

# Info Security

## PROFESSIONAL®

**WINTER 2008**

An (ISC)<sup>2</sup> Digital Publication  
[www.isc2.org](http://www.isc2.org)

The image features two identical photographs of a man in a dark suit standing on a red A-frame ladder in a vast, green mountainous landscape under a cloudy sky. He is holding binoculars to his eyes. The two photos are positioned side-by-side, slightly overlapping, creating a sense of depth and repetition.

**LOOKING BACK,  
LOOKING AHEAD**

CISOs DESCRIBE 2008–09 CHALLENGES

**It's time we  
addressed the holes  
in software development.**



**Don't wait  
for the exam,  
GET CERTIFIED  
NOW!**

**Sign up for the  
Experience Assessment  
(for a limited time)**



Certified Secure Software Lifecycle Professional

Since 2005, more than 226 million records have been breached largely because, as an industry, we've failed to address security during software development. But that's about to change. At (ISC)<sup>2</sup> we've developed a holistic approach to building security across the entire software lifecycle (SLC). Our brand new certification is the only one designed for every SLC stakeholder in your company. And it's going to save millions.

*Education seminars begin in early 2009*

*Exams begin in June 2009*

*Experience Assessments offered now for a limited time.*

*For more info or to register visit [www.isc2.org/csslp](http://www.isc2.org/csslp)*

To view this issue  
online, visit: [www.isc2.infosecpromag.com](http://www.isc2.infosecpromag.com)

## features

### 6 Looking Back, Looking Ahead

CISOs from around the world describe the top information security challenges in 2008, and what they expect in 2009.

BY ANNE TAYLOR

### 10 Info War

Is information warfare a serious threat or simply over-hyped hysteria? Here's what you need to know.

BY JOHN SOAT

### 14 Now Presenting

The thought of giving a presentation often fills one with dread. But that doesn't have to be the case.

BY BRUCE HOARD

## also inside

### 2 Inbox

**Feedback & Suggestions** Readers share their thoughts and suggestions.

### 3 Breaking New Ground

**Executive Letter** From the desk of (ISC)<sup>2</sup>'s Board Chair. BY PATRICIA A. MYERS

### 4 FYI

**Member News** Read up on what (ISC)<sup>2</sup> members worldwide, as well as the organization itself, are doing.

### 5 Events

**Education Opportunities** Upcoming conferences, shows and seminars.

### 17 Your Best Investment

**Career Corner** Advice from a recruitment professional toward furthering your career. BY LEE KUSHNER

### 19 Finding the Right Balance

**Global View** International perspective on the pressures facing today's information security professionals. BY WALMIR FREITAS

### 20 CISSPs Needed in Japan

**Insight** Why new compliance regulations in Japan demand more CISSPs. BY JUNYA HIRAGA

InfoSecurity Professional is published by CXO Media, an IDG company, 492 Old Connecticut Path, Framingham, MA 01701 (phone: 508-935-4796). 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)<sup>2</sup> on the issues discussed as of the date of publication. No part of this document 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)<sup>2</sup>. (ISC)<sup>2</sup>, the (ISC)<sup>2</sup> digital logo and all other (ISC)<sup>2</sup> 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 companies and products mentioned herein may be the trademarks of their respective owners. For subscription information or to change your address, please visit us online at [www.isc2.org](http://www.isc2.org). To order additional copies or obtain permission to reprint materials, please email [infosecproeditor@isc2.org](mailto:infosecproeditor@isc2.org). To request advertising information, please email [tgaron@isc2.org](mailto:tgaron@isc2.org). © 2008 (ISC)<sup>2</sup> Incorporated. All rights reserved.



# inbox

## READER FEEDBACK AND SUGGESTIONS



**First off, I really like** the new magazine and feel like it's a really great value-add to CISSP® membership. I would like to suggest that you expand your conference listings to 12 months. While it's nice to see what's happening in the current quarter, it is generally too late to consider attending. It would be nice to be able to see what's coming up down the road so we could consider attending.

MIKE SPEAS, CISSP  
INFORMATION SECURITY OFFICER  
WINSTON-SALEM, N.C., USA

**(ISC)² responds:** *At the moment, we are limited by the amount of space we have to list events. To find more detailed listings, visit [www.isc2.org/events](http://www.isc2.org/events).*

**I recently achieved** the CISSP credential. Your *InfoSecurity Professional* e-magazine is of great help in getting a global vision of issues related to information security. The best part of the magazine is its content and layout, along with the opportunity to get CPE points. Great work.

Is there a way to speed up the processing of CPEs to reflect on

(ISC)² member login? The present time frame is four weeks.

VENKATA KRISHNA, CISSP  
SENIOR SECURITY CONSULTANT  
BANGALORE, INDIA

**(ISC)² responds:** *Due to circumstances beyond our control, we are unable to shorten CPE processing time. We appreciate your feedback and will do our best to ensure that InfoSecurity Professional continues to be a great resource.*

**Just wanted to comment** on the tremendous work you folks at (ISC)² are doing with the *InfoSecurity Professional* publication. This magazine contains a wealth of valuable content specific to IS professionals and provides real insight into areas we necessarily don't touch everyday but helps furnish the security toolbox. It is well presented and visually welcoming, and provides an incentive to earn CPE credits.

The new "vision" for (ISC)² is certainly coming to fruition. Keep up the great work!

GERARD DUNPHY, CISSP  
SECURITY ANALYST  
ST. JOHN'S, CANADA

## InfoSecurity PROFESSIONAL®

### Management Team

Elise Yacobellis  
Executive Publisher  
727 683-0782 ■ [eyacobellis@isc2.org](mailto:eyacobellis@isc2.org)

Timothy Garon  
Publisher  
508 529-6103 ■ [tgaron@isc2.org](mailto:tgaron@isc2.org)

Marc G. Thompson  
Associate Publisher  
703 637-4408 ■ [mthompson@isc2.org](mailto:mthompson@isc2.org)

Amanda D'Alessandro  
Communications Coordinator  
727 785-0189 x242  
[adalessandro@isc2.org](mailto:adalessandro@isc2.org)

Marcia Thorpe  
Senior Manager of Member Services  
727 785-0189 x219  
[mthorpe@isc2.org](mailto:mthorpe@isc2.org)

### Sales Team

Paul Moschella  
Regional Sales Manager  
New England and Canada  
781 769-8950 ■ [pmoschella@isc2.org](mailto:pmoschella@isc2.org)

Edward Marecki  
Regional Sales Manager  
U.S. East Coast and Europe  
401 351-0274 ■ [emarecki@isc2.org](mailto:emarecki@isc2.org)

Christa Collins  
Regional Sales Manager  
U.S. Southeast and Midwest  
352 563-5264 ■ [ccollins@isc2.org](mailto:ccollins@isc2.org)

Gordon Hunt  
Regional Sales Manager  
U.S. West Coast and Asia  
949 366-3192 ■ [ghunt@isc2.org](mailto:ghunt@isc2.org)

Jennifer Hunt  
Events Sales Manager  
781 685-4667 ■ [jhunt@isc2.org](mailto:jhunt@isc2.org)

### CXO Media Team

Matt Avery  
Vice President, Custom Solutions Group

Amy Freeman  
Project Manager  
[afreeman@isc2.org](mailto:afreeman@isc2.org)

Anne Taylor  
Managing Editor  
[ataylor@isc2.org](mailto:ataylor@isc2.org)

Mary Lester  
Executive Director, Art and Design

**CSO**  
Custom Solutions Group

### ADVERTISER INDEX

Capella University.....p. 16  
ISACA..... C 3  
(ISC)²..... C 2, p.18, C 4  
Microsoft Corp.....p. 13

For information about advertising in this publication, please contact Tim Garon at [tgaron@isc2.org](mailto:tgaron@isc2.org).

## A Year of Milestones

(ISC)<sup>2</sup> COVERED SIGNIFICANT GROUND IN 2008  
AND IS READY FOR A SUCCESSFUL NEW YEAR.

AS WE PREPARE TO LEAVE a tumultuous 2008 behind us and turn the corner on 2009, it's appropriate to reflect on this year's milestones and significant accomplishments, for both (ISC)<sup>2</sup> and the profession as a whole.

We launched a new credential geared toward software lifecycle professionals. The Certified Secure Software Lifecycle Professional (CSSLP<sup>cm</sup>) is an important step for (ISC)<sup>2</sup> because, in addition to addressing an area long in need of attention, it strengthens our position as the premier provider of certifications. In the next three to five years, we plan to continue broadening our credential offerings while ensuring our core certifications, e.g. the CISSP, SSCP, CAP, etc., continue to command the highest levels of respect.

Another big step for us has been the redesign of our Website, which now sports a contemporary look and feel. Its enhanced functionality and new areas of communication will help us better serve our members and those aspiring to hold one of our credentials. (As a byproduct, we also got the database improvements we've needed for so long.) We welcome your comments, feedback and suggestions—which you can now send to us via the Website.

Speaking of communication, we're very pleased with the overwhelming response to the Cyber Exchange contest. Thank you to all who generously shared their cyber security entries and resources

with the entire (ISC)<sup>2</sup> community, and congratulations to the contest winners! (You can read more about them on page 4.)

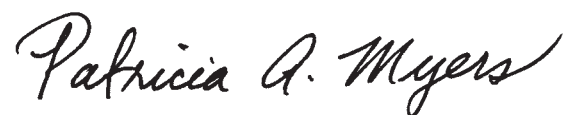
2008 also marked the launch of this magazine. We greatly appreciate the article suggestions, content-related feedback and general comments that have been, and continue to be, so critical to making this

publication successful—and useful—to you in your work. Your ideas and valuable critiques can be sent via email to [infosecproeditor@isc2.org](mailto:infosecproeditor@isc2.org).

You may not be aware of our history, but 2009 is (ISC)<sup>2</sup>'s 20th anniversary. Throughout the year, we will celebrate this momentous occasion at our member receptions worldwide, with special articles in this magazine, and by recognizing the people who have made us the largest certifying body of information security professionals in the world.

Thank you for being a part of (ISC)<sup>2</sup>'s past, present and future.

Best regards,



Patricia A. Myers  
CISSP-ISSMP  
Board Chair, (ISC)<sup>2</sup> Board of Directors





(ISC)<sup>2</sup>  
MEMBER  
NEWS



Hord Tipton, executive director of (ISC)<sup>2</sup>, pictured in the center, poses with the GISLA winners. From left to right, they are: Michael Williams, Adair Martinez, Pam Rusk and Steven Busch.

## GISLA Honorees' Accomplishments Applauded

**ON OCT. 7**, (ISC)<sup>2</sup> announced the winners of its fifth annual Government Information Security Leadership Awards. The 2008 honorees are:

- **Non-Managerial IT Security Professional Pam Rusk**, CISSP, information systems security manager for the Federal Aviation Administration's Office of Regions and Center Operations.
- **Senior Non-IT Security Manager Michael Williams**, executive director of information technology and chief information officer/director of the Information Technology

Customer Service Organization of the Defense Contract Management Agency.

- **Senior IT Security Manager Adair Martinez**, CISSP, PMP, deputy assistant secretary for information protection and risk management at the Department of Veterans Affairs.
- **Federal Contractor IT Security Professional Steven Busch**, senior managing consultant with IBM Business Consulting Services.

You can read more about the honorees at <http://www.isc2.org/PressReleaseDetails.aspx?id=2372>.

## Cyber Exchange Sees Flurry of Uploads

**HUNDREDS OF** (ISC)<sup>2</sup> members have uploaded cyber safety-related materials to the new Cyber Exchange. Based on the most downloads, our contest winners and their submissions are:

- **Rohit Goel**, "Evolution of Information Security"
- **Veera Subrahmanya Kumar Polisetty**, "Data Security in Public Places"
- **Aaron Marco**, "5 Minute All Employee Security Education"
- **K. Rudolph**, "Protect Data on USB Devices"
- **Maurice Stebila**, "Information Protection Survivor Awareness"

Thanks to everyone who submitted resources. These valuable materials will remain available for download by the general public to learn, teach or promote cyber security awareness.

# Asia-Pacific Leaders Recognized for Efforts

**ON OCT. 28**, (ISC)<sup>2</sup> celebrated the second annual Asia-Pacific Information Security Leadership Achievements (ISLAs), in which 15 honorees were recognized at a ceremony in Seoul. In particular, four workforce initiatives, led by the award honorees, were showcased:



**Senior Non-IT Security Professional**  
**Jeong Sik Choi**, CEO and publisher, INFOTHE Co., Ltd.



**Senior IT Security Professional**  
**Dr. Soojung Shin**, executive vice president, Infosec Co., Ltd.

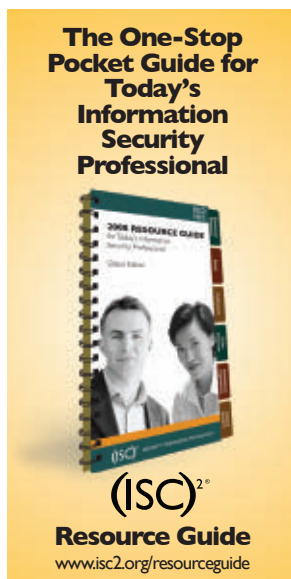


**IT Security Practitioner**  
**Frank Law**, CISSP, senior inspector, Hong Kong Police Force.



**IT Security Practitioner**  
**Wansuck Yi**, director, IT Service Protection Team, Korea Information Security Agency.

For a detailed list of all ISLA honorees, please visit:  
<http://www.isc2.org/PressReleaseDetails.aspx?id=2644>



## Get Thee to the Web

**MAKE SURE** to check out the revamped (ISC)<sup>2</sup> Web-site. You can find all kinds of resources and chat in the forums. Please send your feedback to [webmaster@isc2.org](mailto:webmaster@isc2.org).

**Don't forget  
to take the quiz  
and earn CPEs:**

<http://tinyurl.com/55pr58>

## Upcoming Events

### SecureAtlanta

Jan. 21, 2009  
Atlanta, GA  
[www.isc2.org/events](http://www.isc2.org/events)

### Cyber Warfare 2009

Jan. 28-29, 2009  
London, UK  
[www.iqpc.com/showevent.aspx?id=148734](http://www.iqpc.com/showevent.aspx?id=148734)

### SecureSan Jose

Feb. 3, 2009  
San Jose, CA  
[www.isc2.org/events](http://www.isc2.org/events)

### SecureSeattle

Feb. 5, 2009  
Seattle, WA  
[www.isc2.org/events](http://www.isc2.org/events)

### Black Hat DC 2009

Feb. 16-19, 2009  
Arlington, VA  
[www.blackhat.com](http://www.blackhat.com)

### SC Magazine Conference: Data on the Move

Feb. 24, 2009  
London, UK  
[www.dataonthemoveconference.com](http://www.dataonthemoveconference.com)

### CSO Perspectives

March 1-3, 2009  
Clearwater, FL  
[www.csoperspectives.com](http://www.csoperspectives.com)

### SecureLondon

March 3, 2009  
London, UK  
[www.isc2.org/events](http://www.isc2.org/events)

### Infosec World 2009

March 7-13, 2009  
Orlando, FL  
[www.misti.com/default.asp?page=65&Return=70&ProductID=5539](http://www.misti.com/default.asp?page=65&Return=70&ProductID=5539)

### IAPP Privacy Summit 2009

March 11-13, 2009  
[www.privacysummit.org](http://www.privacysummit.org)

### 2nd ACM Conference on Wireless Network Security

March 16-18, 2009  
Zurich, Switzerland  
[www.sigsac.org/wisec/wisec2009/](http://www.sigsac.org/wisec/wisec2009/)

### Infosecurity Belgium

March 25-26, 2009  
Brussels, Belgium  
[www.infosecurity.be](http://www.infosecurity.be)

PHOTO BY GREG PEASE







## [Cover Story]

# LOOKING BACK, LOOKING AHEAD

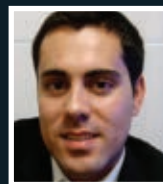
**SEVERAL CISOs SHARE THEIR  
BIGGEST INFORMATION SECURITY  
CHALLENGES THIS YEAR AND  
THEIR EXPECTATIONS FOR 2009.**

**W**e asked three chief information security officers (CISOs) from around the globe what their most significant security challenges were this past year. Though their answers varied—due to industry, company maturity or organization size—their concerns are similar. They include identifying vulnerabilities, managing compliance, ensuring adequate risk management and demonstrating value to the business.

“All these challenges resonate with me,” says Patricia Myers, (ISC)<sup>2</sup> Board Chair. “They’re perennial challenges. When I started ... in the mid-1980s, I was told, ‘You have 18 months to create the information security program.’ It



**MELODI GATES** is the chief information security officer at Qwest Communications, a leading provider of voice, video and data services around the world. She is based in Denver, Colorado, USA.



**NELSON NOVAES NETO**, CISSP, is the chief information security officer of UOL (formerly Universo Online SA), the largest Brazilian Internet service provider. He is based in São Paulo.



**SEKAR SETHURAMAN**, CISSP, is the head of IT security in Greater Asia for LexisNexis, a leading global provider of business information solutions and risk and compliance assessment. He is based in Chennai, India.

was very entrepreneurial. [The] budget hadn't been set. We had five people dedicated to it.

"But compliance regulations are much more granular today ... IT departments have more people and different teams—disaster recovery, business continuity, risk management. Technology has not helped us, but rather given us challenges to stay on track. We'd like to draw a line under these issues and say they're fixed, but there's always a new twist and remediation to do."

The 2008 Global State of Information Security study\* supports this recurring challenges theme. The study is in its eleventh year and—as has been the

case for the past decade—when asked to identify the most critical business issues or factors necessitating spending on information security, the majority of respondents point first to business continuity/disaster recovery, followed closely by internal policy and regulatory compliance.

"These are ongoing challenges because as companies grow, change, merge, acquire, they have to reconsider the security impacts of these changes," says study co-author Mark Lobel, a principal with PricewaterhouseCoopers (PwC). "For example, business continuity has been a factor all along, but it took a huge jump in priority after Sept. 11."

These findings and correlations are subtly echoed in the CISO discussions. Ultimately, though, our three CISOs express optimism about overcoming these challenges—and offer advice based on their own experiences.

## 2008: LOOKING BACK

The need to provide value to the business is a unifying theme among the group. For example, Nelson Novaes Neto, CISO at UOL in Brazil, says ensuring adequate risk management and security metrics management is a challenge his organization faced this past year. He adds that it's clear he needs to work closely with the business to meet organizational objectives.

With regard to risk management, Neto says, "The main challenge for the security area is to guarantee that organizational decisions are supported by a risk management process. But to make that efficient, it is necessary to avoid conflicts between the process and the organization's objectives.

"Security decisions must support business units in a strategic way so that product will have added value," he continues. "Security cannot become an obstacle for the business, impacting the investment and time-to-market. Competition in the global markets demands prompt and transparent development processes."

Similarly, with security metrics management, Neto must justify investments—"a hard task," he says. "We need metrics to be tangible, but to get this, we need to adapt processes and technology in a manner that data is turned into information and the information is well managed."

Sekar Sethuraman, IT security head for Greater Asia with LexisNexis in India, adds: "There is an enhanced need to demonstrate our abilities to significantly add business value." Sethuraman says he must "smoothly integrate the information security program with a number of enterprise initiatives: legal and regulatory compliance; internal business priorities and customer expectations; and enterprise architecture."

Sethuraman's challenges correlate with India's immense growth trajectory in security, and its shift to focusing on information security strategies as they relate to the business—taking a proactive as opposed to reactive approach.

"Companies in India have reported strong, consistent, double-digit gains across virtually every security domain and have taken a strategic approach to security," says PwC's Lobel. "Security efforts of Indian organizations have surpassed those of companies in the United States and we expect this trend to continue given that so many Indian survey respondents expect security spending to increase over the next 12 months."

That's not to diminish the efforts of information security professionals worldwide. Survey respondents across all industries, sectors, countries, business models and company sizes report growth in implementing new security technologies. And 74 percent say that information security spending will either increase or stay the same over the next 12 months.

However, the study found that organizations still struggle with security processes. Lobel says there appears to be misalignment with management's view of security, causing many organizations to fail to capture the full value of their spending.

"Information has become the new currency of business—its portability and accessibility are crucial components of a collaborative, interconnected business landscape," he says. "Organizations need to be prepared to address data security issues, have the proper tools in place, and understand how to use them effectively."

Complicit in this, too, is the need to not just recognize, but also understand the business perspective. Melodi Gates, CISO at Denver-based Qwest Communications, suggests spending "just as much, and preferably more, of your energy on building relationships with key stakeholders across your enterprise than you spend learning the bits and bytes of the latest technical toy. If you have the right relationships with your business, you can always find a means to accomplish your objectives, and learning those technical means together gives you more credibility with those stakeholders than dictating 'The Answer.'"

Neto adds, "We need to be multidisciplinary professionals and great negotiators. We cannot communicate using only technological language; we need to walk alongside the business, with an excellent marketing strategy to sell security. We need to sell security as value-added, positive and strategic; we need to break the paradigm that security generates costs."

**74%**  
say that  
information  
security  
spending will  
increase or  
stay the same  
over the next  
12 months

SOURCE: 2008 Global State of Information Security Study

## TECHNICAL ISSUES

Outside of business-IT challenges, there are day-to-day technical issues that must be addressed. For example, Gates reports an ongoing need to deal with vulnerabilities: "Keeping up with the high traffic in vulnerability disclosures is a perennial challenge and an important part of our program since we focus on proactively identifying and remediating risks."

Behind the high volume of vulnerabilities, Gates says, is the security research community's continued growth and focus on discovering and disclosing them. "That's generally a good thing when the disclosures are made responsibly, although sadly, that was not always the case in 2008," she says. "Regardless, to run an effective information security program, we had to react quickly to every one of those disclosures and that took time."

Gates' other challenges—balancing resources among programs and obligations, and evolving identity management functions—are the result of Qwest's growing information security program. Her organization is addressing these issues by focusing on "people, process, policy and technology."

Her mantra is strikingly similar to that of Sethuraman. "People are the most important component to the success of an information security program," he says. When establishing an information security strategy, he suggests a sound, solid framework driven by business priorities. And let the business know that its priorities are of critical importance. "If you can establish this reputation, you will soon see greater management commitment and support for the information security program that is so very necessary for its success."

This is the approach he is taking as his organization shifts from meeting internal standards to achieving international ones, such as ISO 27001 and 27002—a significant challenge that he says may be unique to his region.

"Greater levels of outsourcing to India over the last many years and the general practices of various companies have resulted in the general expectation for ISO 27001-compliant systems," says Sethuraman. In addition, he must meet these standards while facing "business pressures for greater cost-effectiveness and for ensuring the global standards are quickly established, even in new centers."

As to information security challenges specific to Brazil, Neto says the most prominent one is defining Internet usage regulations. "Industry and Internet experts in Brazil are discussing with the Brazilian government and other authorities the proposal of self-regulation and a law project for cybernetic crime," he says. "This is a process that may consequently incriminate the Internet service providers and may disturb privacy and free will toward Internet usage in Brazil. It is a challenge that should be implemented in desirable directions, according to authorities' concurrence and with the agreement of an organized civil society and industry."

## LOOKING AHEAD: 2009

Our three CISOs anticipate a variety of challenges in the new calendar year:

Neto: "A big challenge will be to integrate business con-

tinuity management in all organizational sectors, following market best practices. Another huge challenge is working on organizational security awareness, including new policies and providing security training for all development fields."

Sethuraman: "One issue will be identifying new and more cost-effective ways to carry out our information security program. Another is integrating the information security program with other enterprise initiatives in a more efficient manner."

Gates: "In 2009, we expect to focus even more on content-based security through our information governance program. The business requirements vary widely and the technical solutions, especially in data leakage prevention, are still maturing—a familiar theme. And there's always a new threat to consider since, ultimately, information security is an arms race—but that's also what makes it challenging and fun."

There's also the need to consider the economy and its effects on information security strategy. (ISC)<sup>2</sup> Board Chair Myers thinks the single biggest challenge will be keeping "security in a steady state in this economy of reduced budgets. Even when you buy security technology or tools, there are still ongoing maintenance and monitoring costs."

Gates concurs. "I expect to see a continued need for vigilance against malicious software and attacks like spear-phishing that are rooted in fraud, along with the ever-present insider threat," she says. "We always seek to maximize the efficiencies of our toolsets, but I also expect to spend even more time on leveraging current solutions to minimize costs."

Cost-effectiveness is key, and security professionals should seek "innovative ways to find new value," says Sethuraman.

However, Neto cautions, "We've got to be ready for a technological investment decision to be cancelled and, furthermore, not let it affect organizational security. Security professionals, in my opinion, must be prepared for any change that may occur in their plans. Our market is in constant mutation and we need to manage security for any situation. For example, your company may acquire another one and you will have to adequately conduct the process of risk management during the joint venture, but also we need to preserve security in this process. We need to be resilient professionals." (ISC)

*Anne Taylor is the managing editor of InfoSecurity Professional magazine.*

\*The study was conducted by PricewaterhouseCoopers, in conjunction with CIO and CSO magazines, and surveyed more than 7,000 information technology and security executives in 119 countries from March to June 2008.



**52%**  
of organizations involve  
both IT and  
business  
leaders in  
addressing  
information  
security issues

SOURCE: 2008 Global State  
of Information Security Study



# info war

John Soat investigates whether information warfare is a serious threat or over-hyped hysteria. Cybersecurity experts offer two words of advice: **BE PREPARED.**

**The headlines last August sounded chillingly familiar, an arctic blast of** Cold War anxiety: “Russia Invades Georgia.” But while its politics seemed like déjà vu, the conflict offered an extensive look at an emerging—and unsettling—form of combat in an increasingly online and interconnected world: information warfare.

Georgia’s cyber infrastructure was under attack even before Russian tanks began rolling in. For several days, extensive denial-of-service (DoS) attacks rendered government Websites useless. Some observers downplayed the significance of the online attacks, ascribing them to “hacktivists”—savvy amateurs bent on inserting themselves into the fight. Russian officials have denied direct participation in the DoS attacks against Georgia, and no one is certain exactly where they originated or who was responsible.

Still, the U.S. government and its defense agencies are taking information warfare seriously. Several cyber warfare programs have been established, including the Air Force’s Cyber Command unit. In January 2008, President George W. Bush approved a new interagency cybersecurity effort to be run by the Department of Homeland Security, and a Silicon Valley-based entrepreneur was tapped to head it.

How seriously should information security professionals take the threat of information warfare? More seriously than they do now, according to many cybersecurity experts.

## When, Not If

In their efforts to address the forest of security problems, information security professionals may be ignoring a few significant trees. In the (ISC)<sup>2</sup> 2008 Global Information Security Workforce Study, almost half (48 percent) of (ISC)<sup>2</sup> members say they are mildly or not at all concerned about the security threat posed by terrorists, and 38 percent say the same thing about organized crime.

“It really is a matter of semantics,” says Andre DiMino, co-founder and director of the Shadowserver Foundation, a self-funded, non-profit

organization composed of security professionals who track and report on the progress of malware, botnet activity and electronic fraud. DiMino points out that one of the most important elements of information warfare is the botnet. Botnets are worldwide networks of compromised computers; those computers currently number in the millions—and that figure is growing (see “Battling Botnets,” *InfoSecurity Professional*, Autumn 2008). “The use of a computer in a targeted attack—that’s my definition of cyber warfare,” says DiMino.

Your organization may have already been the





victim of information warfare, or at least an intended victim. Phishing attacks are often used to obtain funds for terrorist organizations, according to watchdog groups. At the same time, certain nation states are interested in obtaining the intellectual property of companies to exploit the technical advances and competitive advantages represented by patented processes and copyrighted algorithms. Internet addresses in China, for example, have been linked to network intrusions in the U.S., including a well-publicized break-in last year into non-military networks at the Pentagon.

So, while most companies aren't likely to suffer coordinated, intense electronic bombardment, information security

professionals can expect to see a steady increase in the number and sophistication of those attacks with which they're already familiar: worms; Trojans; spam; phishing; network intrusions; and data theft.

## Growing Capabilities

Ultimately, when it comes to security concerns, the "who" is less important than the "how."

"The information security professional can't be concerned with who it is that's attacking his or her network," says security consultant Winn Schwartau. "It's all about the capabilities, and capabilities keep going up." With the publication of *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*, he literally wrote the book on info warfare. According to Schwartau, it can be divided into three areas:

► **Class 1:** Personal Information Warfare, where the individual is the target. "We didn't call it identity theft back in the day," Schwartau says.

► **Class 2:** Corporate Information Warfare, or "the rough equivalent of what we used to call industrial espionage," he says.

► **Class 3:** Government Information Warfare. The Russia-Georgia conflict is an example of this. Another example is a similar situation that developed in Estonia last year, where that former Soviet satellite's cyber infrastructure was compromised by DoS attacks over several days after Estonian officials removed a Russian war memorial from the center of the capitol.

Businesses must be aware of all three areas of potential attack. "The information security professional has to understand the complete environment," Schwartau says. That's because, for example, Class 1 information warfare—identity theft—"may be coming from a Class 2 or Class 3 source," he says, making it more dangerous. Guarding against sophisticated phishing or malware attacks places greater emphasis on Web controls and PC security.

Class 2 information warfare involves "patents, copyrights, business deals—that is, the real value of companies," Schwartau says. It can be perpetrated by outsiders through network intrusions, but also by insiders. That's why it's important for information security professionals to work closely with their human resource departments to screen applicants for critical IT positions, including H-1B workers.

Schwartau says it has become increasingly important that all areas of security—HR, cyber security and physical security—are integrated as closely as possible. An example is a disgruntled ex-employee, "the insider that becomes an outsider," as he puts



it. To address that scenario, “part of the HR process should be irrecoverable revocation of all assets,” Schwartau says—including, perhaps especially, electronic assets.

In the U.S., Class 3 info warfare will increasingly involve private companies because they own and operate most of the critical infrastructure used by government and military operations, such as the telecom network or the electric grid. Experts are divided on just how vulnerable that infrastructure is, and how aggressively it’s being probed. There is still speculation that the 2002 power outage on the East Coast resulted from probing of the SCADA systems. While that speculation flirts with hysteria, the lesson is: Be prepared. “If you have a critical



## “Is [info warfare] going to get nastier? Yes, it’s going to get nastier.”

Winn Schwartau, security consultant and author

system on the Internet, chances are it’s going to be knocked,” says Shadowserver’s DiMino.

An important element to consider is the global supply chain. Andrew Colarik, an information security consultant and cybersecurity expert, says information security professionals must factor the possibility of regional information warfare conflicts, like those in Estonia and Georgia, into their business continuity plans. That means having alternatives ready, in terms of logistics and resources, if Internet access to supply chain partners is interrupted.

O. Sami Saydjari, president of the security consulting and research firm Cyber Defense Agency and a former cybersecurity expert with the National Security Agency, says most organizations aren’t taking the cyber warfare threat seriously enough, and one area he points to is outsourcing. Because software coding and maintenance is often sent to other countries, information security professionals have to be aware of the possibility of “contamination in our corporate infrastructure,” or applications that “come back with Trojan horses and back doors that can be exploited later on,” he says.

It’s a sensitive issue politically, but a risk that shouldn’t be ignored. “In a global environment, they’re going to have to put software quality assurance controls in place” to deal with that risk, Saydjari says.

## Cyber Consequences

Cybersecurity experts say DoS attacks—or the threat of them—are used to try to blackmail organizations. They’re also used by criminal organizations to demonstrate prowess. Shadowserver’s DiMino recommends analyzing network infrastructure for the load balancing and redundancy needed to withstand a sustained DoS attack. “We see many sites that don’t have that design built in,” he says.

On a professional level, those involved in information

security, particularly those who work at critical infrastructure organizations, need “more training in the aspect of how to deal with a crisis,” says John Bumgarner, CTO and research director for security technology for the U.S. Cyber Consequences Unit, a non-profit research organization funded by the Department of Homeland Security and other government agencies. This unit advises “the highest levels of government” on cybersecurity issues, Bumgarner says.

Information security professionals “usually respond to events that have already occurred,” he says. The Georgian and Estonian incidents demonstrate that security professionals might benefit from training in how to respond while an attack is taking place. “A lot of agencies do not train that way, do not train for aggressive response,” Bumgarner says.

Various types of info warfare resources are available. The Estonian Ministry of Defence recently posted a document titled “Cyber Security Strategy” on its Website ([mod.gov.ee](http://mod.gov.ee)) that calls for, among other things, “the development and implemen-

tation of international cyber security policies.”

The U.S. Cyber Consequences Unit offers a cybersecurity checklist intended to provide “a comprehensive survey of the steps that corporations and other organizations should take to reduce their vulnerability to cyber attacks.” The checklist contains 478 questions grouped into six categories: hardware, software, networks, automation, humans and suppliers. It is “a baseline where we think organizations should be,” Bumgarner says. He urges information security professionals to examine the checklist and offer their input. “It’s not something created in a vacuum,” he says. “We welcome any comments on it.”

Schwartau says information security professionals must convince upper management that the threat of information warfare is real. That’s because it’s not just the security person’s problem. “Too often the info sec guys get laden with things they shouldn’t,” he says. For instance, are the costs involved in implementing better power backup systems worth more than a potential data loss? “That’s a business decision, not a technical decision,” Schwartau says.

On the other hand, the threat of information warfare indicates how critical cybersecurity issues are in the Internet age. “There should be an info sec signoff on any major corporate decision,” says Schwartau.

Finally, the most important lesson of the Georgian attacks may lie in how they compare to the Estonian attacks: While the Estonian attacks were simplistic and scattershot, the Georgian attacks were targeted. The level of sophistication “jumped from ground zero to three,” says Bumgarner. “An information security professional should worry about this.”

Schwartau is more blunt. “Is it going to get nastier?” he asks. “Yes, it’s going to get nastier.” (ISC)

---

*John Soat is a freelance business and technology journalist based in Cleveland, Ohio, USA.*



# THIS IT STAFF



# IS ARMED AND READY

[Microsoft.com/Security/MSAT](http://Microsoft.com/Security/MSAT)

Microsoft

**Find the tools and guidance you need for a well-guarded network at [microsoft.com/security/MSAT](http://microsoft.com/security/MSAT)**

Download the free Microsoft Security Assessment Tool (MSAT) to help you discover the security state of your business and begin to prioritize your security efforts for improvement. MSAT can aid you in assessing security weaknesses, revealing a prioritized list of issues, and provide you with specific guidance to help minimize risk identified in your IT environment.



# NOW PRESENTING

THE THOUGHT OF HAVING TO GIVE A  
PRESENTATION OFTEN FILLS PEOPLE WITH  
DREAD. BUT THAT DOESN'T HAVE TO BE  
THE CASE, REPORTS BRUCE HOARD.

IT'S ALMOST INEVITABLE THAT, AT SOME POINT IN YOUR CAREER, you will have to give a business presentation. It may be an overview of a new security development or policy to your coworkers, a business case for increased funding to your managing director or CEO, or an informational session to a packed room at a conference. ♦ Public speaking is nerve-wracking for many people; it brings heightened levels of apprehension. We asked some experts for their advice on getting over that fear, as well as how best to present oneself.

## Style Counsel

The content of your presentation is an important ingredient. But it's the way you present it that matters most. "You may have the best content in the world, but if you don't deliver it well, people are going to shut you down pretty quick," says Tom Walsh, CISSP, president of Kansas-based Tom Walsh Consulting LLC. Walsh has given hundreds of presentations, including one called "Presentation Skills for Information Security Professionals."

"You only have about 10 seconds to capture their attention," he says, and suggests starting with an interesting story or humorous anecdote. However, steer clear of jokes unless it's one about you: "It's OK if I'm making fun of myself," Walsh says, "but if I poke fun at someone else, I have to be very careful. Jokes should be reserved for comedians."

When it comes to visual components, most speakers use PowerPoint to create a slide presentation. Here again, style and format is important. "Unless you make your presentation provocative

or somewhat interesting, you're really asking for some people to go to sleep right in front of you," says Patricia Myers, (ISC)<sup>2</sup> Board Chair.

Myers, who has 23 years of information security experience at companies including American Express and Wells Fargo, suggests interspersing a few text slides covering the most salient points with some relevant bar charts or graphs. "People are really impressed by numbers, so make sure to include them in your presentation," Myers says, adding that statistics are especially likely to attract the attention of senior executives, who have a keen interest in operations performance and benchmarks.

As you customize your slides, beware of overdoing it. Dave Paradi, Mississauga, Ontario-based author of *Guide to PowerPoint* and *The Visual Slide Revolution* (see his blog at [pptideas.blogspot.com](http://pptideas.blogspot.com)), says we are "suffering through an epidemic of overloaded text slides." Paradi conducts surveys asking what people find most annoying about PowerPoint presentations. According to his latest survey ([www.thinkoutsidetheslide.com/survey2007.htm](http://www.thinkoutsidetheslide.com/survey2007.htm)), some of the problems include:

- ▶ The use of full sentences instead of bullet points;
- ▶ Poor slide design and layout, including poor color selection and layouts that are inconsistent throughout the presentation;
- ▶ Text too small to read.

The worst thing you can do in a PowerPoint presentation is to read the slides word for word. "Don't read a report off the screen," Paradi says. "Information security professionals might feel that they have to present lots of data. The data is important, but the audience wants to know: how will this data make me a better decision maker?"

"Boil down the data to the key message," Paradi continues, and increase the use of visuals to replace text. "Have the data as a separate handout, not a slide, and only if audience members ask for it. They trust you as a professional." As you work through your content, anticipate questions that audience members will have, and be prepared to answer them.

## Ready, Set, Breathe

Once you're comfortable with your slides and the message you want to present, it's critical that you practice. Walsh recommends doing a dry run of your presentation in front of other people. Time yourself, and ask for feedback about the tone of your voice, the way you emphasize words and the presentation's visual content. Running through your presentation a few times before your final delivery will help ease your nerves.

Both Walsh and Paradi encourage presenters to visualize their presentation and to create a conversation with the audience. This can be done in several ways—for

example, asking questions or suggesting exercises such as breaking into small groups to work on hypothetical problems. If possible, incorporate specific examples you have encountered in your own professional life. This connects you with your audience on a personal level, Walsh explains.

To help boost your confidence the day of your presentation, dress appropriately. "It is important to always dress like you're the expert," says Myers. "A speaker has to be sincere and particularly credible-looking—especially if they're asking for resources from their CEO, but even if they're presenting at a conference. It's really important to dress the part."

Finally, it's quite common to get a case of the jitters—dry mouth, shaking hands, slight twitches—right before or upon standing up to give your presentation. To help overcome this, focus on breathing normally and try to speak slowly. Walsh suggests having a glass of water at your side.

"Nervousness prior to speaking is actually a good thing," Walsh says, "because when you're nervous, it kicks in the adrenaline, and if you harvest that adrenaline, it will come out as energy and enthusiasm. When the presenter is enthusiastic about the presentation, the audience also gets enthused." (ISC)

---

*Bruce Hoard is a freelance business and technology journalist based in Bangor, Maine, USA.*



# How can you leverage your CISSP® certification to further your career?

Use it to earn credits toward an MS or BS degree at Capella

Eric Hollis

Field of Study: Information Technology  
Lieutenant, U.S. Navy



For more information call 1.866.736.1755  
or visit [www.capella.edu/isc2](http://www.capella.edu/isc2)



**Credit for your CISSP® and work experience may save you substantial time and money<sup>1</sup>.** You could earn up to 30 credits toward your BS in IT by documenting your current certification and work experience. For the MS in IT, you may be able to earn up to 20 credits through a petition process.

**Apply what you learn.** Capella's information security specializations are designed to build on your understanding of security technology. Our curriculum focuses on solutions architecture to enhance your ability to assess needs and implement appropriate security measures across the enterprise. Additional benefits include:

- ▶ **Online flexibility** for working adults pursuing PhD, MS, and BS degrees from an accredited\* university.
- ▶ **Designated** as a National Center of Academic Excellence in Information Assurance Education by the National Security Agency and the U.S. Department of Homeland Security.
- ▶ **Reduced tuition** for education alliance members, which includes more than 100 leading U.S. companies, 20 percent of U.S. community colleges, and every branch of the U.S. armed forces.
- ▶ **A Virtual Lab Environment<sup>SM</sup>** that provides hands-on access to the latest tools and technologies.



<sup>1</sup> Residents of Washington may receive credit for prior learning only in the bachelor's program.

**\* ACCREDITATION**

Capella University is accredited by The Higher Learning Commission and is a member of the North Central Association of Colleges and Schools (NCA), [www.ncahlc.org](http://www.ncahlc.org).

**CAPELLA UNIVERSITY**

225 South Sixth Street, Ninth Floor, Minneapolis, MN 55402,  
1.888.CAPELLA (227.3552), [www.capella.edu](http://www.capella.edu)

## Your Best Investment

REAP LONG-TERM BENEFITS BY STEADILY INVESTING  
IN YOUR CAREER. **BY LEE KUSHNER**

“CONGRATULATIONS,” THE LETTER READS. “You have just passed your CISSP exam and are now a Certified Information Systems Security Professional.” You’ve joined approximately 60,000 CISSPs around the world, and with your mind at ease, you begin to get excited about where this accomplishment might take you. But before you go too far into dreams of your career future, you should think about ways



to position yourself for success.

The field of information security is becoming increasingly competitive. When sourcing for premier leadership roles, hiring managers are selecting from a pool of candidates that fit both the position requirements and the corporate culture—but they can still choose only one. How do you become that “one”?

The candidates selected for these opportunities generally have one trait in common: They regularly invest in themselves. Because there is no clear-cut formula for predicting the long-term benefit of any one career investment, a

steady pattern of investing is the best way to differentiate yourself. This pattern illustrates qualities found in leaders, including commitment, dedication, education, sacrifice and passion.

Career investments can take many forms. Traditional ones include education and certification. Some investments focus on specific skill development, such as technical training, public speaking and business communication. Others may have indirect benefits, such as life coaching, time management—or even golf lessons.

Understanding your career

goals and long-term objectives are key factors. Begin by defining your strengths and weaknesses to gauge which skills you must acquire. Then you can make an informed decision on which investments will be the most valuable.

Investments share two components: sacrifice and impact. Sacrifice is defined in terms of money and time. Impact is defined by how, and how quickly, your investment will move you closer to your career goal. Determining how much of both it will take to achieve your goals should be a significant factor in your career investment decision. Analyze the value of your investment and determine if the sacrifice and impact are equivalent.

Career investments are personal in nature, providing levels of value and impact that are unique to each professional. But whatever you choose, any investment in yourself and your career traditionally pays great dividends. (ISC)<sup>®</sup>



*Lee Kushner is the president and founder of LJ Kushner & Associates, an executive search firm dedi-*

*cated to the information security industry. To take part in his career management survey, visit [www.infosecleaders.com/survey](http://www.infosecleaders.com/survey).*

**Upgrade your system preferences.**



**Specialize in one of three CISSP Concentrations.**

While a CISSP® prepares you for high level work in information security, specialization allows you to explore more senior positions with larger organizations. Go for the (ISC)<sup>2</sup>® CISSP-ISSAP®, the CISSP-ISSEP® or the CISSP-ISSMP®. Find out how at **[www.isc2.org/concentrations](http://www.isc2.org/concentrations)**.

For those in search of excellence – you just found it!



**SECURITY TRANSCENDS TECHNOLOGY®**



## Finding the Right Balance

BUSINESS, MARKET AND GOVERNMENTAL PRESSURES  
PUT INFORMATION SECURITY PROFESSIONALS IN  
A HARD SPOT. **BY WALMIR FREITAS**



INFORMATION SECURITY PROFESSIONALS are under a lot of stress. They face business pressure to provide access to data to meet objectives, mitigate risks, and follow policies and procedures. They also face governmental pressure to comply with regulations. And they are left at times to deal with these tasks without adequate support from management.

How do they strike the right balance?

Obviously, governmental regulations must be complied with. Implementing security controls through the use of technology, including software and hardware, can help. But doing this requires the right budget. Plus, there are many regulations yet to come and the information security professional must develop a framework to match them, using existing resources and investments.

We live in a global economy: What happens in one country affects us all. The Sarbanes-Oxley Act is a classic example of this. When some U.S. companies—including Enron and WorldCom—crashed, it changed the way that corporations worldwide manage their internal controls. For example, if a company in Brazil, France or India wants to have its stocks listed on the New York Stock Exchange, it must implement all the

required controls and obtain an appropriate independent statement. Even companies that are not affected by certain compliance regulations have started to follow the same path to compete in the market.

Each country typically has its own specific regulations regarding data security. Information security professionals must be aware of them, and stay up to date on global regulations and trends. For example, privacy regulations are not as critical in Latin America as they are in North America, but compliance with the Payment Card Industry Data Security Standard is required. Keeping a watchful eye on how other countries handle privacy concerns as we implement our own security controls prepares us if—or when—privacy regulations go into effect in our own.

There is a well-known recipe for striking a balance among business, market and government pressures for governance, and mitigating risks while achieving compliance: Convince management that they are also part of the solution. Many information security professionals act like lonely cowboys who are just trying to do what's right. What they should do is bring management into the game and share responsibilities with those outside of IT security, while ensuring the safety of information.

What happens in information security—good or bad—affects the business as a whole. That is what information security professionals must communicate to business managers. Doing so will gain their support, which will help mitigate some of the enormous responsibility that information security professionals shoulder. (ISC)<sup>2</sup>



*Walmir Freitas, CISSP, CISM, CISA, CBCP, is the CISO of Fidelity National Information Services in Brazil. He is also a member of the (ISC)<sup>2</sup> Advisory Board of the Americas.*

## CISSPs Needed in Japan

NEW COMPLIANCE REGULATIONS  
ARE INCREASING THE NEED FOR  
MORE CISSPs. **BY JUNYA HIRAGA**

THE FINANCIAL INSTRUMENTS AND EXCHANGE LAW (which is also known as J-SOX, the Japanese version of Sarbanes-Oxley) was enacted in Japan on June 7, 2006. At the start of fiscal year 2008, it was applied to all publicly listed companies—and created a need for more CISSPs in Japan.

One of the goals of J-SOX is to maintain the soundness of financial reporting by promoting internal controls, and IT governance is a key factor in meeting that goal. According to the IT Governance Institute's *IT Control Objectives for Sarbanes-Oxley*, internal controls consist of three layers:

**1. Entity-level controls:** strategies and plans; policies and procedures; risk assessment activities; training and education; quality assurance; and internal audit, among others.

**2. Application controls:** completeness; accuracy and existence/authorization; and presentation/disclosure.

**3. IT general controls:** program development; program changes; access to programs and data; and computer operations.

This third layer contains the key factors to IT governance success. Specifically, IT general controls can be roughly classified into two categories: management of program and data, and management of access privileges. Each operation that involves these two categories requires a process for requests and a process for approval of the requests, as well as segregation of duties and documents that define these procedures.

Roughly 3,700 public companies are subjected to J-SOX—including many smaller ones with only one or two IT staff members. It is quite difficult for companies like these to comply with the IT general control requirements. For example, in an emergency only a database administrator can modify data stored in a database by logging into the database. But small companies often lack the organizational structure, segregation of duties, and documented procedures required to do this.

This is where CISSP-certified professionals can help. They are educated on how to implement three types of security controls:

- **Administrative security.** The emphasis here is to promote documentation that defines: how after-the-fact requests for data modification and after-the-fact request approvals are handled; a way to confirm the data modification results; the need to periodically audit access database logs to monitor for fraudulent access.

- **Technical security.** This ensures that the database server is on the protected network segment with a router or firewall.

- **Physical security.** This ensures that the database server room housing the database server is protected with a robust wall and locking system that includes entrance and exit monitoring.

These security controls can compensate for a lack of staff, inadequate segregation of duties and a weak organizational structure. And by providing the manpower and know-how to put those controls in place, CISSP-certified professionals can help smaller Japanese companies become J-SOX compliant. (ISC)



**Junya Hiraga**, CISSP, is the assistant manager, Service Infrastructure Section, Project Support Division, for CSK Systems Corp. He is based in Toyko.



# INVENT YOUR FUTURE. Get Certified!



## **Certified Information Systems Auditor™ (CISA®)**

Since 1978, the CISA certification has been renowned as the globally recognized achievement for those who control, monitor and assess an organization's information technology and business systems.

## **Certified Information Security Manager® (CISM®)**

CISM certification is for the individual who manages, designs, oversees and assesses an enterprise's information security program.

## **Certified in the Governance of Enterprise IT™ (CGEIT™)**

ISACA's new IT Governance certification is intended to recognize a wide range of professionals for their knowledge and application of IT governance principles and practices.

**CISA®**  
CERTIFIED INFORMATION SYSTEMS AUDITOR™

**CISM®**  
CERTIFIED INFORMATION  
SECURITY MANAGER®

**CGEIT™**  
CERTIFIED IN THE GOVERNANCE  
OF ENTERPRISE IT™

Visit [www.isaca.org/rgcertification](http://www.isaca.org/rgcertification).

**ISACA®** 40th ANNIVERSARY  
Serving IT Governance Professionals



**Press your escape button.**



**Get out and enjoy a variety of (ISC)<sup>2</sup>® Events!**

Advance your knowledge of emerging issues and stay current on information security trends with (ISC)<sup>2</sup> Events. Choose from one of our renowned Security Leadership Series events around the world on a variety of information security topics. From live events to online seminars, we offer worldwide education choices that keep you on your game. Not to mention CPE credits for members.

For more info, visit **[www.isc2.org/events](http://www.isc2.org/events)**.



**SECURITY TRANSCENDS TECHNOLOGY®**