InfoSecurity PROFESSIONAL®

ISSUE NUMBER 8

An (ISC)² Digital Publication

www.isc2.org

Ripple effect

Global concerns arise over localized legislation

YOU DON'T NEED MORE SECURITY. YOU NEED BETTER SECURITY.

CA Security Management software streamlines your IT security environment so your business can be more secure, agile and compliant without upsizing your infrastructure. All with faster time to value. Greater efficiency starts with more efficient IT. That's the power of lean.

Learn more at ca.com/security/value

SC MAGAZINE AWARDS 2009 WINNER Honored in the U.S.

SC Magazine Reader Trust Award for
Best Identity Management Solution

ca. Software

issue 8
2009 VOLUME 4

To view this issue online, visit *www.isc2.infosecpromag.com*

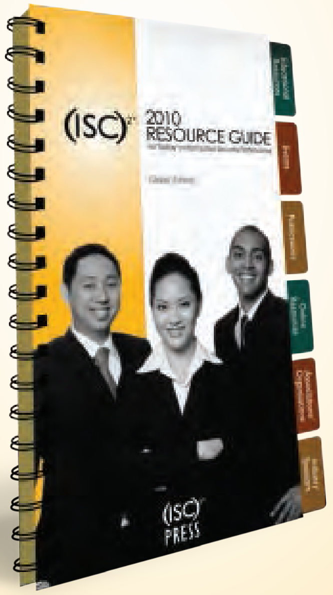
[features]

[also inside]

20 (ISC)² years of excellence

COVER MAP PHOTO BY RANDALL FUNG/CORBIS; RIPPLE IMAGE BY ISTOCKPHOTO

InfoSecurity Professional is published by IDG Enterprise Custom Solutions Group, 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)² 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)². (ISC)², the (ISC)² digital logo and all other (ISC)² 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 www.isc2.org. To order additional copies or obtain permission to reprint materials, please email infosecproeditor@isc2.org. To request advertising information, please email tgaron@isc2.org.



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

http://bit.ly/2AjLxS

For a list of events (ISC)² is either hosting or sponsoring, visit *www.isc2.org/events*

InfoSecurity PROFESSIONAL

Management Team

Elise Yacobellis
Executive Publisher
727 683-0782 ■ eyacobellis@isc2.org

Timothy Garon
Publisher
508 529-6103 ■ tgaron@isc2.org

Marc G. Thompson
Associate Publisher
703 637-4408 ■ mthompson@isc2.org

Amanda D'Alessandro
Communications Coordinator
727 785-0189 x242
adalessandro@isc2.org

Sarah Bohne
Director of Communications and Member Services
727 785-0189 x236 ■ sbohne@isc2.org

Judy Livers
Senior Manager of Marketing Development
727 785-0189 x239 ■ jlivers@isc2.org

Sales Team

Paul Moschella
Regional Sales Manager
New England and Canada
781 769-8950 ■ pmoschella@isc2.org

Edward Marecki
Regional Sales Manager
U.S. East Coast and Europe
401 351-0274 ■ emarecki@isc2.org

Christa Collins
Regional Sales Manager
U.S. Southeast and Midwest
352 563-5264 ■ ccollins@isc2.org

Gordon Hunt
Regional Sales Manager
U.S. West Coast and Asia
949 366-3192 ■ ghunt@isc2.org

Jennifer Hunt
Events Sales Manager
781 685-4667 ■ jhunt@isc2.org

IDG Media Team

Charles Lee
Vice President, Custom Solutions Group

Amy Freeman
Project Manager ■ afreeman@isc2.org

Anne Taylor
Managing Editor ■ ataylor@isc2.org

Kim Han
Art Director

Lisa Stevenson
Associate Production Manager

CSO
Custom Solutions Group

ADVERTISER INDEX

CA	Inside Front Cover
BCI	p. 10
CRC Press.	p. 7
DRI International.	p. 16
HISPI.	p. 13
IEEE	p. 12
ISACA.	Inside Back Cover
(ISC)²	p. 4, Back Cover
Norwich University	p. 11

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

Some Closing Remarks

BOARD CHAIRPERSON PATRICIA MYERS REVIEWS (ISC)^2'S ACCOMPLISHMENTS AND LOOKS AT WHAT'S AHEAD

AS 2009 WINDS DOWN, I'd like to take one more opportunity to thank all of our members for helping us celebrate (ISC)^2's 20th anniversary this year. We enjoyed seeing you at celebratory member events, and looking back at the organization's rich and fruitful history.

This year has had its own share of milestones:

- (ISC)^2 updated the Career Tools site, making it easier for members to post résumés, collaborate and network with other members, and view job postings.
- Following its successes in the United Kingdom and Hong Kong, the Safe and Secure Online Program, which aims to educate children ages 11 to14 on how to stay safe online, has been launched in the United States. Already the program is generating excitement and commitments of support from top-notch organizations including Microsoft, several of whose (ISC)^2-certified security professionals have become volunteers. Find out how to join them at https://cyberexchange.isc2.org/volunteers.
- (ISC)^2 created and launched its own professional networking site, InterSeC. Here you can share knowledge with other (ISC)^2 members and build virtual groups based on your professional interests.
- (ISC)^2 announced it will be transitioning to computer-based exams, starting with the CSSLP, in 2010. An exclusive contract has been signed with Pearson VUE to deliver (ISC)^2's certification exams.

Indeed, it has been a busy year at (ISC)^2, and the future promises to bring more of the same. We are continuing our global expansion and providing opportunities for members to not only collaborate, but also to better address the day-to-day challenges they face in their work. Security transcends borders; threats and vulnerabilities exist no matter if you work in France, Australia, Singapore or the United States. That is why (ISC)^2 will continue to provide education and training, and to foster networking among members across the globe.

Finally, I encourage you to find ways to continue the growth and positive influence of the information security profession. As John Rossi writes in this issue's Career Corner (p. 19), it's critical to use our CISSP credential to give something back. It not only does a good turn for your community, but it also boosts your own career. For example, having been a volunteer member of the (ISC)^2 board for the past 10 years, I have met the most incredible people, while also helping to promote the information security profession.

It has been a distinct pleasure serving you, the members of (ISC)^2. I wish you all continued success.

Sincerely,

Patricia A. Myers

Patricia A. Myers
CISSP-ISSMP
Board Chairperson, (ISC)^2 Board of Directors

GLOBAL SECURITY NOW HAS A COMMON ADDRESS

At last, there is the ideal place for you to meet and collaborate with your fellow members, wherever you are located, and the address is https://www.isc2.org/MemberHome.aspx. With a few clicks you can register and start building your personal community, without the noise and clutter of other open social networking sites. That's right, InterSeC is purpose-built for the information security field, so you can be sure that everyone you meet online is governed by a similar code of ethics and has the same passion and interest driving their quest for shared knowledge.

Meet other professionals from across the world or down the street, swap ideas with CISSP®s who work in the same line of business or why not form an online special interest group. With over 60,000 (ISC)²® members you are bound to find someone who thinks like you.

INTER SEC

where secure minds meet

[fyi] (ISC)² MEMBER NEWS

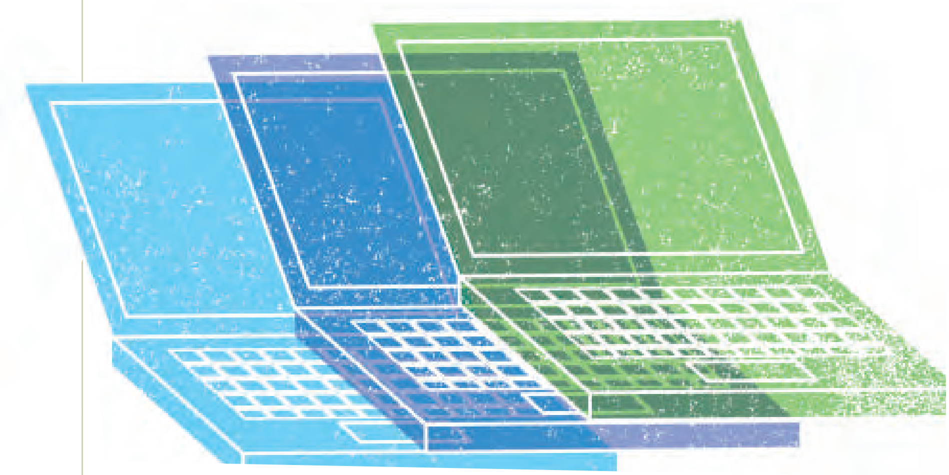


ILLUSTRATION BY ISTOCKPHOTO

From Paper to Computer Screen

TO MEET the growing demand for certified information security professionals, (ISC)² will soon offer computer-based delivery of some of its exams, thanks to a partnership with Pearson VUE, a global provider of computer-based testing.

Starting in mid-2010, the Certified Secure Software Lifecycle Professional (CSSLPcm) exam will transition from traditional paper exams to a computer-based test, which individuals can take at one of Pearson's more than 250 centers worldwide. To ensure the security and integrity of the test, all centers include biometric collection, monitoring and other safeguards.

(ISC)²'s other credential exams, including the CISSP, will be phased into this computer-based model over the next three years.

"Our relationship with Pearson VUE is an important investment in the future of our certification programs," says W. Hord Tipton, CISSP-ISSEP, CAP, executive director for (ISC)². "It allows us to take advantage of technical advancements to offer our candidates more, conveniently located venues, as well as the ability to register for an exam online 24 hours a day, seven days a week, for any time a testing center is open. Also, candidates will no longer have to wait several weeks to receive notification of their test results."

New (ISC)² Member Services Advisor in Hong Kong

IN RESPONSE to Asia-Pacific members' requests to have a Member Services Advisor available in their region of the world that can speak languages such as Korean and Chinese, (ISC)² recently hired Michaella Park. Michaella joined (ISC)²'s Hong Kong office as Member Services Advisor for the Asia-Pacific region in July 2009. She is responsible for handling all member requests, as well as credential queries and renewals in the region. Park has a strong customer service background, having spent more than three years in the hospitality sector in sales and customer service functions. She has a Bachelor of Arts degree from Chung-Ang University in Korea, and is fluent in English and Korean.

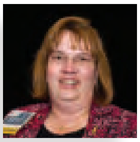
Government Leaders Honored for Accomplishments

(ISC)² recently honored the winners of the sixth annual Government Information Security Leadership Awards (GISLAs) in four categories. The GISLAs are awarded to information security professionals who have demonstrated a significant leadership role in the implementation or management of an information security workforce improvement initiative, program or project, either government-wide or agency-specific. (ISC)² certification is not a pre-requisite for receiving a GISLA. **The winners of the 2009 GISLAs are:**

Non-Managerial Information Security Professional: BOBBY AKINS, CISSP, MSCE, Security +, Network +, ITIL V3 Foundations, network integrator, 561st Network Operations Squadron at Peterson Air Force Base. Akins bolstered mission-critical systems and ensured compliance with the U.S. Department of Defense (DoD) 8570.1 Directive, which requires all DoD information security personnel to obtain professional certification. Due to his work, his squadron increased compliance from 13 percent to 87 percent, with all remaining uncertified personnel to complete certification this year.

Senior Non-Information Security Manager: ERIN FINKES, director of workforce development, Defense Contract Management Agency (DCMA). Finkes serves as the contract operations technical representative for IT training contracts and program manager for the Information Assurance Workforce Improvement Training Program. She significantly contributed to the fulfillment of DCMA's strategic and tactical goals to train, certify and manage its assurance workforce.

Senior Information Security Manager: STANLEY JOSEPH JARZOMBEK, JR., CISSP, CSSLP, PMP, director of software assurance, U.S. Department of Homeland Security's National Cyber Security Division. Jarzombek has exhibited outstanding leadership in focusing on the improvement of software security through a program of improved software development techniques, stronger acquisition practices and improved software security research and development.



Federal Contractor Information Security Professional: MARGARET SPANNINGER, who leads the Security Awareness, Training and Professional Development Services at Booz Allen Hamilton Inc. Spanninger has set up online awareness training and has developed an innovative way to assist students in focusing on key aspects of information security. As a result, more than 7,000 individuals have been trained in information security best practices.

*For more information about the GISLAs and the winners, please visit www.isc2.org/gisla.

CISSPs Head Back to School

The Safe and Secure Online Program, which educates children ages 11 to14 on how to stay safe online, is quickly expanding in the United States. Standing at the front of the classroom is Dan VanBelleghem, CISSP, who works at NCI Information Systems, Inc. He recently talked about online safety with students at Swanson Middle School in Arlington, Virginia. Find out how you can become a volunteer at https://cyberexchange.isc2.org/volunteers.

PHOTO BY CHARLES JABLOW, MATHESON COMMUNICATIONS

Always Evolving Resources from Auerbach / CRC Press

– publishers of the Harold Tipton Certification Book Series –

While today's info-security threats may be bolder and more complex, we have the tools, resources, and expertise to keep you more than a step ahead of any sort of malfeasance, whether it comes from outside or within.

Vulnerability Management

Park Foreman, GroupM, New York

Shows how much easier it is to protect against a threat than clean up in the aftermath of an attack

Catalog no. K10093, August 2009, 347 pp., $79.95 / $63.96

Data Protection

Governance, Risk Management, and Compliance

David G. Hill, Mesabi Group LLC, Westwood, Massachusetts

Discusses existing and emerging data protection technologies including forcloud computing, storage tiering, server virtualization, and green computing.

Catalog no. K10353, August 2009, 330 pp.,, $69.95 / $55.96

Cyber Fraud

Tactics, Techniques and Procedures

James Graham, Verisign iDefense Security Intelligence Services, Dulles, Virginia

Exposes the patterns and operations of the cyber criminal with an insider's look

Catalog no. AU9127, April 2009, 520 pp., $79.95 / $63.96

Information Security Management

Concepts and Practice

Bel G. Raggad, Pace University, Pleasantville, New York

Illustrates how to audits that conforms with the ISO 17799 the new ISO 27001

Catalog no. AU7854, January 2010, c. 568 pp., $79.95 / $63.96

The Executive MBA in Information Security

John J. Trinckes, Jr., Hampton, Florida

Allows busy executives to get up to speed on what it takes to develop an effective efficient info security program

Catalog no. K10501, October 2009, 352 pp., $69.95 / $55.96

Information Security Management Handbook

2009 CD-ROM Edition

Edited by

Harold F. Tipton, CISSP, HFT Associates, Villa Park, California

Micki Krause, CISSP, Pacific Life Insurance Company, Newport Beach, California

Includes all three volumes of the sixth edition print version plus material that has never appeared in the print.

Catalog no. AU0984, July 2009, CD-ROM, $199.95 / $159.96

Order securely online at www.crcpress.com • Free Standard Shipping on All Orders

***Enter promo code 601LA at checkout to receive your discount.**

Offer good through January 31, 2010

Ripple Effect

A small U.S. state has created big international waves with its data security regulations, reports **Efrain Viscarolasaga**.

A new set of regulations coming out of the Commonwealth of Massachusetts has the potential to create some serious headaches for information security professionals.

After some some delays and revisions, the data security regulations—which are a product of an identity theft protection act signed into law in September 2007—will go into effect on March 1, 2010. The core of this new legislation requires any company or organization with customers in Massachusetts to protect sensitive data through encryption, both internally and when shared with partner vendors. In other words, just as a Massachusetts-based bookstore must ensure the security of the personal, identifiable information of its Massachusetts-based customers, so too must an online vendor in California or an IT services provider in India—making the law a national and international concern.

"What makes the Massachusetts law unique is that it is the first state law that requires any business that has Massachusetts customers' personal information to implement certain specifications, including administrative, technical and physical safeguards, for compliance," says Lynne Barr, a partner in law firm Goodwin Procter's Boston-based office.

Critical Criteria

Keys to the legislation include the requirement that each company have a written, feasibly implemented data privacy procedure, as well as a response plan in case of a breach. And organizations that share personal data with partner vendors must ensure those partners comply with the regulations as well.

In addition, says Barr, the spectrum of data covered by the legislation is broad, and includes any data that links the name of a Massachusetts citizen with a Social Security number, driver's license number or broadly defined "financial account number."

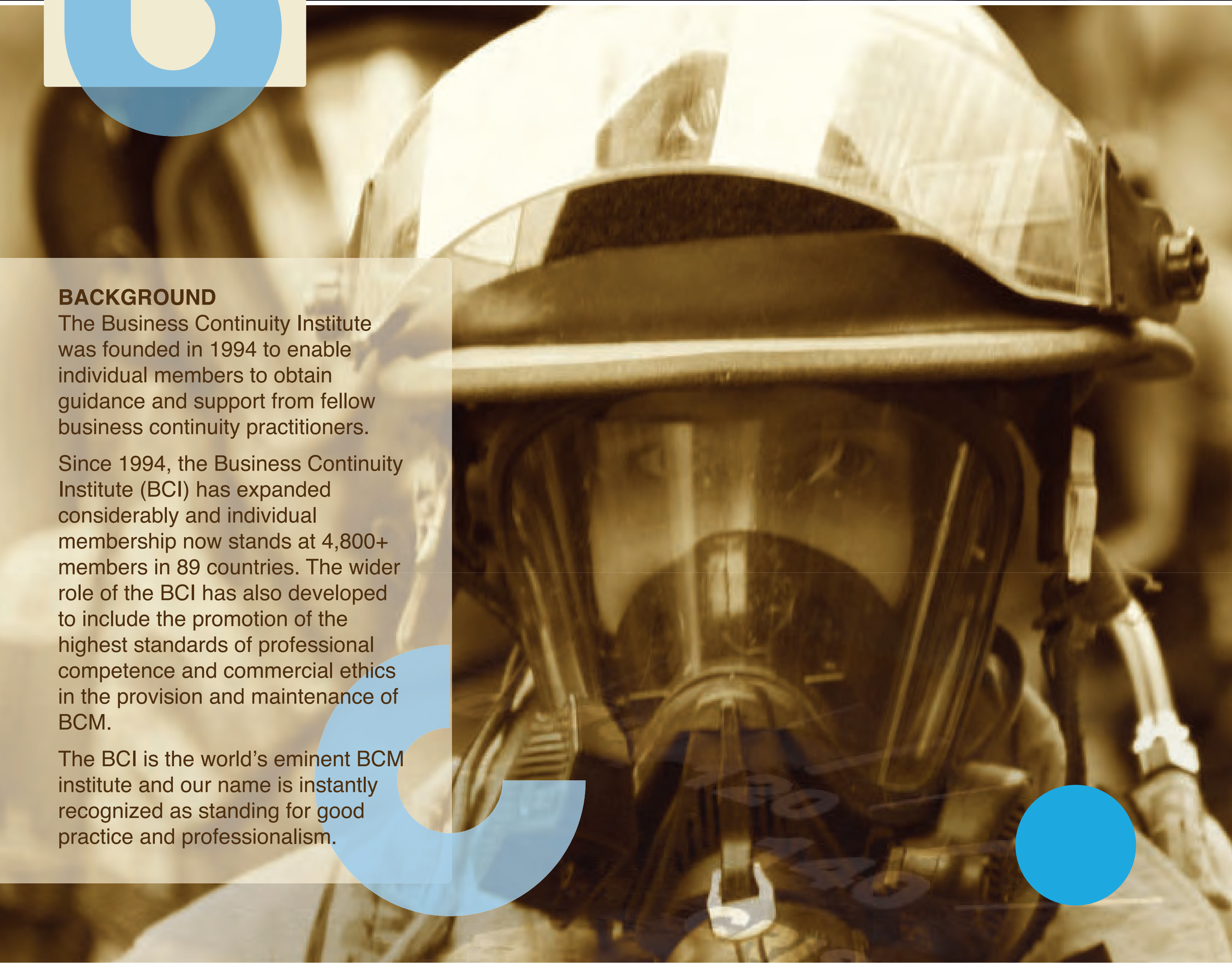
The legislation also includes technological demands for encryption, though while the original incarnation of the bill set specific technological standards for encryption, those parameters have been modified to require encryption that is "reasonable and technically feasible."

For companies and industries accustomed to strict data privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act and the Payment Card Industry Data Security Standard (PCI DSS), the legislation may not seem challenging. However, for many others, the time, cost and complexity of compliance with the new regulations could pose problems.

According to Peter Kosmala, assistant director of the International Association of Privacy Professionals (IAPP), there has been concern—both in the U. S. and globally—about the legislation, particularly the time frame in which vendors must become compliant. Although it was originally incorporated in 2007, the compliance date has been moved several times and now rests on March 1, 2010.

"As a general response, there has been a concern that the legislation presents an unnecessarily hard burden to meet, but the underlying purpose is still valid," he says.

And it's not just U.S.-based businesses that will struggle. "We held a privacy conference with GDD [a German data privacy organization] in Europe last spring," Kosmala says, "and the number one question at the event was 'What's going on with the Massachusetts legislation?'"



BACKGROUND

The Business Continuity Institute was founded in 1994 to enable individual members to obtain guidance and support from fellow business continuity practitioners.

Since 1994, the Business Continuity Institute (BCI) has expanded considerably and individual membership now stands at 4,800+ members in 89 countries. The wider role of the BCI has also developed to include the promotion of the highest standards of professional competence and commercial ethics in the provision and maintenance of BCM.

The BCI is the world's eminent BCM institute and our name is instantly recognized as standing for good practice and professionalism.

ADVANCE YOUR BC KNOWLEDGE WITH OFFICIAL BCI LEARNING SOLUTIONS.

BCI E-LEARNING

Based on the internationally recognized BCM Life Cycle, this E-learning program is available as individual chapters or as a complete course. Content is based on the six elements of the BCI's Good Practice Guidelines, and incorporates the British Standard BS25999.

While this program is not designed exclusively as preparation to sit for the BCI Certificate, much of the material on the exam is covered.

BCI TRAINING

World-Class Official GPG training can be taken as an Onsite ILT or via the world-wide web with BC Live Online ILT.

BCI SCOPE

The only online BC self assessment tool that offers a BCI certificate exam experience with scores based on the official testing algorithm that delivers a completely logic based and unbiased analytical evaluation to be used to assess your readiness for certification.

Business Continuity Institute

+1 (703) 637-4424 | EDUCATION@THEBCI.ORG | WWW.THEBCICERTIFICATE.ORG

The Costs of Compliance

According to a recent survey[1] of information privacy professionals conducted by the IAPP and Goodwin Procter, 60 percent of respondents said their organizations would be ready by the deadline, while 29 percent said their compliance efforts would "probably" be complete.

One reason for the uncertainty is the vendor requirement dictating that partner vendors, whether they're in Massachusetts, the U. S. or overseas, also adhere to the Massachusetts requirements. Sixty percent said their organizations have more than 10 vendors with access to personal information, while 30 percent said they have more than 100 such partners.

Dealing with that complexity will involve expenses, primarily in terms of the time incurred by information security and privacy professionals to ensure compliance is in order, as well as documentation and filing fees. According to the survey, 33 percent have already spent more than $50,000 on compliance efforts toward the new regulation, while another 12 percent have spent between $10,000 and $50,000.

Most industry experts expect small businesses will be financially hardest hit by the regulations. The Massachusetts Office of Consumer Affairs and Business Regulation has estimated that the new rules would cost a 10-person firm $3,000 in upfront costs and another $6,000 yearly. "For larger institutions, the feeling has been that they do a lot of this stuff anyway, so it is just another compliance headache," says Barr.

"Small businesses are going to have to make the decision of whether they spend the money to comply or risk not being in compliance," says Stephen Adams, an independent consultant and former New England small-business advocate for the U.S. Small Business Administration.

The penalties for noncompliance could be even greater than the cost to comply, should the organization experience a data breach. For example, following the TJX Companies data breach, Massachusetts instituted fines of $5,000 per individual record violation for companies found in noncompliance following a data breach.

Steps Toward Compliance

Darrin Maggy, the president of security consulting firm Provisional Security Group, says a robust culture of security—the basic tenet behind any data protection legislation—is something every company should strive to have. This culture of security should filter through all departments, from management to finance to human resources, not just the IT department.

"Don't do it for compliance," Maggy says. "Do it for your clients, your employees and your corporate reputation. It's much harder to recover from a breach than it is to establish a solid plan."

Maggy's number one recommendation: Take a hard look at sensitive data under management and build a procedure to

[1] The Goodwin Procter and IAPP survey was conducted in August 2009, among more than 200 IAPP members from businesses of all sizes and all parts of the world.

secure it. A company culture of security should behave as an umbrella over sensitive data, providing more coverage than attacking each compliance criterion individually would.

Part of the information security culture should be the development of written and technological procedures for handling sensitive information, including encryption. While the specifics of such procedures will differ according to size and type of organization, the principles remain the same and effective execution brings compliance.

As the deadline for compliance approaches, Adams recommends that information security professionals be aware of the regulations' details, and realize that there is no single solution for all companies to bring them into compliance. Adams stresses there is no "silver bullet" to meeting the regulations, particularly with the less-stringent encryption requirements in the latest version of the legislation.

"What's crucial here is that the small and medium-sized businesses do not get taken [advantage of] because of the new regulations," he says. "Small businesses do not need the same systems that a [large global financial institution] needs for compliance, and there may be disreputable firms out there that will use compliance to overcharge."

What's Next

Another complicating factor in the mix is the possibility of additional legislation, including at the federal level. There is similar existing legislation in California (Senate Bill 1386), although its reach is limited to businesses in that state. However, as the Massachusetts bill goes into effect, at least 40 other U.S. states have data security bills on the books or in debate.

U.S. federal legislation, including the Personal Data Privacy and Security Act that was submitted earlier this year, could gain traction. The act recommends fraud and racketeering charges for individuals or companies that do not protect sensitive, personally identifying information. It would also make it illegal for companies to conceal a data breach of sensitive information gained in a fraudulent manner. As this issue of *InfoSecurity Professional* magazine was going to press, the bill had been passed by the U.S. Senate Judiciary Committee and was being considered by the U.S. Senate.

It's not surprising that the federal government has stepped into the data security regulation fray. "Because e-commerce doesn't recognize state borders, state-by-state regulation of e-commerce is illogical," says Adams. "There is no good reason for state regulations in digital commerce."

For now, however, companies all around the world will look to Massachusetts as they seek policy and compliance with data protection—at least if they want to do business with Massachusetts companies or residents, that is. (ISC)²

Efrain Viscarolasaga is a freelance business and technology journalist based in New Hampshire.

GAME OF CAT AND MOUSE

SECURITY WATCH LIST 2010

Researchers have helped to identify the most troublesome security spots for the year ahead. Analyst firm Frost & Sullivan fills us in.

The Black Hat annual conference, held in July, is a large, well-known event where world-class researchers gather to report critical IT flaws. Some notable revelations from past conferences include:

- Dan Kaminsky's report of a domain name system (DNS) cache poisoning vulnerability (Kaminsky is director of penetration testing at IOActive)
- A Cisco IOS flaw that resulted in a lawsuit—and a media circus
- A report on using virtualization to create undetectable malware
- A showcase of vertical-specific exploits, such as global mobile system vulnerabilities and asynchronous transfer mode problems
- Revelations of network security technology weaknesses, such as network access control

Black Hat conferences are known in the information security community for being trend-identifiers. As such, the following are the top 10 areas that analyst firm Frost & Sullivan, using information from the July 2009 Black Hat conference, believes should be on every information security professional's watch list.

THREAT VECTOR 1

MOBILE SYSTEMS

Mobile subscribers sent and received more than 900 billion short message service (SMS) messages in 2008—an increase of 132 percent compared to 2007. The number of transmitted multimedia messaging service (MMS) messages was approximately 32 billion. SMS and MMS traffic is expected to continue to grow rapidly in the coming years. This increased volume presents an attractive opportunity for hackers to disseminate malware to a vast audience.

At the conference, Luis Miras and Zane Lackey of iSEC Partners reported a vulnerability in the way mobile phones handle SMS messages. This flaw enables an attacker to hijack

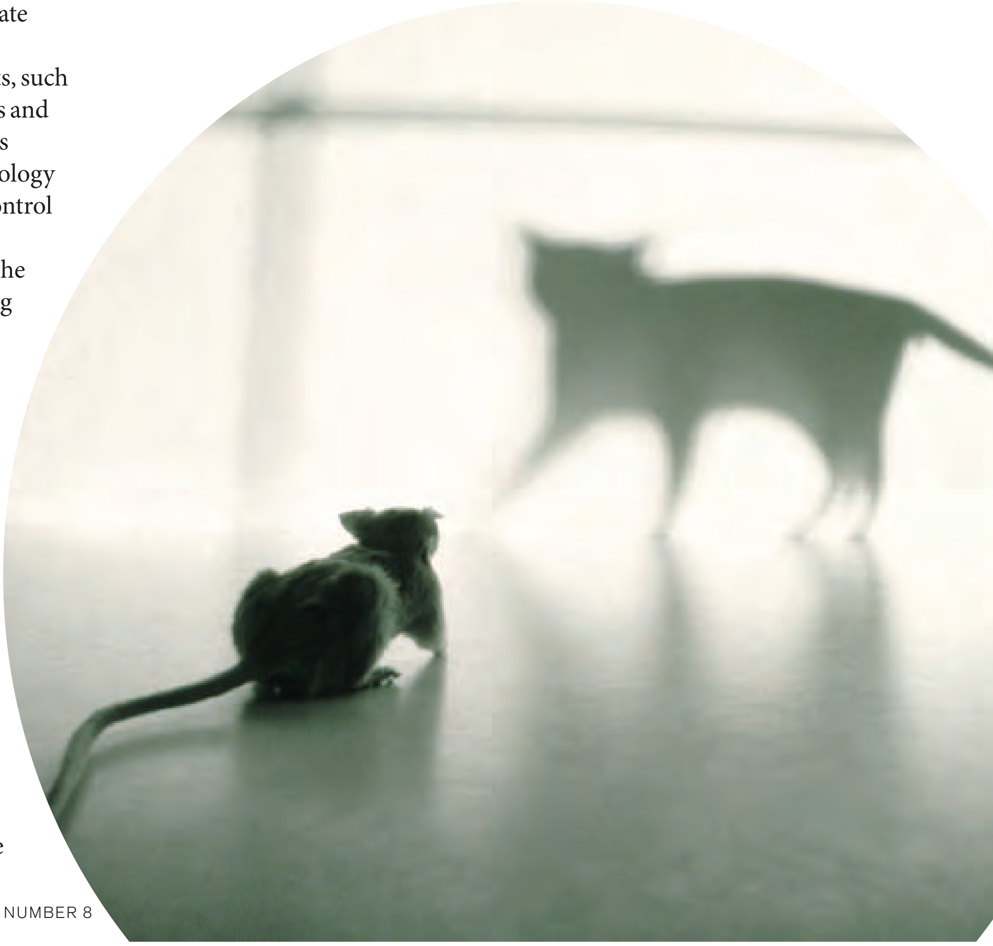


PHOTO BY RANDY M. URY

smartphones, with varying degrees of control depending on the phone. Miras and Lackey also released “There’s an Attack for That” (TAFT), a suite of proof-of-concept tools for jailbroken (a process by which the device is modified so that unauthorized or unofficial code can be installed) iPhones that searches for flaws.

THREAT VECTOR 2

ROOTKITS

Rootkits are a rare form of malware gaining popularity among hackers. A rootkit—often spread through viruses and worms—is a piece of malware that can take full control of a system, obscure itself, and survive system restores or memory wipes. It can even defeat antivirus programs.

Numerous presentations at Black Hat discussed rootkits. Some included illustrations of rootkits found in the wild, while others focused on detecting them. The clear message is that rootkits are dangerous, difficult to detect and here to stay.

THREAT VECTOR 3

ALL THINGS APPLE

Apple’s machines and devices have been the target of rootkit-related attacks. An Apple keyboard, for example, was discovered to be susceptible to a rootkit attack through its firmware update system. Also, to demonstrate an Apple vulnerability, security researcher Dino Dai Zovi released a proof-of-concept toolkit that loads an advanced rootkit on Mac OS X machines.

Many Apple users believe their devices are immune to attacks. The July Black Hat conference debunked this urban legend, revealing that the hacker community is taking a close look at Apple and that users must be aware of the security threats.

THREAT VECTOR 4

OFF-THE-SHELF SOFTWARE

Some Black Hat presentations were related to security concerns over preinstalled software or software straight from the factory. There have been incidents of malware being preinstalled during the production process, such as with the Insignia digital picture frames in 2008. Also, Sony BMG’s attempt at digital rights management ended up as a rootkit on their music CDs in 2005.

Researchers at CoreLabs, the research center of Core Security Technologies, discovered software that behaves as a rootkit. Computrace LoJack for Laptops (from Absolute Software), which comes factory-installed at the basic input/output system (BIOS) level, is designed to protect and help locate stolen laptops. While not inherently malicious, the researchers claim that it’s not very secure, leaving the possibility for devastating attacks.

THREAT VECTOR 5

SECURE SOCKET LAYER (SSL)

That lock on the bottom right of your browser may mean little before long. SSL is a trusted, secure protocol for encryption and authentication. At this year’s Black Hat event, Dan Kaminsky discussed problems with X.509 certificates, which are used for SSL encryption and authentication. X.509 has been known to be flawed since 2004 because it uses MD2, an outdated, weak cryptographic hash function.

VeriSign, the leading provider of digital certificates, downplayed this announcement, saying it no longer uses X.509. Regardless, businesses have invested millions of dollars in X.509 despite its technical and structural issues.

In a similar presentation, security researcher Moxie Marlinspike showed how an attacker could spoof SSL certificates using a “null” or empty string character. This tricks the Web browser into accepting code and can give an attacker a range of attacks to perpetrate.

These presentations illustrate the need for vigilance on the part of end users and vendors, as products and technologies once deemed secure may now be compromised.

THREAT VECTOR 6

DAILY DEVICES

Many presentations at Black Hat illustrated new attacks on everything from parking meters to smart grid electricity networks, demonstrating the need for baked-in security on all devices and functions, regardless of size or type. In an interesting twist, a card skimmer was installed on an ATM near the hotel at which conference attendees were staying—whether it was a coincidental or intentional act is not known. Chris Paget, an RFID security expert for Google, discovered the device and reported it to authorities.

THREAT VECTOR 7

SOFTWARE ENGINEERING

Conficker, a computer worm that targets the Microsoft Windows operating system, has infected up to 10 million machines. It captured the world’s attention due to its April 1 activation date. Although the hype has died down, the worm continues to infect machines.

Conficker uses numerous advanced malware techniques to avoid detection and deletion, making it unique among malware. Many reports suggest that the software engineering techniques used in Conficker rival those of top software companies. Malware has become more sophisticated—and criminals are using development best practices to ensure that their code works as designed.

THREAT VECTOR 8

PRIVATE DATA

Private data is big business and numerous presentations at Black Hat looked at the security flaws surrounding it. Joshua “Jabra” Abraham, a security consultant for Rapid7, and Robert “RSnake” Hansen, CISSP and a security strategist for several startup companies, gave a presentation titled “Unmasking You!” which demonstrated many of the weaknesses associated with popular techniques used to protect privacy, such as anonymizers and remote tracking of computer user names.

A presentation by Alessandro Acquisti, associate professor of information technology and public policy at Carnegie Mellon University, titled “I Just Found 10 Million SSNs” showed that information about an individual’s place and date of birth can be exploited to predict his or her Social Security number (SSN). The method by which SSNs are assigned has been public knowledge for many years and has been used to estimate when and where a known SSN may have been issued.

The message of the presentation is simple: SSNs and many other pieces of private information were not designed to be used as authenticators, but as simple identifiers. Businesses and other third parties should stop using SSNs and other personally identifiable information as if they were confidential passwords.

THREAT VECTOR 9

VIRTUAL MACHINES

By significantly reducing the power consumption and number of machines required, virtualization technology has enabled companies to realize tremendous data center cost savings. But virtual machines (VMs) carry their own set of security challenges.

For example, an administrator could easily and accidentally undo a virtual machine's security protections when it is being moved from one cluster to another. In addition, VMs present increased opportunities for a single point of failure or infection. If a virus got on the first install or base machine, potentially hundreds of VMs could be comprised.

Presentations by Matt Conover, principal software engineer at Symantec Research Labs, and security researcher Kostya Kortchinsky offered these examples and illustrated that there are plenty of holes in the security architecture of virtual machines.

THREAT VECTOR 10

ELECTRICITY

Even with the best anti-malware software in place, it's still possible to physically detect keystrokes. Security researcher Andrea Barisani and system administrator and IT consultant Daniele Bianco illustrated that there are plenty of ways to remotely sniff laptop and desktop keystrokes using mechanical energy emissions and power line leakage. The attacks are done with inexpensive equipment and are difficult to guard against.

THE GAME CONTINUES

The information security industry is involved in a continual cat-and-mouse game with hackers. For 2010, Frost & Sullivan predicts an increase in attacks against non-traditional targets.

Most of the buzz of previous Black Hat conferences was around widespread attacks that could wreak widespread havoc. Many of the attacks cited this year appear to directly target end users on the devices they use on a daily basis—phones, ATMs and the like. This increases the complexity of securing these devices and ups the ante for security researchers and practitioners. (ISC)²

Working in the Network Security Practice, Rob Ayoub, CISSP, is a research manager and Chris Rodriguez is a research analyst at Frost & Sullivan, a global analyst firm.

Pausing for REVIEW

Before you give or get a performance review, consider the objectives, writes John Soat.

ILLUSTRATION BY CSA IMAGES

Performance reviews often create anxiety. For managers, they mean either trying to keep a well-performing employee motivated and happy, or figuring out how to get more out of an underperforming individual. For employees, it's often a question of how a review will affect their compensation and career advancement.

For information security professionals, a comprehensive review process—in connection with a metrics-driven security strategy and supported by ongoing evaluations—can help the infosec operation function more effectively, be integrated more closely with IT and the overall business strategy, and comply with internal and regulatory controls.

The Big Picture

"The first step to determine whether an information security professional is doing a good job is to establish a competence management process in line with and managed by the company's personnel department," says Nelson Novaes Neto, chief information security officer at UOL, one of Brazil's leading Internet media portals.

It's important that reviews for security personnel speak to the operations and goals of the information security organization. Professional competence is equated with knowledge and experience in distinct areas, such as telecommunications and risk management, as well as information, operations and network security. Performance in those areas should be measured against the organization's policies, program implementations and related metrics.

But competence on the job also involves "abilities and attitudes, and sometimes personal qualities that bring a competitive benefit to the organization," points out Neto.

That idea is key for Pamela Fusco, vice president and chief financial officer of the Information Systems Security Association (ISSA) and former chief security officer of Merck & Co., Citibank and MCI. "Security isn't just about security," she says.

"You may have an individual who says, 'Hey, I worked 10 hours on this and I caught 10,000 intrusions,'" but that person may fail to comprehend how that "spills over into the next level." She believes the more pertinent question is: How does that fit into the company's business model?

Giving Reviews

The first rule for managers in the performance review process is: Do your homework. Go over the goals and objectives established in your organization's strategic plan at the beginning of the year and see how and where an individual's work got the organization closer to those goals and objectives—or didn't. Include a self-evaluation for the person being reviewed.

The second rule is to be specific. "The most important factor is to provide appropriate feedback consisting of clear and objective daily examples," says UOL's Neto.

Many managers employ what's called a 360-degree review process. It involves garnering feedback on an individual from multiple sources including colleagues, managers, executives, etc. This process brings up a critical but often underplayed aspect of measuring performance: customer service. Gary Baney, CEO of IT services firm Boundless Flight, and former vice president of distributed systems at Key Bank, says this is something many formal performance review processes fail to address. "There is no customer satisfaction loop built into the review process," he says.

Rule number three is to think in terms of the infosec organization as a whole. Just because a certain individual is assertive and demonstrative doesn't mean that person is the most valuable member of the team—and vice versa. "Caution the more proactive individuals not to put out the flame of someone else," says Fusco. Similarly, it's okay to provide your best performers with perks, such as additional training, but make sure those perks don't take too much time away from working with the team.

Perhaps the hardest part of the review process is the negative review. If that's what's called for, make sure you have evidence of poor performance. Again, be as specific as possible. Don't be intrusive or personal, but be assertive, says Fusco.

Getting Reviewed

When it comes to your own performance review, know your company's review process and how it is employed within the organization. Engage your manager in a dialogue and get that person to be specific. "I want professional advice about how to improve as a manager based on performance results," says David Ruiz Silva, CISO of Nacional Financiera SNC, a financial services agency in Mexico City.

Keep track of your successes. Look for concrete examples over the past six to 12 months, such as finished projects, problems resolved, and process improvements and innovations. "I check my list of accomplished goals and activities during the year, and take note of the problems and solutions that happened during my management," says Silva.

Be honest. Note where you've had problems and discuss those with your manager. "We must not only stress the competencies where we have achieved high levels of performance, but also mention the deficiencies and failures identified in the self-evaluation, as well as present an action plan in line with the manager to assist in the continuous improvement of performance," says UOL's Neto.

> "The review process should be part of a formalized information security **STRATEGY** that gathers as much objective and **TANGIBLE DATA** as possible and transforms that data into information. We cannot manage what we cannot measure."
>
> – NELSON NOVAES NETO,
> CHIEF INFORMATION SECURITY OFFICER AT UOL

If you get a bad review, think it over. Were there valid points in the assessment, and what can you do to improve in those areas? Schedule a follow-up conversation with your manager.

And don't be afraid to discuss career advancement opportunities. "I want to have a clear perspective of what development path is available for me within the company," says Silva.

An Ongoing Process

Even though most formal performance reviews occur once or at most twice a year, many management experts stress that performance evaluation should be on ongoing process. "I believe it is essential to perform daily follow-up of team and staff members' performance to ensure that performance is continuously controlled," says Neto.

Fusco has has developed what she calls a "litmus test" approach to judging team performance. During monthly or quarterly staff meetings, she has put her own performance review on a screen behind her, with sensitive areas redacted. It's an effort to share information about goals and objectives and to make staff members feel part of the overall objectives of the organization.

Fucso's approach highlights a general rule: Performance reviews should not come as a surprise. From the reviewer's perspective, if the person being reviewed is surprised by a criticism, there's a lack of communication. From the perspective of the person being reviewed, it means you aren't in touch with your team leader's expectations.

Ultimately, performance reviews should never be ad hoc or happen in a vacuum. Neto advises that the review process should be part of a formalized information security strategy that gathers as much objective and tangible data as possible and transforms that data into information. "We cannot manage what we cannot measure," he says. (ISC)^2

John Soat is a freelance business and technology journalist based in Ohio.

Stand Up & Be Recognized

AS CISSPs, IT'S IMPORTANT TO CONTRIBUTE TO OUR CAREERS, COMMUNITIES AND PROFESSION, WRITES JOHN ROSSI.

THERE ARE NEARLY 65,000 CISSPs worldwide, and the number is constantly growing. This growth is a testament to the fact that the world recognizes the value of this professional certification.

It is critical that we continue to nurture this distinction by using the credential to give something back to the certification community, the information security profession, and society. Each of us has a gift, talent or skill developed through hard work, study and experience. Each of us is an expert in some specific area of information security.

I invite and challenge my fellow CISSPs to stand up and be recognized. Each time you make a mark, no matter how small or large, you get opportunities to leverage and accelerate yourself while elevating your profession, your credential and your country.

There are many different ways to do this. First, think about your area of expertise within the information security field, be it network security; firewall configuration; policy writing; encryption technologies; personnel security; physical security; or a particular manufacturer's product.

Next, think of a way to share your expertise. This could mean writing an article for a newsletter, journal, or conference package. You could give a presentation; coach students about career opportunities in your field; teach a short course at a local college; provide a free demonstration of your company's product; or moderate a vendor panel or roundtable discussion. As public speaking is my forte, I often give talks at local high schools, infosec conferences and other venues.

Once you've made a contribution, there are several things you can do. Notify (ISC)² of your activity. (ISC)² may publish it to the world. Update your résumé to include the accomplishment. Let your managers and colleagues know what you did, perhaps in the office newsletter. Ask the organization to which you've contributed if they will give you a letter of appreciation. Use your past accomplishments to do something similar at another venue.

Every time we stand up and are recognized for our talents, we bolster our confidence. We add more credibility to the CISSP credential because the community sees what CISSPs can accomplish. And we strengthen (ISC)²'s reputation—a reputation from which we ourselves benefit, because of our affiliation with this trusted international certification and education body.

I encourage and challenge you to take one small step today: Reach out to the community in some way that will allow you to stand up and be recognized. (ISC)²

John Rossi, CISSP-ISSEP, is the Professor of Systems Management/Information Assurance at the U.S. National Defense University in Washington, D.C.

PHOTO TOP BY MOODBOARD/CORBIS

Mobile Insecurity Issues

THE GROWTH OF MOBILE DEVICES IS CAUSING MANY NEW SECURITY CHALLENGES, WRITES DAVID RUIZ SILVA.

MOBILE DEVICES are transforming quickly into a solid and viable candidate to replace our current and for now, typical computing platforms—including the PC and laptop.

Following Moore's Law, chip makers are now on the path to deliver 32nm system-on-a-chip (SoC) technology, which will enable more powerful computing capacity in a new breed of smaller devices that are the size of the palm of your hand. These devices will offer users an enriched experience when accessing the Internet and a whole new set of multimedia applications. The possibilities are promising in terms of the applications and solutions that people will use to make their lives easier with this more powerful and energy-saving technology. Trends show that these low-cost devices can be obtained extensively, even in emerging markets.

Because the Internet is becoming increasingly open to crackers and phishers, identity management for mobile devices will gain more relevance when using them to make electronic transactions and acquire a broad scope of services through e-commerce. To minimize the risks, it is necessary to protect the user's identity to avoid fraud against their financial assets.

3G and GSM measures are already deployed for smartphones, relying on several methods to protect data in transit or user identity. However, these standards only work in the network layer, not in the application layer, which is most commonly used by individuals to conduct transactions. Other ways to connect to public networks using these gadgets—such as WiFi connections, WEP, WAP, WiMax—are not as secure as they should be.

Certainly, there is a need to develop solutions based on open standards oriented to the application layer for these mobile devices—for example, to secure centrally sensitive information such as personal information or identity numbers, Social Security numbers, credit card data, or passwords to access financial services. One possibility is tokenization, which is a technology that uses a payment card industry-compliant central repository with a unique token reference, allowing an individual's data to reside safely outside the device.

Issues such as user authentication with these mobile products must be addressed with great care. There is an effort underway to use cell phones to make payments by relating the cell phone number to a bank account. This initiative is gaining momentum in Mexico, where there is draft legislation for banking transactions allowing this technology for multiple payment purposes.

Another way to verify identity is to have specific IDs for mobile devices with a security management service. It would provide correlation with the mobile device owner, resembling the way PKI certificates are used in PC applications to verify users' identities.

The good news is that we, as information security professionals, will be busy. There is a lot of work to do to secure mobile devices. (ISC)²

Ing. David Ruiz Silva, CISSP, CISA, CGEIT, is the CISO of Nacional Financiera SNC, and is based in Mexico City. He can be contacted at druiz@nafin.gob.mx.

PHOTO TOP BY GEORGE DIEBOLD

succès
success
Hatzlaha
Успех
επιτυχία
sucesso
성공
éxito
succes
成功
successo
Erfolg
Sukces
Successo