you. One route is your professional network in organizations, such as (ISC)$^2$ or LinkedIn.

**6.** Verizon's Shabbir Bashir also returns to a fundamental for any large and sensitive rollout. "First and most important, get executive buy-in."

**7.** Get the architecture right to get standards around identity across the enterprise infrastructure, including middleware. At the same time, reach out and work with the app owners. Push app owners to comply with identity standards. Wiese notes that in the case of ephemeral social media, there is pressure to overlook IPS and IDS network deployment and internal server endpoint security. "Valuation is king and IPO the ultimate goal, and both of those things are directly tied to usability, functionality uniqueness, present and future user population, and future revenue models/streams. None of those things focuses on security."

**8.** In addition to controlling access to passwords to the accounts, it's also important that an IAM program control access once people log in. Miller provides an example. "For shared accounts on UNIX, organizations need to focus on least-privileged access. Have controls in place, but still hold people accountable by tracking what actions each individual took, even while using a shared account. You should never have shared passwords. Instead, practice shared account password management so all administrators log into a password safe with their own credentials, and, they are granted or denied access to accounts."

**9.** Beware of internal weaknesses, Miller warns. "When people think about PIM, they think about malicious admins, but insiders can be exploited with social engineering, or there are those careless insiders with excessive privileges who can cause damage." The latter can happen within a group or as an individual moves to another group within the larger organization yet maintains access. Both scenarios violate the principle of least privilege. ●

vendors and others are approaching these technologies from another direction. While integrated solutions from IAM vendors may be useful, do not overlook best-of-breed solutions."

### › *Beyond omni-channel access with the "Internet of Things"*

Tyson Whitten, director in API Management at CA Technologies, notes that omni-channel engagement initiatives will have a direct impact on API growth and the need for privileged identity management.

"We're seeing a significant amount of focus on improving engagement across the customer experience lifecycle. No longer is access limited to the Web and mobile app; it has expanded to new channels, where the Internet of Things has become a strategic method of engagement, with the API as the fundamental connectivity point enabling access to these endpoints. But just blocking at the border is no longer acceptable. Access must be allowed, so there's a trend towards more sophisticated access control across all channels—web, mobile and APIs—to enable unified access without negatively impacting experience, and identity is key," he says.

Whitten continues, "It's all about context. Omni-channel access has moved beyond traditional engagement models. Consumers are now using apps to physically access the automobile with partners such as insurance companies accessing driver behavior informa-

RETURN TO CONTENTS

## ADVICE FOR ACCESS CONTROL AND APPLICATION PROGRAMMING INTERFACES (API)

**Tyson Whitten, who works in API development for CA Technologies, offers some advice for integrating access control into the API lifecycle.**

**Design** your solution for performance and scaling by using a common standard. If you think of mobile apps, whether they are internally developed or a cloud app or a third-party app, you can use a standard at the appropriate handoff.

**Integrate** with an existing authentication investment, such as CA Single Sign-on (formerly CA SiteMinder), etc., within the larger identity infrastructure.

**Establish** token governance policies that manage token lifecycles centrally.

**Ensure** appropriate grant types to provide different experiences with different authorization based on scenario, application and user, including privileged user. ●

tion. It's no longer only about privacy but ensuring safety. Organizations must implement more fine-grained control to be effective given the volume of users, devices and identities that are accessing applications."

### › *Password vaults*

Javvad Malik, senior analyst at New York-based 451 Research, says, "Unless inherent insecurities are found, we'll probably see a rise in the use of password managers and 'password vaults' within organizations. This is good, as today we're still trying to educate users on strong passwords and relying on them to remember each."

### › *Securing the open enterprise through APIs*

As companies go to market in the application economy, they are dealing with additional levels of risk as they externalize data or internal services, dissolve borders with cloud services, and increase connectivity to mobile app developers. CA Technologies Whitten sees a new demand for end-to-end security as a result. "Whether it's a firewall or an API, you're opening up the business. Proper security of APIs must account for malicious threats that can circumvent vulnerable APIs. But user and application access to the API also must be controlled.

## MASTERING INTEGRATED MULTIPLE PRIVILEGED ENVIRONMENTS

Scalability and integration with partners, vendors, legacy systems, and acquisitions are the twin challenges for companies in a growth mode.

Starting with the idea that "understanding is the foundation of PIM," Miller offers a mini-checklist for a successful integration:

- What are their work hours?
- What devices do they use?
- What is their data?
- What are the crown jewels?
- What data is the most damaging?
- What do you need to protect by law or regulation?
- What do you need to look at for vulnerabilities?

*(See "7 PIM Vulnerability Mitigation Guidelines," p. 18.)*

New York Life's Platoff argues that in addition to technical solutions, privileged accounts need special attention under identity lifecycle management. "Some companies go in hoping their partner will disable an account, but they should create a contractual obligation and requirements for recertification of access with the partner.

"Federated identity is powerful, because when they disable a user, that user can no longer get into yours either. A lot of companies utilize jump stations with more stringent auditing when they bring in partners, rather than employees. Of course, this applies to all identity management, not just PIM/PAM."

Verizon's Bashir stresses standardization as the key to moving forward fast. "Keep it simple. For example, be able to say 'you must only use these three access control vendors moving forward.' If you eliminate unnecessary complexity, you'll [be able to] develop repeatable business processes against those standards."

## EXECUTIVE CONSIDERATIONS ON THE WAY TO PRIVILEGED SUCCESS

Bashir offers a tactical view of an IAM organization. He has found that "because you are changing the culture for the better, an IAM program manager or director should not be more than a step removed from the CSO or CISO."

He details that "in an ideal organization, you'd

RETURN TO CONTENTS

## 7 PIM VULNERABILITY MITIGATION GUIDELINES

**1. Expand the focus to the privileges beyond the system admin.** Points of vulnerability involving privileged access also include network administrator, executives with excessive privileges, and the often-overlooked graveyard shift worker with operator privileges. Albany Medical Center's Ed Nadareski points to other categories outside the admin role, such as "super users" and orphaned accounts created during the development process.

**2. Don't overlook segregation of duties, especially in a culture where everyone "needs access to everything."** Shabbir Bashir describes the procedure at Verizon Wireless. "We have a questionnaire for a resource or application owner who wants to integrate with a platform through either physical or logical access. We obtain their current segregation of duties (SOD) requirements and evaluate what changes should be made as part of the integration to ensure SOD rules are adequately met."

**3. Know and manage your vendors.** We learned hard lessons from the Target breach where hackers gained initial access to their network through an HVAC (heating, ventilation and air-conditioning) vendor.

**4. Be aware of privileged accounts.** FishNet's Bryan Wiese advises that they are just as vulnerable to "classic social engineering or phishing of passwords as any other account and are constant targets for disgruntled current or former workers. The elevated value of these accounts and the internal risk they can bring to an organization has accelerated PIM's evolution of multi-factor authentication, advanced password management concepts like password aging, versioning, and archiving, and credential lifecycle management across different types of systems, applications, operating systems, and databases, both on-premises and in the cloud."

**5. Look for protections for shared password vulnerabilities.** Service accounts, root or admin, typically use shared passwords. Dangers increase when the users' efforts to change it after every personnel change prevents them from doing so.

Michael Platoff says, "This is really the gist of PIM/PAM solutions. One approach manages a shared password, but the privileged user never sees the password. The solution also automatically submits the password, so the user never sees the password. These solutions are agentless and typically push users through a jump station to record sessions. The agentless approach is simpler to deploy. It uses session recording as a detective control and has some preventative controls that restrict the commands that can be invoked under the shared privileged account. Agent-based solutions are more complex to deploy, but, due to their agents, they typically have better preventative controls. These solutions also need to support a "break-glass" scenario, where a privileged user actually needs to know the root password (e.g., booting a Unix box into single-user mode). In this case, the user checks out the privileged account password, uses it, and then checks it back in. The solution then changes the root password automatically."

**6. Beware of zero-day vulnerabilities, or vulnerabilities in a program or OS for which there is no patch.** Typically, these exploit access to the admin on the account. Therefore, PIM is an important preventive measure and a control.

**7. Understand that a whole new class of privileged accounts exist in virtual environments, often underpinning the cloud.** These accounts have access to the Hypervisor, and hence all the systems, which "multiplies the opportunities to attack privileged accounts the way the Shellshock breach did," says Miller. "But we're beginning to apply the principle of least privilege to even a root account on UNIX or Linux or an admin account on Windows, based on role, before a hacker can do anything. This can foil even what would normally have been a successful breach." ●

*—Michele Kreigman*

want a manager for physical IAM, a manager for privileged account management access, and one for logical identity management—all reporting to an IAM director. You need that executive air cover at all times."

Platoff says a security career spanning big pharma and insurance has taught him that "there is a correct organizational structure for privileged IAM, and it's in IT. If HR takes over, they may overlook business process outsourcers, contractors, and other non-employees."

Ed Nadareski, manager for security, IAM and disaster recovery at the Albany Medical Center in upstate New York, voiced a view that is gaining traction.

"Hands down, there should not be a silo approach. The more [IAM] becomes 'siloed,' the less effective [it is], and it is not included in discussions around updates or system purchases. In my opinion, it should be in au-

RETURN TO CONTENTS

dit and compliance with other aspects of risk management, not in IT, where it creates a conflict of interest. Ultimately, there should be a report into the board."

To achieve a balance between localization and centralization of security, Whitten believes "there has to be a level of risk that is understood and communicated to the business. In terms of process and approvals, everyone in the organization should be involved, including business and IT. In terms of purchasing, budget is shifting over to the business. For IT to stay relevant and keep a seat at the table, it needs to show relevance."

"The contrarian view is that it's 'not so critical whether it falls under the business units or the CIOs as that it be aligned.' Security needs to be increasingly aligned with the business," according to Wiese.

Miller sidesteps the ownership debate with a fresh view of data. "Traditionally, people in security have been thought of as preventing access. Now you can use security to share more data with your customers and partners. Have the business understand what it can do to lock down data."

Naturally, when talking to executive peers, a key issue arises: demonstrating ROI. Wiese believes it is no longer valid to use cost reductions from people cuts—elimination of full-time equivalents (FTEs)—as the justification, though this has been a successful pitch in past years.

"Frankly, that doesn't happen often," he says. "We've all heard that in the past and have been asked to build ROI models as justification for investment, but the reality is that soft ROI benefits are much more prevalent than hard ROI.

"I think the clearer goal for both large and small organizations should be to focus on building and improving processes that allow good FTEs to focus on other important internal needs, to automate those processes over time with technology investment and implementation, and to govern those processes and technology as part of the IAM lifestyle."

Platoff agrees that the expected saves on people-heavy production costs have proven hard to quantify. He concludes that "compliance, risk avoidance, cost reduction alone won't sell it," so he leans toward qualitative benefits by suggesting that "you can give a better user experience, reducing log on time for soft costs across employees. What are we protecting externally? Reputation for stability."

## TOP 5
## API VULNERABILITIES FOR PRIVILEGED IAM

**CA Technologies' Tyson Whitten outlines the following most common and/or most dangerous flaws in today's privileged IAM programs:**

**1.** Client impersonation to learn where keys are hidden. We're beginning to see more threats from privileged access to external users, as was the case with Snapchat.

**2.** Phishing combined with contact impersonation.

**3.** Both SQL and LDAP injections for escalation of privilege.

**4.** Unauthorized access through three sets of vectors: internal APIs, where someone leverages their relationship with the developers; APIs for social; and lifecycle management inconsistencies in the issuing of tokens between external, internal, or partner users.

**5.** Brute force attacks, such as the Snapchat find-a-friend exploit, where we've begun blocking certain patterns at the API level. ●

Then there's follow-up, according to Bashir. "It's not so much the ROI metrics you present to executive peers per se. It's the act of updating them and keeping the PIM program on their minds."

He recalls that "much of the first year was taken up with communicating and obtaining buy-in for the program charter with stakeholders within various business units."

The same aspiration should apply post-launch, Bashir says. "I would update directors and VPs regularly. Let them know what you've done and what you plan to do before the next time you meet with them."

Miller suggests two additional qualitative approaches. One is anecdotal: "Tie improvements to breaches in the past." The other is to "tie security management to enablement. Security allows you to share more information, a part of revenue-generating activities. You can offer a solution that you previously couldn't because of security. Now, security is part of driving revenue"—to the point that "business metrics can be security metrics." ●

MICHELE KRIEGMAN, *CISSP, is a New Jersey-based technology program professional specializing in IT security and data privacy strategy.*

RETURN TO CONTENTS

(ISC)² | INSPIRING A SAFE AND SECURE CYBER WORLD®

# VULNERABILITY *Central*

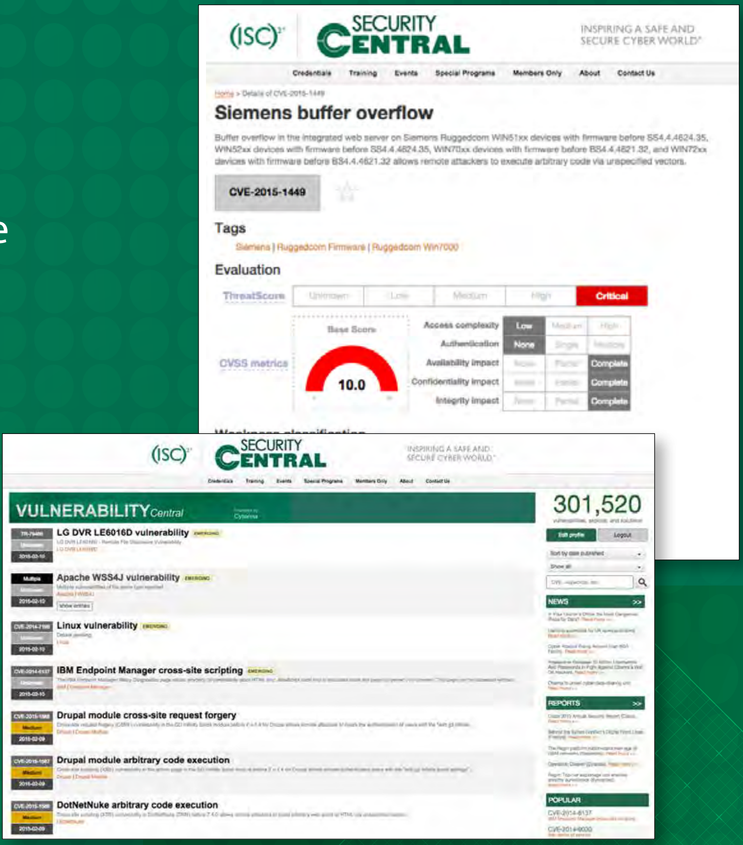
## Start tracking the vulnerabilities keeping you up at night.

Get Started

vulnerability.isc2.org

This exclusive, members-only resource researches and tracks vulnerabilities using proprietary, state-of-the-art algorithms to aggregate, categorize, and prioritize vulnerabilities affecting tens of thousands of products.

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



Siemens buffer overflow

Buffer overflow in the integrated web server on Siemens Ruggedcom WIN51xx devices with firmware before SS4.4.4624.35, WIN52xx devices with firmware before SS4.4.4624.35, WIN70xx devices with firmware before BS4.4.4621.32, and WIN72xx devices with firmware before BS4.4.4621.32 allows remote attackers to execute arbitrary code via unspecified vectors.

CVE-2015-1449

Tags

Siemens | Ruggedcom Firmware | Ruggedcom Win7000

Evaluation

ThreatScore: Unknown | Low | Medium | High | **Critical**

CVSS metrics — Base Score 10.0

| | | | |
|---|---|---|---|
| Access complexity | **Low** | Medium | High |
| Authentication | **None** | Single | Multiple |
| Availability impact | None | Partial | **Complete** |
| Confidentiality impact | None | Partial | **Complete** |
| Integrity impact | None | Partial | **Complete** |

VULNERABILITY *Central*

301,520 vulnerabilities, exploits, and solutions

- LG DVR LE6016D vulnerability — EMERGING — Unknown — 2015-02-10
- Apache WSS4J vulnerability — EMERGING — Multiple — Unknown — 2015-02-10
- Linux vulnerability — EMERGING — Unknown — 2015-02-10
- IBM Endpoint Manager cross-site scripting — EMERGING — Unknown — 2015-02-10
- Drupal module cross-site request forgery — Medium — 2015-02-09
- Drupal module arbitrary code execution — Medium — 2015-02-09
- DotNetNuke arbitrary code execution — Medium — 2015-02-09

*No new account is required to use Vulnerability Central and it's free to members, just login with your (ISC)² member account.*

# THWARTING THE THREAT WITHIN

## THE MOST SIGNIFICANT DANGER TO A COMPANY'S INFORMATION INFRASTRUCTURE MAY COME FROM ITS OWN STAFF

BY **CRYSTAL BEDELL**

ILLUSTRATION BY ©ENRICO VARRASSO

**WHEN IT COMES TO CRIME**, the "inside job" traditionally has been associated with stock trading and banking. The most recent dramatic example was the economic collapse of 2008. However, as the information security field has expanded dramatically, so does the potential for the leveraging of a system's vulnerabilities by those closest to them.

RETURN TO CONTENTS

The technologies themselves are colluding to increase those vulnerabilities. Mobile devices have transformed the way we work. We work in fast but short bursts, shooting off an email while in line at the grocery store or reviewing a document before boarding a plane. Thanks to the cloud, sharing data is as easy as a couple of finger touches or a drag-and-drop. Data changes hands quickly and many times throughout the day. As data becomes more accessible, the challenge of protecting it, especially from those who know it best, has grown exponentially.

Internal threats, says Daniel Redding, information systems security engineer for Virginia-based Saint Security Services LLC, actually haven't changed much over the years, despite advances in technology.

"Six years ago, everyone still had cameras on flip phones, and now we're carrying technology straight out of a Bond movie," he says. "I can back up gigs of video offsite with the blink of an eye without any real stress to myself."

> **"A lot of companies don't have a sense of their crown jewels—what their sensitive data is, where that data resides, and what are they doing to protect that data."**
>
> *—DAVE ROATH, IT risk and security leader, PricewaterhouseCoopers*

Ben Rothke, information security manager at a major hospitality firm, puts it this way: "The challenge is there's so much inherent data sharing going on, and it's very difficult to work around it. We're swapping data left and right through all these systems. There are vast amounts going around, and that adds to the challenge."

To complicate matters further, insiders have knowledge about sensitive data that companies themselves do not. To turn Aristotle's maxim on its head, the individual parts are greater, or in this case, more knowledgeable, than the whole.

"A lot of companies don't have a sense of their crown jewels—what their sensitive data is, where that data resides, and what are they doing to protect that data," acknowledges Dave Roath, IT risk and security leader for PricewaterhouseCoopers in New York. "Insiders that have access to systems are a threat to all of that because they may know where the data resides, what the data is, and what the company is doing or not doing to protect it."

Internal threats can be accidental or malicious. "The reality is, both risks exist. Whether unintentional or intentional, it's hard to say which is more significant. I'd say both," says Roath.

## UNINTENDED THREATS AND UNINTENDED CONSEQUENCES

"The reality is they're both dangerous," Rothke agrees, "but they're both very different." While the damage caused by intentional insider threats can be significant, they occur less frequently. "The unintentional insider threat—that's happening thousands of times throughout corporate America, and there are a lot of things firms can do to deal with those. Policies, processes and the like can go a long way."

Saint Security's Redding also sees the unintentional threat as a ubiquitous danger. "We want to be friendly to each other. We want to hold the door for each other. If we hold the door for the wrong person, we become an insider threat. Those are more common but also more easily preventable."

A common example of unintentional insider threats is users falling victim to phishing attacks. According to PricewaterhouseCoopers' Roath, phishing averages up to a 30 percent success rate, meaning that 30 percent of users who receive a phishing email will click on a link that sends them to a malicious Website or submit personal information.

"It's very much an issue in the sense that it is so easy to create an email that looks and feels like it's coming from the company, and it's really, really scary. We have had clients hire us to do phishing attempts, and they click on the links themselves," Roath says. "You're only really as strong as your weakest link, and when there are so many weak links out there, it's really a significant challenge."

Georgia Weidman, founder and CEO of Bulb Security LLC in Austin, Texas, also asserts that the unintentional insider threat is the bigger threat.

RETURN TO CONTENTS

"It's easy to forget that 1) most people don't know much about security, and 2) they don't even care. I think that, just in general, most people still aren't thinking about security, and security pros have a tendency to forget that," she says.

## WITH MALICE AFORETHOUGHT—INTENTIONAL THREATS

The same trends that increase the risk of unintentional threats also increase the risk of intentional threats. Dave Roath sees the expansion of the data world providing the doorways for "inside jobs."

"There are more technologies today, and what's happening is a lot of companies have many different technologies, but they don't have the resources and time available to adequately secure all those devices, so, inherently, they have a number of different issues and weaknesses in the environment."

> **"Explain how an attack works and how to stop it both for the enterprise and the family, and you can get people interested and involved."**
>
> *—GEORGIA WEIDMAN, founder and CEO, Bulb Security LLC*

To make matters worse, Roath adds, malicious insiders have more information at their disposal. "There are so many different ways that a disgruntled employee can do damage. There's so much knowledge out there on how to do some of these things, and a lot of it is free—software you can download, videos on how to hack. People in general are becoming more sophisticated on how to do these things because the tools are readily available."

## PREVENTING THE 'ACCIDENTAL' THREAT

The experts we spoke to generally agree that security awareness training plays a key role in preventing insider threats, but training must go beyond the obligatory and often-ignored in-house Web-based training.

"Reading and taking a test is not going to help anything, but it can be more effective if you can make it interesting," Bulb Security's Weidman advises. "Explain how an attack works and how to stop it both for the enterprise and the family, and you can get people interested and involved. It won't solve every problem; everyone will make a mistake at some point, but at least some awareness will help."

Daniel Redding encourages dynamic training that focuses on users' security responsibilities. "Having a security professional within the organization conduct the training and talk about users' responsibilities in a slightly more interesting manner can help, especially if people can ask questions and be part of the conversation," he explains. "If they feel a sense of ownership, then they are less likely to become apathetic."

Beyond security awareness training, Redding urges security professionals to be an ongoing presence. This may mean sending a mass email, for example, to warn users that spear phishing emails are being received internally and to advise them on what to look for in such an email, or simply letting users know how things are going in the security department.

"Not only are you reinforcing what you've equipped them with in training, but you're also making sure they know that you are responsive and accessible," he says. The key is to remind users about their training so that it's at the forefront of their minds but not to be so overbearing as to be ignored.

## OUTWITTING THE DELIBERATE THREAT

Security awareness training helps prevent unintentional insider threats, but it doesn't necessarily help prevent intentional threats. This is where technology comes in.

"But the main reason that intentional threats can be so dangerous is because a lot of the time, they are committed by people with an intimate knowledge of the system," Redding says, "who have a high level of expertise on the system and how it works."

For example, some data-loss-prevention solutions can mask data and prevent the copying of data. "But the biggest thing is if a person can turn that solution off, it doesn't matter what system you have in place. If they have that level of knowledge of the system, it comes down to making sure they can't do it alone and

RETURN TO CONTENTS

that you can track them and find out about it."

This means practicing job rotation and separation of duties.

"With separation of duties, you want to make sure that if your admins are doing something that can be tracked, they can't go in and delete the audit logs," Redding explains. "And you want to force collusion. If a user is going to do something bad, you want it to be at least two or three people who need to actively and knowingly do something wrong. Most people are going to be content and complacent in their job. They don't want to do something to jeopardize their jobs."

## KNOW YOUR RISK LEVEL

Prevention measures don't end there.

Pricewaterhouse's Roath stressed the need to comprehend the company's risk.

"Understand the company's security maturity today in terms of controls, where the company wants to get to, and how secure they need to make systems and controls," he says. "Understand where sensitive data is, what the sensitive data is, where it resides and what the company is doing to protect the data to the level they want to reach in terms of maturity."

Ben Rothke sums it up: "It's a fine line, because we trust our users and want to enable them, yet we need to control and protect the data. Every organization needs to understand what their risk appetite is. Once they determine that, they can put the right controls in place." ●

CRYSTAL BEDELL *is a contributor to* InfoSecurity Professional *who lives and works near Spokane, Wash.*

RETURN TO CONTENTS

# RELAX

## ACTIVITIES FOCUSED ON 'NEURO-HACKING' HELP MANAGE STRESS SO YOU CAN BE MORE PLEASANT—AND PRODUCTIVE

BY **ANNE SAITA**

**STRESS IS A** natural reaction we all experience, resulting from a range of daily demands and occasional confrontations or life-changing events like a death or divorce. Information security can be a particularly taxing profession given the frustrations associated with fluctuating, often unrealistic, expectations.

Even normal challenges—responding to event logs or tackling child care—lead to pent-up stress (and the mental and physical woes it creates) if not handled in a meaningful, sustainable way.

This is where neuro-hacking comes in, a broad term for manipulating brain activity. Many of us experience this when we drink caffeine for a quick mental boost or consume alcohol to settle down or build up our nerve.

RETURN TO CONTENTS

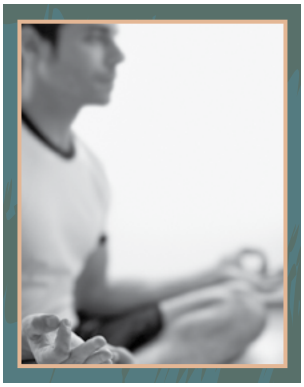
A growing number of professionals are turning to other solutions to re-engineer their thinking. Meditation, yoga therapy, tai chi, and qigong are just a few practices information security professionals use to respond better in both typical and tough situations.

These also are practices endorsed by longtime security expert Mike Rothman and (ISC)² board member Jennifer Minella in their popular RSA and Security Congress presentation, "Neuro-Hacking 101: Taming Your Inner Curmudgeon."

> **"I find mornings are the best time to calm my mind and get into a meditative state and develop a sense of gratitude heading into the day."**
>
> *—DAVID SHEARER, (ISC)² executive director*

The techniques have been embraced by information security practitioners worldwide, including (ISC)² Executive Director David Shearer, who incorporates tai chi, yoga, and qigong into daily living. "I find mornings are the best time to calm my mind and get into a meditative state and develop a sense of gratitude heading into the day," he said during the presentations.

The key to creating a meaningful practice is commitment. Start slowly, build a practice, and then maintain a better state of wellness. Remember, too, that proper nutrition is essential to a healthier lifestyle. Through practice in the meditative arts, you should achieve a better, more balanced you.



Photographs ©iStock

## MEDITATION

WHAT:

The practice that appears to be the easiest is actually difficult for a lot of people. That's because it takes a great deal of mental and physical energy to clear the mind and focus 100 percent of your attention on a single area. When we're conditioned to be thinking ahead, it can be difficult to concentrate on the here and now.

If done correctly, mediation can move brain activity from the stress-prone right frontal lobe to the calmer left side of the lobe, thereby moving you closer to tranquility.

RECOMMENDATIONS:

Among the tips for beginners, according to various meditation enthusiasts:

- Pick a specific room with a calming atmosphere (adding candles, removing distracting piles) to meditate regularly. Put up a "Do Not Disturb" sign, if need be.
- Stretch prior so you can hold your body still during the duration of the meditation session.
- Take deep breaths to slow the heartbeat and help focus in the "now."
- Become more aware of your body, including internal organs, as you move into a deeper state.
- Give meditation time to work.
- End a session with a sense of gratitude.

There are many books, videos and CDs or e-audiobooks you can digest to create a routine that works for you. Among the bestsellers, especially for beginners: 1995's *Wherever You Go, There You Are* by Jon Kabat-Zinn, Ph.D.

PROVEN BENEFITS:

Scientific studies show meditation can reduce stress, anxiety, and depression. Even meditating as little as 10 minutes daily has shown positive results.

## YOGA

WHAT:

The growing popularity of yoga has broadened the scope of this centuries-old Indian form and led to

RETURN TO CONTENTS

criticism over its commercialization (as outlined in the documentary *Yoga, Inc.*) and hybridization (PiYo, anyone?). On the plus side, it's much easier these days to find yoga classes if you prefer group instruction. At its heart, yoga as a discipline uses specific physical, mental, and spiritual techniques to transform body and mind using different techniques.

### RECOMMENDATIONS:

Newbies, unless you are already in great shape, holding those poses is harder than it looks. Many recreational athletes, particularly longtime runners and cyclists, are surprised at their initial inflexibility. Just remember—this isn't a competition, and a good instructor will help you progress at your own pace.

There is also no shortage of videos and guidebooks to help you get into and hold poses to improve your strength and flexibility. Read up on the different varieties to find one that fits your own needs. Concentrate on areas where you tend to hold tension, such as neck, shoulders, and back, to help reduce stress at work.

### PROVEN BENEFITS:

Studies show decreased stress and tension, increased flexibility, muscle strength, balance, and decreased levels of the hormone cortisol associated with stress and overeating. So put away the junk food and get out that yoga mat.

## TAI CHI

### WHAT:

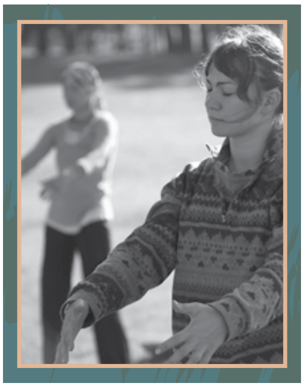
This ancient Chinese discipline relaxes body and mind using prescribed movements to remove stress from the body, both general and specific areas. Mental relaxation is achieved through movements and intentions to enhance our chi, the life force within each of us. Martial arts-like movements differ by four styles: Yang, Chen, Wu, and Hao. It's possible to incorporate more than one style into a practice.

### RECOMMENDATIONS:

Some moves can be complicated, and you should be sure to get down the correct movement and alignment of basic moves before moving into more difficult ones—despite how easy they appear from a distance. There are plenty of online resources to get you started.

### BENEFITS:

Tai chi is said to restore nervous systems to their baselines and create calmness. It is especially popular with those who prefer low-impact exercise and has been shown to promote better sleeping patterns. Lack of sleep, over time, can contribute to increased stress in the body.



## QIGONG

### WHAT:

Related but different from tai chi, qigong also incorporates mediation, body alignment, and martial arts—but to awaken our life energy and discover our true nature through various methodologies. It uses both active and passive techniques to experience a higher realm of being.

### RECOMMENDATIONS:

Because qigong can be done lying down, sitting, or standing, the discipline is attractive to those with physical limitations. Instructors fluent in the format may be more difficult to find, and beware of those making medical claims that haven't been substantiated by scientific study.

### BENEFITS:

Qigong has been known to help people alleviate physical and emotional pain and reduce blood pressure, though much of the evidence to date has been anecdotal. ●

ANNE SAITA *is editor-in-chief of* InfoSecurity Professional *magazine.*

RETURN TO CONTENTS

# STRESSED? CONSIDER VOLUNTEERING!

BY **JULIE PEELER**

ONE OF THE most rewarding outcomes of volunteering is witnessing its positive impact on a community. Almost daily, we at the (ISC)² Foundation experience such fulfillment because of our member volunteers.

If those volunteers seem a little more upbeat and less downtrodden, it may be because scientific research has long shown volunteers derive fulfillment from enriching the lives of others, resulting in lower levels of stress, depression, and even helping to foster a deeper sense of purpose.

Through the (ISC)² Foundation, there are a number of ways for members to help. Among the most popular is becoming an ambassador for the Safe and Secure Online program. With training, members introduce children to the concept of online safety by delivering an interactive presentation to schools and community organizations.

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

Volunteers leave with a sense of satisfaction, knowing they have played a small role in helping keep schools and families a little safer from cyber intrusions and even real-life threats, like bullying. Volunteers can also assist current and future information security practitioners by completing the bi-annual (ISC)² Global Information Security Workforce Study (GISWS) survey. The Study, which just wrapped up for this cycle, is a respected benchmark referenced by governments, employers, professionals, and industry stakeholders around the world

Researchers' data analyses provide much-needed insight into current cyber security opportunities and trends in pay scales, skills and training requirements, budgets, career progression, pressures facing the industry, and the future outlook of the industry. The Study would not be possible without the critical input of both (ISC)² members and non-members.

The (ISC)² Foundation also supplies future cybersecurity professionals with scholarships, helping them prepare for careers in this exciting and growing field, while bridging the gap between cybersecurity experts needed and those available to fill the void.

Volunteers can help the (ISC)² Foundation grow the next generation of cybersecurity professionals by spreading the word about the scholarship programs and even helping to evaluate scholarship candidates. You can also bring the popular program to new nations through a financial contribution.

Our foundation is strengthened by the good deeds and participation of our members from around the world. Whether it's serving on a scholarship committee, carving out time to complete a survey or signing up for Safe and Secure Online, we have an opportunity for each of you to broaden your skills base, meet other professionals, help shape the future of the profession, and make the cyber world a little safer.

You might even find that in helping others, you've also helped raise your own spirits, professional network, and resume. So if you feel like you could use a boost, give our staff a call, and discover the many benefits of helping others. ●

(ISC)² FOUNDATION

RETURN TO CONTENTS

5 Minutes With...

# JEFFERSON GUTIERREZ

Jefferson Gutierrez is currently the managing director in charge of the forensics services practice for KPMG in Bogota, Colombia. He's been an (ISC)$^2$ member for the past nine years. EDITED BY **ANNE SAITA**

Q

**When did you know you wanted to have a career in information security?**
Very early into my studies as a systems engineer (computer science) at the Universidad Nacional in Colombia. It was back in 1994, when the Internet was just in diapers in our country. A couple of friends and I had the chance to use some IBM mainframes. The need to understand how these devices worked moved us to explore more and more. Curiosity was driving us.

**How did you get your first break in the information security industry?**
Informally, at the university, I had the chance to learn a lot from very experienced people. The Internet boom and the possibility of interacting with many people in the academic space allowed me to experiment and gave me access to valuable knowledge.

Professionally speaking, it was at KPMG when I joined the Information Protection Privacy practice. I refined my skills, learned about consulting, and got in touch with a huge network of professional people delivering services around the globe to many different clients in several industries.

**What made you specialize in forensics?**
I was offered the opportunity to join the forensics practice some years ago, initially leading the Forensic Technology (FTech) area. Information security and forensic technology are two disciplines that are connected in several ways. So, after several years of practicing pure information security, I took the opportunity to explore this exciting area, which was not so far from my previous background.

**As part of the (ISC)$^2$ Latin American Advisory Council, what do you believe are the top three most challenging technology issues (ISC)$^2$ members face in those countries?**
Cultural issues are, in my opinion, the big ones. There is a tendency to believe that information security incidents happen only to others. Non-financial industries feel that they don't need to invest in information security because they "don't handle other people's money." Additionally, the initiatives on critical infrastructure protection still need more support. I have seen great security initiatives in the biggest economies in the region, mainly in Brazil, but there is still a lot of room for growth and improvement.

Corporations in our countries are subjected to targeted attacks, criminals are infiltrating companies, privacy incidents happen all the time, and we are still looking at the other side of the fence. ●

› **Jefferson Gutierrez** reveals more in our upcoming April 2015 e-newsletter, **INSIGHTS**.

RETURN TO CONTENTS

infosecurity®

EUROPE

• 02-04 June 2015 • Olympia • London •

Securing the
connected enterprise

# Join Europe's biggest free-to-attend information security conference & exhibition

www.infosecurityeurope.com

Collect
**CPE/CPD**
credits

**REGISTER YOUR INTEREST NOW**
www.infosecurityeurope.com

- **98.1%** of 2014 visitors, were satisfied to completely satisfied
- **84.1%** of visitors are very likely to recommend participating in Infosecurity Europe to a colleague
- **96.6%** of 2014 visitors are more than likely to attend in 2015
- **97.2%** of exhibitors were satisfied in 2014 and 80% have already rebooked to participate in 2015
- **£447.5m** of future orders expected to be placed with exhibitors as a direct result of Infosecurity Europe 2014

CELEBRATING 20 YEARS

02-04 JUNE15
OLYMPIALONDONUK

Managed by: infosecurity™ GROUP  Part of: Reed Exhibitions®