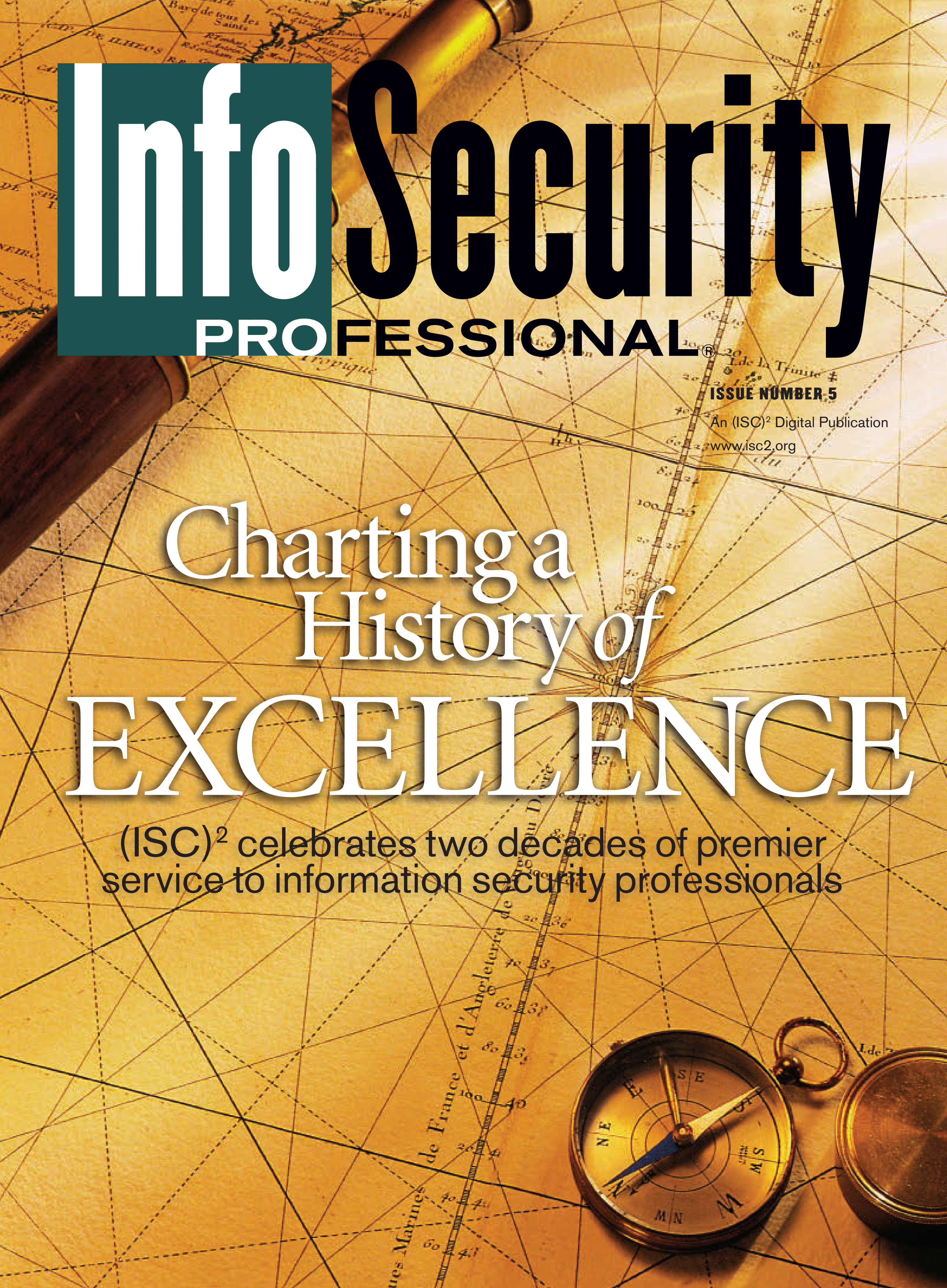


InfoSecurity PROFESSIONAL®

ISSUE NUMBER 5

An (ISC)² Digital Publication
www.isc2.org

Charting a History *of* EXCELLENCE

(ISC)² celebrates two decades of premier service to information security professionals

issue 5
2009 VOLUME 1

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

features

20 (ISC)² years of excellence

also inside

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)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. © 2009 (ISC)² Incorporated. All rights reserved.

COVER IMAGE BY VEER. ILLUSTRATION ABOVE BY CAMPBELL LAIRD/VEER

PHOTO BY GREG PEASE

Upcoming Events

RSA Conference 2009
April 20-24
San Francisco
www.rsaconference.com/2009

JAX09
April 20-24
Mainz, Germany
http://it-republik.de/jaxenter/jax

The Computer Forensics Show
April 27-29
Washington, D.C.
www.computerforensicshow.com

Infosecurity Europe
April 28-30
London
www.infosec.co.uk

ChicagoCon
May 4-9
Chicago
www.chicagocon.com

SecureAmsterdam
May 12
Amsterdam
www.isc2.org/EventDetails.aspx?id=2648

SecureChicago
May 12
Chicago
www.isc2.org/EventDetails.aspx?id=3342

The 10th InfoSecurity Conference
May 21
Hong Kong
www.eq-events.com

SecureScandinavia
June 2
Stockholm
www.isc2.org/EventDetails.aspx?id=3810

SecureAmericas
June 4-5
Crystal City, Va.
www.isc2.org/EventDetails.aspx?id=3720

2nd Digital Security Forum
June 26-27
Lisbon
www.digitalsecurityforum.eu

SC Magazine Conference
July 7
London
www.onlinethreatsconference.com

SecureAsia
July 7-8
Kuala Lumur
www.informationsecurityasia.com

SD Best Practices
September 21-24, 2009
Boston
www.sdbestpractices.com

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

http://tinyurl.com/ckur6r

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

CXO Media Team
Matt Avery
Vice President, Custom Solutions Group

Amy Freeman
Project Manager
afreeman@isc2.org

Anne Taylor
Managing Editor
ataylor@isc2.org

Mary Lester
Executive Director, Art and Design

CSO
Custom Solutions Group

ADVERTISER INDEX

CA	C2
Norwich	p. 5
Microsoft Corp.	p. 13
SCIPP	p. 14
Capella University	p. 17
ISACA.	p. 22
(ISC)².	p. 20, C3, C4

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

The Value of Currency

RECESSION HIGHLIGHTS NEED FOR INFORMATION SECURITY PROFESSIONALS TO STAY UP TO DATE.

IN THIS STRESSED ECONOMY, organizations typically conserve and even reduce resources, and the inevitable result is employee layoffs.

Because there is so much data to protect and increased pressure to guard it, IT professionals, and in particular information security professionals, are often the last to be let go. However, individuals in the IT security field are not completely immune to downsizing, which is why it's critical to ensure your job skills, credentials and professional networks are current.

PHOTO BY ALEX McKNIGHT

Information security professionals should be asking: What's next? Do I need greater specialization? Will my skills and résumé demonstrate that I am prepared to meet the needs of the future?

As you consider the answers to these questions, remember that (ISC)² membership offers advantages in shaping your career path. As a global organization, we are able to provide resources to our members worldwide. Here are some of the benefits that you should take advantage of:

The updated (ISC)² Career Tools site. This site allows you to post your résumé, collaborate and network with other members, view job postings and much more (see page 4).

Free CPE opportunities. From e-Symposia to local workshops, there are many free ways to keep your knowledge current. Visit the CPE page on the member Website for more information.

Networking opportunities. Stay connected with your peers through the CISSP forum, member community on LinkedIn or a member reception—all free services to members.

The new Certified Secure Software Lifecycle Professional (CSSLP^{cm}) certification, which focuses on ensuring the software security throughout the lifecycle development process. Having the CSSLP on your résumé is one more way to distinguish yourself from others vying for similar jobs.

Most sectors are showing increasing interest in information security professionals who have certifications. In particular, the highly regulated banking and financial services industry is experiencing more sophisticated IT-related attacks and typically requires security certifications for many positions.

With regard to hiring trends, (ISC)² has seen greater emphasis in two areas: security architects and security specialists. In fact, research shows that these positions are rated near the top in terms of the most needed and protected jobs.

The bottom line is that it's critical to be current. Keep your résumé and certifications up to date, stay on top of your professional networks and sharpen your knowledge by checking out the (ISC)² Website and the articles in this magazine.

Sincerely,

W. Hord Tipton

W. Hord Tipton
CISSP-ISSEP, CAP, CISA
(ISC)² Executive Director

(ISC)² MEMBER NEWS

[fyi]

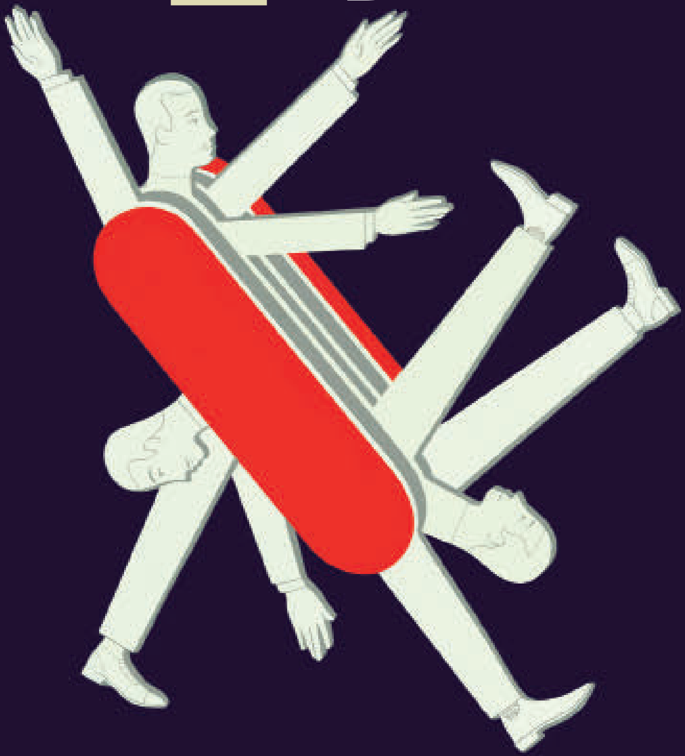


ILLUSTRATION BY NICK DEWAR/VEER

Putting Tools to Work

IF YOU'RE IN the market for a new job, or just want to see what's out there, visit the rebuilt Career Tools section–formerly called the Career Center–on the member Website.

Career Tools provides a one-stop shop for job seekers and employers. Certified members can post multiple résumés targeted to specific industries and search job postings. They can also sign up to receive job alerts when new employment opportunities are published and save postings for later follow up.

Unlike most career-based Websites, posting job opportunities on (ISC)²'s Career Tools site is free to employers and recruiters, who can also search résumés and sort them by industry and location.

"Career Tools is a fantastic benefit for our members, especially in this economy," says W. Hord Tipton, executive director of (ISC)². "It offers job seekers exclusive access to employers who either require or prefer an (ISC)² credential holder. And employers know they're getting superior, qualified candidates with knowledge and experience."

Check out Career Tools at: https://www.isc2.org/careers.

Help Celebrate 20 Years

(ISC)² will celebrate its 20th anniversary throughout 2009. For starters, see the special article in this issue that highlights the organization's founding (page 6). In addition to periodical news announcements commemorating (ISC)²'s history, there will be special receptions to honor members. Here are some of the locations and dates:

March 18
Tokyo, Japan

April 22
San Francisco, Calif.

April 29
London, U.K.

June 4
Crystal City, Va.

September 2 or 3
São Paulo, Brazil

For more information, or to register for a member reception, please visit: www.isc2.org/receptions (login required).

Member Milestones

(ISC)²'s worldwide membership is growing. Here are some recent milestones in member numbers:

Australia	1,000
Canada	3,000
India	1,000
Singapore	1,000
U.K.	3,000

Secure Americas

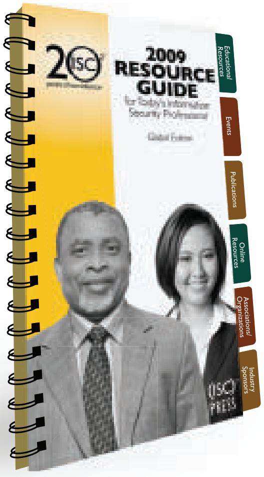
(ISC)²'S 5TH ANNUAL Secure Americas information security conference will be held June 4 and 5 in Crystal City, Va., and will bring together world-class speakers from the private and public sectors.

This year's conference will have two tracks. The first is a government track, focusing on security issues at the federal, state and local levels. Topics will range from the use of Web 2.0 to how government and law enforcement agencies face the ongoing battles against terrorism. The second track will focus on the public-private partnership as it affects security issues, including discussions around working with defense contractors, and the latest in security regulatory compliance.

For more information, visit www.isc2.org/EventDetails.aspx?id=3720.

2009 Resource Guide Now Available

The (ISC)² 2009 Resource Guide is now online. This guide is a great educational and networking tool for information security professionals and managers. It can be accessed at http://resourceguide.isc2.org.



CSSLP UPDATE

THE CERTIFIED SECURE Software Lifecycle Professional (CSSLP^{cm}) is the only certification in the industry to ensure that security is considered throughout the entire software lifecycle. Attend one of (ISC)²'s education seminars, which will be starting in May, with exams starting on June 27. Visit www.isc2.org/csslp for more information, seminar dates and locations.

Defining MOMENTS *in* (ISC)^2 HISTORY

As technology grew and shaped the way we worked, an urgent need appeared for standardization and education about information security, reports **Peter Fretty**.

TWENTY YEARS AGO, thriving businesses were ratcheting up their productivity, and computer technology was quickly evolving beyond clunky mainframes. Soon, personal computers were the lifeblood for most organizations. Most networks and technology-related communications were dependent on dial-up connections, data still predominantly existed on paper and security threats were limited—in the public's mind, hackers were largely fictional creations.

As (ISC)^2 celebrates its 20th anniversary, *InfoSecurity Professional* examines the security scene then and now by talking to some of (ISC)^2's founders. Future issues will continue to dig into the organization's roots.

PHOTO BY VEER

But it wasn't long before hackers broke into high-profile computer systems—at First National Bank of Chicago, at Los Alamos National Laboratory, at Sloan-Kettering Cancer Center and at Security Pacific Bank, among others. The U.S. government responded with hearings and later with legislation to address the concerns. And within a short period, the need for capable computer security professionals became obvious.

With few standards, there were many questions about the career path and responsibilities of these new security professionals. These questions set the stage for the International Information Systems Security Certification Consortium, or (ISC)^2.

With hopes of bringing a level of consistency and professionalism to the computer security space, (ISC)^2's founders and original participants came from all sorts of organizations dealing with computer security and information systems.

The CISSP CBK

The CISSP certification extensively covers these domains:

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigation
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security

FIRST THINGS FIRST

From initial meetings, it became clear that the overriding goal of (ISC)^2 would be to develop a professional certification in information security, to establish the policies and processes that protect an organization's information assets.

But first, the founders agreed on the need to define a common body of knowledge (CBK®). Doing so would provide the congruence necessary when administering a standardized certification exam like the Certified Information Systems Security Professional (CISSP®). A properly developed CBK would not only set standards, it would also serve as the first crucial step in defining the profession.

"The first major accomplishment was to develop the common body of knowledge," says Hal Tipton, CISSP-ISSAP, ISSMP, an independent consultant, past president of (ISC)^2 and former director of computer security for Rockwell International Corp. "We came up with a series of topics broken into about 16 categories that appeared to cover the waterfront. The idea was to create an exam that would address these areas and see if people were qualified."

After receiving input from the U.S. National Institute of Standards and Technology (NIST), the group pared the categories to the 10 in existence today (*see box, The CISSP CBK*).

While people from many organizations, institutes and groups played significant roles, the vast majority of the volunteers came from the ranks of the Information Systems Security Association (ISSA). "We all agreed that the eventual development of a certification program based on a common body of knowledge was a natural progression for our field," recalls Sandra M. Lambert, CISSP-ISSMP, founder of ISSA, now managing partner with security consultants Lambert & Associates LLC.

(ISC)^2 Fellow Dr. Corey Schou, associate dean and professor of informatics and information systems at Idaho State University College of Business, helped codify the CBK. "Starting the process by documenting the common body of knowledge was a significant step," he says. "After all, this same thinking has remained and is what the U.S. government uses with NIST and the Committee on National Security Systems."

GLOBAL GROWTH

Next, (ISC)^2's leaders turned their attention to developing a global presence. The first push was made by Johanni Saari, who worked with Finnish Telecom. He quickly convinced information security professionals working in Finland of the importance of (ISC)^2's mission and the need to have a professional security qualification. Finland was the first European country to have a significant number of certified professionals.

John Colley, from the U.K., was invited to become a board member in 1999. The International Committee of the board under the chairmanship of Randy Sanovic included Colley, Saari and Diana-Lynn Contesti.

Colley, CISSP and now managing director for Europe, the Middle East and Africa, admits that at the outset, growing membership was a challenge. "It was hard work," he says. "Initially, we needed to convince people that CISSP certification was important."

Another challenge dealt with courses without exams, and exams without courses. "People did not want to take exams without courses. And, understandably, no one wanted to provide courses without first seeing interest from individuals," Colley says. That all changed in 2001 when the MIS Training Institute joined forces with (ISC)^2, agreeing to work together to prove the merit of security education and accreditation.

"Today, people realize the CISSP can be a career differentiator, which makes it a must-have qualification," Colley says. This change in perception is reflected in the growth in membership: from 23 CISSPs in the U.K. in 1998 to 3,200 today. In 2002, a Danish information security professional became the 10,000th (ISC)^2 member. Today the Europe, Middle East and Africa region has 10,000 members in its own right.

Meanwhile, (ISC)^2 launched in the Asia-Pacific region in early 2004 when NTT Communications declared the CISSP the default certification requirement for its information security professional employees. "Security was becoming a major focal point for enterprises, with many new sophisticated threats and complicated security needs," says Toshiaki Kinugawa, CISSP, who coordinates business development for Asia-Pacific, (ISC)^2. "The industry needed professionals with recognized credentials. Previously, there were no professional-level credentials in Japan dealing with security issues."

(ISC)^2 capitalized on NTT's support by approaching "senior industry experts in academia, government as well as

"(ISC)^2 has come up with a disciplined and well-respected way to keep things ordered over time." — COREY SCHOU, IDAHO STATE UNIVERSITY COLLEGE OF BUSINESS

the business community," Kinugawa says. "We talked about the CISSP to general audiences and localized almost everything, including the exam and the customer service function. This way, people saw the commitment of (ISC)^2, which made it easier for them to accept the organization and the CISSP."

ASSESSING THE ENVIRONMENT

During (ISC)^2's early years, information security professionals dealt primarily with issues that today would seem quite basic, such as allowing system programmers to securely dial in to a mainframe computer to resolve production problems. "We did not have to worry about wireless, networks were more closed, the Internet was not used for business, and systems were mainly centralized," says Lambert.

Hacking and viruses existed, yet not at the level they do now. "At the time, the goal in penetrating systems was often motivated with attacks designed to cause disruption and to feed the hacker's ego," she says. "Today, hacking is financially motivated and is populated by the criminal element. People have developed an expertise, and they are searching for financial gain."

IT environments have also changed. "Initially, information was stored on a mainframe, later it was moved onto servers, and then we had data warehousing, which is very similar to a mainframe environment from a security point of view," Lambert says. "Today, we are facing wireless issues with the array of portable devices in use—BlackBerry, laptops, etc."

Information storage has shifted, too, in terms of size, price, capacity and portability. For example, retail marketing executives segment customer information, from buying habits to historical transaction data. "This is why the Payment Card Industry developed the Data Security Standards [PCI DSS], which require certain cardholder data to be stored in encrypted form," she says. "I anticipate that in the future we will see encryption requirements on the transmission of cardholder data."

The European security industry of the 1990s mirrored that of the United States. "The growing use of the Internet saw the rise of issues around protecting corporate information and fighting off viruses," Colley says.

For the Asia-Pacific region especially, "Y2K put a spotlight on secure information backup as well as maintaining data integrity," says Kinugawa. "At the same time, the Japanese government developed a program for organizations to prove their security management [was] in accordance with the recognized standard."

FOUNDING FATHERS

The initial groups that joined together to form (ISC)^2 included:

- Canadian Information Processing Society
- Computer Security Institute
- Data Processing Management Association (two special-interest groups)
- Idaho State University
- Information Systems Security Association
- International Federation for Information Processing

THE JOURNEY AHEAD

Lambert sees the emergence, acceptance and application of cryptographic technology as a positive step for the security environment. "In the past, business unit managers did not appreciate the risks associated with unencrypted or unsigned data, and cryptographic keys were hard to manage. Now we have crypto products embedded in systems and applications, more user awareness and more efficient key management techniques," she says. "The same is true for biometric products, which were available 20 years ago but were not as accurate or user-friendly and were more cost-prohibitive."

Schou says that all these factors have led to a definable career progression for information security professionals. "With the evolution of our environment and acceptance of the CISSP worldwide, security professionals have started doing things that are career-like, which yields a pathway for future progress," he says. "Today there is a need to turn out people who are also C-suite-qualified. (ISC)^2 has come up with a disciplined and well-respected way to keep things ordered over time."

Tipton adds: "We need to focus on developing secure applications. Not doing so opens up attack avenues. We have a serious need for better techniques," he says. "For instance, it would be ideal if systems could detect a problem and try to 'cure' themselves. Unfortunately, accomplishing this type of automation is going to be expensive, and it is going to require government participation. One step forward may be to encourage more student research in this area."

Recognizing that the Internet is the key to world communication and business networks, Tipton suggests an interesting path for security professionals.

"The core issue rests with the fact that the Internet was not initially designed to be secure. It was originally designed to make it easy for academic and research professionals to communicate among themselves," he explains. "The scary part is that we have come to rely on the Internet to control our infrastructure—power, water, transportation—and it would not take a lot of imagination to disrupt it. Even backups can also be readily identified and attacked."

These threats underscore the need for the certifications and education that (ISC)^2 provides, and make the information security professionals in its ranks more vital than ever.

Peter Fretty is a freelance business and technology journalist based in Michigan.

Mobile computing is more than just a trend, and that makes mobile security more than just a strategy, according to John Soat.

A Moving Target

BLAME IT ON APPLE.

"The factor in the market that's changed the way C-level officers think about [mobile security] is the iPhone," says Al Potter, senior consulting analyst with ICSA Labs, an organization involved in research, intelligence and certification testing of products. The iPhone, with its ability to access the Internet and download applications, has raised users' expectations for wireless devices. It has also complicated the job of information security professionals and raised awareness of how vulnerable mobile computing devices can be.

As these devices get smaller, more powerful and more ubiquitous, information security strategies must adapt. In the long term, the mobility imperative may force a refocusing by security professionals in their orientation toward information security.

BEGIN AT THE BEGINNING

Mobile computing started with laptops; mobile security starts there, too. The techniques used to lock down PCs and workstations—authentication, strong password protection, corporate firewalls—should be applied to laptops. Implement state-of-the-art security software, including antispam, antivirus and antispyware applications. Enforce corporate security procedures, such as patch management and aggressive Web monitoring. And require a written security policy regarding laptops, along with regular awareness training to familiarize users with that policy.

ILLUSTRATION BY PETE MCARTHUR/VEER

"The phone-that's-more-than-a-phone has more legs in Asia-Pacific and Europe than in the U.S. The threat is propagated more there than [in the United States]." – AL POTTER, ICSA LABS

Since laptops are portable, they can operate outside the corporate network. When not connected to the network, users should be required to interact with corporate resources over virtual private networks, and all data should be encrypted. Also, laptops must be secured when left unattended—an effort that should be highlighted in the corporate security policy.

Unfortunately, there are continued cases of laptops containing confidential corporate data being left by users in cars or at airports. That's why hard-drive encryption on corporate laptops is a growing trend, with hardware vendors often offering it as an added feature. Also, encryption is now incorporated into operating systems, such as FileVault on the Mac OS and BitLocker on Windows.

Security software vendors offer server-based management consoles that can automatically update antivirus applications on laptops, implement encryption, monitor email and Web traffic, back up and restore data, and lock out users who aren't authenticated and then remotely wipe data off those hard drives.

BALANCING RISK AND REWARD

With the proliferation of wireless devices, mobile computing has become more than laptops. "We're trying to come to terms with how we can embrace the reduced cost and agility and flexibility of these platforms while balancing the risk," says Christopher Hoff, CISSP, chief security architect at IT services vendor Unisys.

Though viruses and trojans targeted at cell phones have been reported, so far there have been no widespread, widely publicized attacks against mobile phones. But that doesn't mean it can't or won't happen. In its 2009 *Emerging Cyber Threats Report*, the Georgia Tech Information Security Center predicts an increase this year in malware aimed at mobile phones, and an equivalent increase in the number of bots attached to them. Patrick Traynor, an assistant professor in the School of Computer Science at Georgia Tech, writes in the report, "Malware will be injected onto cell phones to turn them into bots. Large cellular botnets could then be used to perpetrate a [denial of service] attack against the core of the cellular network."

Cellular data concerns are different in different parts of the world. "The phone-that's-more-than-a-phone has more legs in Asia-Pacific and Europe than in the U.S.," says ICSA's Potter. "The threat is propagated more there than [in the United States]." In Japan, for example, cell-phone phishing is a growing problem. This is due to the country's widespread practice of banking over mobile phones.

The corporate applications most closely associated with PDAs and smartphones are e-mail and, increasingly, data access. Unfortunately, security measures implemented at the corporate level can be problematic for wireless devices.

"To be successful in the wireless space, it's all about balancing constrained resources," says Scott Totzke, vice president of global security at Research In Motion (RIM), maker of the BlackBerry. Mobile devices, while small, incorporate limited but increasingly powerful processing power, communications capability and storage. Specifically, Totzke points out that battery technology "is not evolving at the pace of Moore's Law."

That's why security measures like antivirus applications and personal firewalls may present problems: They use resources that can drain battery life. In the *Emerging Cyber Threats Report,* Traynor pointed to "battery power as a primary security hurdle" in the cell-phone environment.

Not true, says Daniel Hoffman, author of the book *BlackJacking: Security Threats to BlackBerry Devices, PDAs, and Cell Phones in the Enterprise* and chief technology officer at Smobile Systems, which develops mobile device security software. The effect of anti-malware software on cell phones is "almost negligible," Hoffman claims, "if you have the appropriate solution."

There are security systems developed specifically for wireless devices. They offer comprehensive applications, including antivirus, antispam and firewall protection, as well as ways to control those devices remotely, such as remote lockdown and data wipe.

This is where the BlackBerry has an advantage over other PDAs and smartphones. First, RIM designed and built the BlackBerry from the ground up. "We wrote our own radio code, we have our own operating system, we have our own Java," Totzke says. Second, security features such as encryption are hard-wired into the device. Third, RIM offers the BlackBerry Enterprise Server, which provides many of the security measures mentioned, as well as remote-control and management capabilities, tailored specifically for the BlackBerry.

PROBLEM AREAS

While security problems associated with smartphones and cell phones are similar to those for laptops, there are unique variations. For example, cell phones are easier to steal. Another thing for global travelers to keep in mind, says Smobile's Hoffman, is that if they pass their wireless devices over to uniformed officials and other strangers, they're opening themselves up to risk. "If I can get a hold of it for less than a minute, I can pull all the contact info and a lot of data," he

continued on page 16

THIS IT STAFF
IS ARMED AND READY
MICROSOFT.COM/SECURITY/MSAT
Microsoft

Advertorial

HIPAA Now Applies Directly to Business Associates

Mark D. Rasch, Esq.
Principal – Secure IT Experts
mrasch@secureITexperts.com

As part of the federal stimulus bill passed February 17, 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act (HITECH). The new law applies the HIPAA privacy and security requirements directly to "business associates" of doctors, hospitals and insurance companies; enhances penalties and enforcement for violations of HIPAA; and requires both "covered entities" and their associates to notify patients, consumers and the government when there has been a breach involving health data. As a consequence, the HIPAA requirements of certification, training and awareness now apply not only to the healthcare provider, but also to their business associates. Moreover, ignorance of the law is no excuse. You may suffer new Civil and Monetary Penalties for not training your employees.

> **"As a consequence, the HIPAA requirements of certification, training and awareness now apply not only to the healthcare provider, but also to their business associates.**

Just in: "Business Associates" now covered by HIPAA

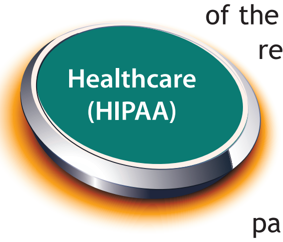
HIPAA required "covered entities" to have administrative, physical, and technical safeguards, and policy, procedure, and documentation demonstrating compliance with the security and privacy policies under the law. These safeguards included ensuring that all staff with access to Personal Health Information (PHI) were informed about the privacy and security requirements, and that they were adequately trained in the techniques and methods for protecting the privacy, confidentiality and security of this sensitive data.

The new law extends these requirements to virtually any entity that may receive PHI. If you perform "any function or activity" involving PHI, you are likely a "business associate." The definition of "function or activity" is all encompassing: legal, actuarial, accounting, consulting, data processing, management, administrative, accreditation, financial services and anything else for which a covered entity might contract out are included, if access to PHI is involved. As a result, not only must hospitals or medical insurers train their staff about the privacy and security of HIPAA data, but now lawyers, accountants, consultants, and even Internet Service Providers and others who transmit or process PHI must comply.

Under prior law, a business associate was only required to sign a contract with a HIPAA covered entity indicating that they would provide "reasonable and appropriate" security. Not any more. Now the business associate is directly liable under HIPAA if they haven't complied with all of the HIPAA requirements, including those for awareness and training. In fact, if they find that they are not compliant, they may have to notify their customer and/or the government.

HIPAA Requires Security Awareness Training

The best way to avoid a data breach is not only to have appropriate hardware and software security, but to make sure that your employees know how, when and where to deploy and use security measure. In most incidents involving data breaches, an employee or group of employees failed to take actions to prevent or detect the breach, mostly due to inadequate awareness and training. All the technology and policy in the world cannot prevent a breach if people don't know what to do. Failure to train employees, staff, management and others about the new requirements in general and the importance of security and privacy in particular – and how to achieve these security goals – is now a direct violation of the new HIPAA regulations, and can result in enhanced fines and penalties, not to mention loss of reputation and business. Now, not only must covered entities have awareness and training, but all partners must have such training and awareness. Moreover, most data breaches result not from bad technology, but from bad choices about technology, improper deployment of technology, or inadequate attention to potential vulnerabilities or incidents. Implementation of a strong and documented security awareness program will help mitigate these threats and satisfy HIPAA requirements.



SCIPP International offers Security Awareness courses tailored specifically to satisfy HIPAA requirements. All courses are interactive web-based solutions that feature state of the art production capabilities, an unparalleled teaching core of information security luminaries and complete participation metrics for audit support. For more information please visit: **www.SCIPPinternational.org**

SCIPP
INTERNATIONAL™
THE SECURITY AWARENESS CERTIFICATION COMPANY

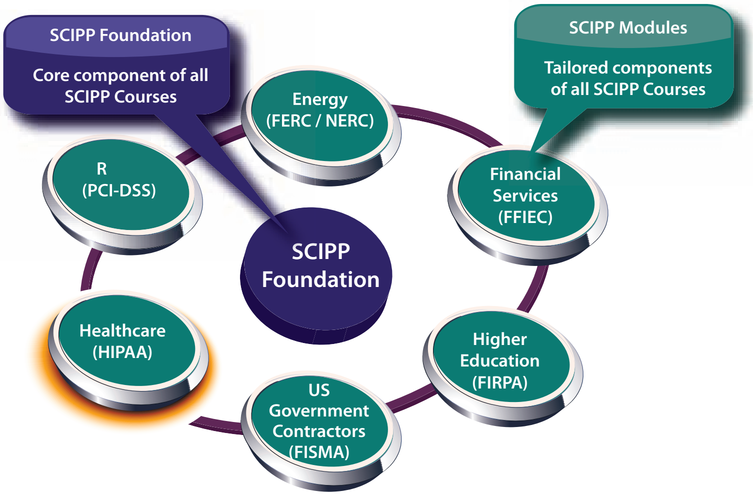
Somebody on your back about annual security awareness requirements?

Annual security awareness training compliance is not only critical to the continued health and wellbeing of your business it is a requirement. SCIPP International can help you to get this monkey off of your back.

Every organization that handles personal data is required by law to provide, implement and track security awareness training on an annual basis - but every industry is regulated differently, so how can you be certain that your company is compliant?

SCIPP International has taken the guesswork out of the compliance equation by developing a world-class security awareness training product suite that will satisfy security awareness training requirements as they apply to specific vertical markets such as healthcare, retail, higher education, energy, financial services and government contractors.

All SCIPP courses are offered as interactive web-based solutions that are tailored to meet industry requirements and feature state of the art production capabilities, an unparalleled teaching core of information security luminaries and complete participation metrics for audit support. **And the best part?** SCIPP International guarantees that its courses meet all known security awareness training requirements within your industry. **What are you waiting for?**



SCIPP Foundation

Core component of all SCIPP Courses

SCIPP Modules

Tailored components of all SCIPP Courses

SCIPP Foundation

Energy (FERC / NERC)

Financial Services (FFIEC)

Higher Education (FIRPA)

US Government Contractors (FISMA)

Healthcare (HIPAA)

R (PCI-DSS)

Contact SCIPP International today to find out just how easy it is for you to get the monkey off your back and implement your tailored security awareness program. **Please visit: www.SCIPPinternational.org**

SCIPP International™

The Security Awareness Certification Company

> “Our strategy is to make sure we can secure the data in the forms it shows up in. The focus is on protecting the data, as opposed to [protecting] the host itself.” – PATRICK HANRION, MICROSOFT

continued from page 12

says. Hoffman ought to know; he identifies himself as an ethical hacker.

Both laptop and mobile device users need limits imposed on their Web surfing. With wireless devices, though, the form factor itself contributes to the problem. Because the small screen can cut off the URL at the top, users have a harder time identifying illegitimate Websites.

In the same way e-mail should be monitored, text messaging must be tracked, both externally to guard against loss of intellectual property, and internally to guard against harassment and other human resources problems.

Another problem area has to do with peripherals. Most wireless devices incorporate cameras, so organizations are increasingly prohibiting their use in the corporate environment. “There are a lot of liability issues with people taking pictures,” says James Naftel, senior product manager for Sybase.

USB storage devices can hold a tremendous amount of data and are hard to track. Storage devices for smartphones and cell phones, such as the microSD card, are even smaller and harder to control. As much as corporations would like to, few have the ability to enforce a ban on consumer technologies such as these.

POLICY MATTERS

Security policies for wireless devices should be similar to those for laptops, and in line with corporate security standards. Companies must block access to public Wi-Fi networks, especially if users are attempting to connect with the corporate network. If possible, mobile device users need to connect to corporate networks over VPNs.

Password protection is a must. Password access on cell phones can be a pain, both for users and for IT support staff besieged by requests for forgotten passwords, but it’s worth the trouble. Encryption is equally important, because mobile workers access and store sensitive corporate data. Encryption protection should extend to wireless storage devices, especially in large companies that struggle to enforce a ban on such technology.

Make sure all smartphones and cell phones go through IT. It’s one thing to keep track of wireless devices when management controls them; it’s another problem when those devices are purchased and controlled by individual workers. It’s essential to have some method of remote control for content filtering, backup and recovery of data, remote lock and wipe, and the ability to shut down certain features such as cameras.

Finally, education is as important an element in wireless-device security as it is with laptops, perhaps more so. Users must be made aware of the security risks associated with their mobile computers. As things stand now, many aren’t.

Apple is the exception that proves the rule. The original incarnation of the iPhone got a bad reputation in the corporate environment for being security challenged. Yet the iPhone is working its way into business through increasingly sophisticated computing capabilities and continuing consumer appeal.

Due in part to complaints from corporate users, last year’s iPhone 3G addressed some of the device’s security limitations, including hooking into Microsoft’s ActiveSync server. But the iPhone is “still lacking in capabilities some enterprises absolutely require,” says Unisys’ Hoff, such as full-device encryption and centralized security management tools. And that’s why many organizations, Hoff’s included, are still pilot testing it.

REFOCUSING AND REORIENTING

There are trends in corporate computing that may help address some mobile security challenges. For example, virtualization technology is finding its way to the desktop. By moving most of the processing and all of the data storage to a central server, virtualization helps mitigate the threat to mobile computing’s most vulnerable element: the end device. Similarly, cloud computing, which taps into data storage and processing taking place in a central, remote, secured location, will help automate and enforce many of the elements of mobile security.

Some security experts suggest the increasing use of mobile computing devices is forcing a rethink of information security strategy. If the first stage had as its focus protecting the perimeter, and the second stage was about securing the host, the third is about protecting data—wherever it resides and in whatever form. “Our strategy is to make sure we can secure the data in the forms it shows up in,” says Patrick Hanrion, CISSP and principal architect in IT security at Microsoft. “The focus is on protecting the data, as opposed to [protecting] the host itself.”

That may require a slightly different orientation for information security professionals. “The device is the vector by which the data leaks,” says ICSA’s Potter. “The real problem is classifying the data. You have to understand what your data is, where it’s supposed to be, and where it really is.”

From that perspective, mobile devices are simply a means to a computing end, as important as any element in the IT architecture. That puts additional responsibilities on both security professionals and end users to make the most of the devices while ensuring the safety and security of the enterprise.

Blame it on Apple.

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

enabling team intelligence

How to enhance team awareness, stability and performance.

By Scott Holbrook

TEAM LEADERSHIP IS challenging, even on a good day with a great group. Leaders are constantly scanning the horizon for strategic input, working to increase customer satisfaction, dealing with operational constraints and handling day-to-day personnel issues. Add in an underperforming team and you have a recipe for frustration that, left unaddressed, becomes a ticking time bomb for everyone involved.

Teams often sabotage their own success by creating artificial boundaries to include their strengths and exclude their weaknesses. This hinders success and often results in a growing chasm between the organization's goals and the team's ability to execute.

The Team Scenario

Teams are a unique mix of players with various talents, including overachievers, underachievers, extroverts, introverts, thinkers and doers. Often leaders have a favorite team, one that overcame all odds to create excellence in spite of seemingly insurmountable obstacles. These groups likely exhibited team intelligence, and created team awareness as individual members learned each other's strengths and developed strategies for success.

In this era of globalization and geographically disparate teams, leaders are no longer afforded the luxury of creating the perfect team from a blank roster. How can they move their teams up the performance ladder? How can they inspire sustained excellence? By nurturing individuals, developing an environment of trust and communication, and enabling team intelligence.

Defining Team Intelligence

Team intelligence is an extension of the concept of emotional intelligence, largely accredited to Daniel Goleman (danielgoleman.info/blog), who has authored several books on the topic, including *The Emotionally Intelligent Workplace*. There are four major components of emotional intelligence:

Self-awareness: being conscious of, and understanding, your emotions

Self-management: controlling your emotions and impulses in a variety of situations

Social awareness: being conscious of, and understanding, how emotions affect others

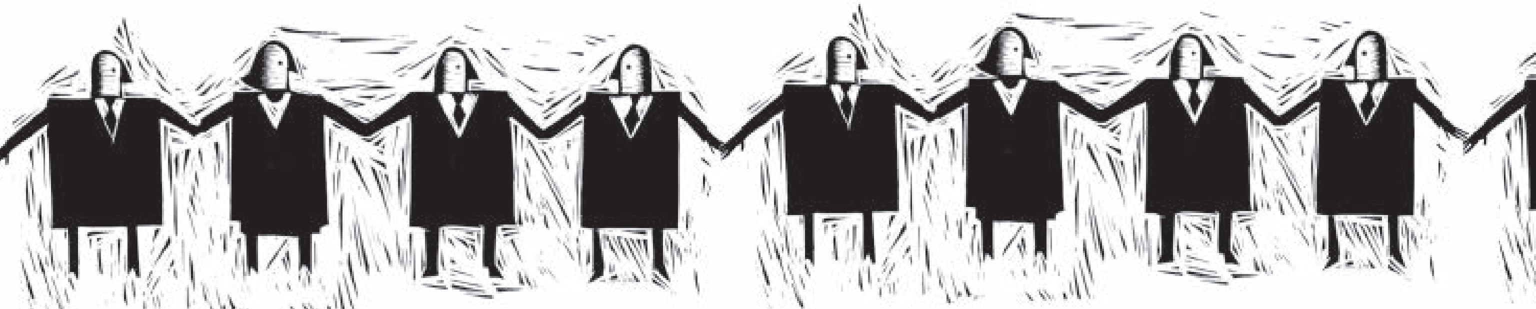
Relationship management: creating and maintaining relationships across a spectrum of social levels; the ability to motivate others even in challenging situations.

Effective leaders begin at the individual level and foster team awareness. This process includes an honest internal assessment of the team's capabilities by the individuals themselves, as well as an external customer's assessment of the same capabilities. Combined with a team-specific focus inventory, a plan of action and built-in reviews, even underperforming teams can achieve growth and move toward sustained excellence.

Start State

First, assess the team's current strengths and weaknesses. Does the team need to develop its communication skills? Does it need to hone its visioning skills? Is the team effective at customer service? Does it have a high level of trust?

ILLUSTRATION BY VEER



Next, discuss the overall strategy for improvement. A focus inventory should be introduced as one of several performance enhancement tools, part of a larger framework for continuous improvement. The focus inventory is a set of skills selected by the team leader indicating the key attributes of a highly performing team. While the inventory can change based on industry, there are certain core skills that should be included, such as communication, teamwork and accountability. It might contain from five to 15 skill areas; the team should select its primary areas of improvement based on the three or four lowest-scoring team skills.

The next step begins with individual, closed-door interviews with each team member. To gather accurate data, create an atmosphere of trust and convey to each person that the focus inventory data is being considered from a team roll-up context. Ask them to rate each focus area on a scale of one to five based on how the team performs in that area. This changes the framework from self-assessment to team assessment. And keeping the rating scale small forces members to carefully consider their choices.

Transition Phase

Once the data has been collected, review it for patterns of strength and weakness. Consider some supporting tools to prepare for a team discussion of the focus inventory results.

Perhaps the best tool to enhance team communications and awareness is the Myers-Briggs Type Indicator (MBTI) assessment. It reveals personal preferences in four quadrants: introversion/extraversion; sensing/intuition; thinking/feeling; and judgment/perception. The assessment is taken individually, and indicates each team member's predilection for interacting with others and the world around them. There are several MBTI assessment questionnaires available online.

The MBTI results can be displayed on a 4x4 grid with the type descriptor. In each block, place the names of the team members whose assessment matches the MBTI type. This provides a unique view of the team, and can be used to help members understand and better communicate with each other.

Growth Phase

During the growth phase, the team evolves from individuals to a cohesive unit. This phase includes the ongoing reinforcement of team awareness, and the creation and validation of the team's vision and goals.

Allow time to create a team vision; getting the group to agree is usually a lengthy and sometimes painful process. Team buy-in to the vision is an essential part of enabling team intelligence. Once the team has developed its vision, make it a stated part of daily life. For example, begin each meeting with the vision statement: Make it rote, and make sure the team is aligned around its meaning.

Review and Feedback Cycles

Periodic reviews are a key component to keep the team moving in the same direction. Determine early in the development cycle how often and what types of feedback will be provided. One way to gather feedback is to use Post-it® assessments. Here, each team member is given a Post-it pad and asked to write answers to specific questions, such as "Where are we succeeding?" and "Where can we improve?" Separate the answers into related groups on a whiteboard; brainstorm ways to celebrate success and cultivate ideas to stimulate progress in areas where the team has stalled. This approach creates team alignment and generates momentum.

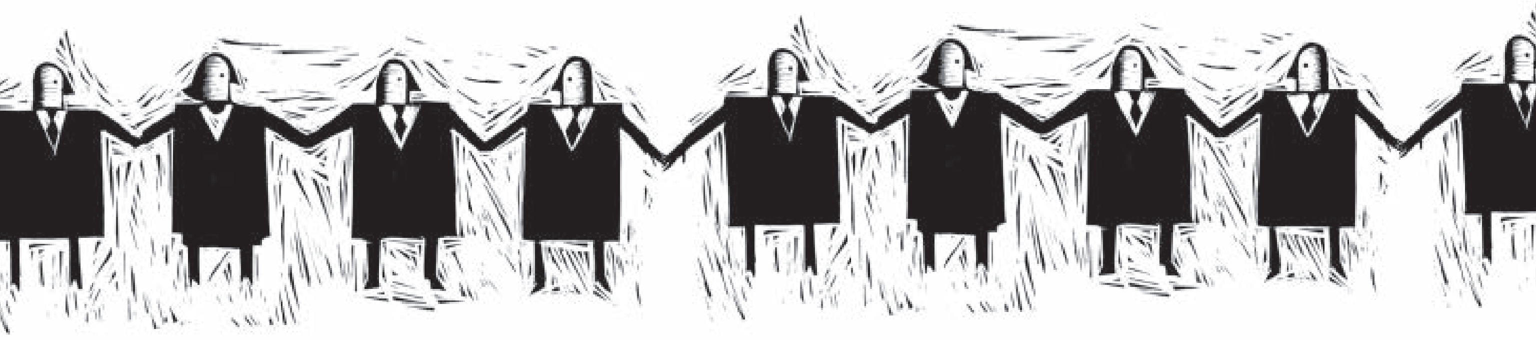
Now it's time to turn the team's intelligence toward solving the customer's biggest problems—those that the team could never have surmounted before the intelligence cycle. The team is now prepared to assess customer needs and apply its newly developed communication and visioning skills to effectively partner with the customer.

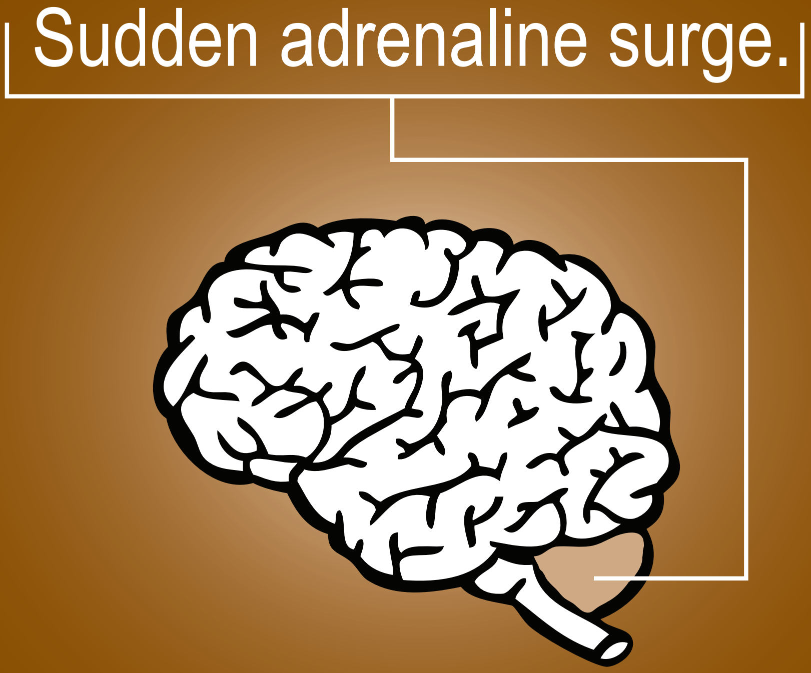
Reflection

Team intelligence is a cyclical process and should begin and end with reflection on the team's performance. Once the team has completed its first evolution of the intelligence cycle, reassess the team goals, revise the focus inventory, determine next steps and restart the cycle with new growth targets. The focus inventory is a useful tool for defining core skills, and when combined with a plan of action and a team commitment to improve, it can serve as a baseline of common understanding.

Identifying strengths and weaknesses alone does not constitute team intelligence but represents the first step on the path toward maximizing team performance. Developing team intelligence takes work, commitment and time on the part of the leader as well as the team. It's important to set realistic goals and allow enough time for changes to yield results. (ISC)²

Scott C. Holbrook, PMP, CISSP, is the manager of Information Security and Disaster Recovery for CaridianBCT, a global medical device manufacturing company. He is based in Colorado.




Sudden adrenaline surge.

At the Head of the Pack

IF YOU'RE LOOKING FOR A NEW JOB, TAKE TIME TO PREPARE AND POSITION YOURSELF. **BY JOYCE BROCAGLIA**

PHOTO BY MOODBOARD/CORBIS

MANY PROFESSIONALS HAVE BEEN AFFECTED by downsizing due to the economic crisis. Jobs are limited and competition is fierce. Consider these tips to put yourself at the head of the pack.

Define your attributes and accomplishments.
Look at your career roles and responsibilities and identify your most significant accomplishments. Determine how they add unique value to each position for which you are applying, and ensure they are depicted clearly, accurately and concisely in your résumé.

Research the organization and make sure you understand its business goals. During the interview, listen closely and ask probing questions. Then find ways to match your accomplishments with the hiring manager's goals. Tailoring your answers to show how you can add immediate value will give the interviewer confidence in your abilities.

Perception is reality.
From the time you submit your résumé until you accept an offer, you are being evaluated by your new employer. Pay attention to the following four areas:

- **Responsiveness.** Once you have been contacted by a recruiter or prospective employer, respond quickly. Lengthy delays in returning emails or phone calls will put you at a great disadvantage compared to other candidates.
- **Communication.** The tone and caliber of your verbal and written communications are indicators of your professionalism. Many positions require interfacing with lines of business, and corporations are sensitive to a person's ability to interact and articulate.
- **Preparation.** Companies expect you to know their history, their competitors and why you want to work for them.
- **Etiquette.** You will be judged by how you interact with everyone you meet—from the administrative assistant to the executive. Never let down your guard, and always remember your manners.

Leverage your network.
Leveraging your personal network can give you a competitive advantage. Many jobs are never advertised—they are filled through personal referrals. Make everyone in your network aware that you are looking for a new opportunity and ask them for referrals.

Your professional network is important, too. It should include your peers, managers, clients, previous employers, memberships and associations. Also, a recruiter can market your skills and increase your chances of successfully landing a position. (ISC)²

Joyce Brocaglia is the founder and president of Alta Associates, a New Jersey-based recruiting firm that specializes in information security, IT risk management and privacy.

The Security Specialist

IONUT IONESCU DESCRIBES THE YEAR AHEAD AND THE OUTLOOK FOR INFORMATION SECURITY PROFESSIONALS.

PHOTO BY GEORGE DIEBOLD

MARKED BY A GLOBAL ECONOMIC slowdown, 2009 will bring changes for the information security professional in three ways: Organizations will outsource more of their security needs; audit and verification will get the upper hand over technical measures; and professionals will have to broaden their skills to be successful.

Organizations in all sectors will bring costs in line with the predicted drop in demand. This should put managed security service providers (MSSPs) and security-as-a-service providers in a good position, provided that they offer clear and fair service-level agreements. If something is noncore to the business, such as security management, and it can be contracted out with reasonable expenditure outlays, it very well could be.

If firms cannot fully avoid capital expenditures, acquisitions of new security technologies will be kept to a minimum, and leasing will take preference over buying. Expect the emphasis to move from having the latest technical wizardry to having "good enough" defense systems, coupled with a thorough audit and verification schedule. IT leaders will have to do more with less, and security will have to prove its worth by getting more out of the audit schedule and requiring less dedicated expenditure. This, in turn, will put pressure on security professionals to adapt.

Those working in professional services firms will have to pick up new skills. Faced with economic contraction and dropping consulting fees, consultants will have to prove their worth by doing more client-billable security tasks.

The same goes for those working in internal security operations positions. Technical specialists will have to focus not only on firewalls, access violation and intrusion prevention systems, but also on router and switch management. Policy and audit professionals must be knowledgeable about several standards and protocols and be able to check technical controls to a certain degree.

For security managers, the key terms are "flexibility" and "people skills." Few organizations can continue to support separate physical security and information security roles. The same applies to technical versus policy roles.

Security professionals will have to turn security into a business enabler. This means speaking with business leaders as often as with law enforcement agencies. Also, it will be critical to combine IT, physical security and facilities threats, and present a coherent view—with a cost-benefit analysis for any suggested countermeasures—to business leaders.

Expect to do more in 2009, but don't wait to be asked what value you provide. Pick up two or three new skills, survey the market for good MSSP providers, and look for synergies with your IT colleagues and get involved in their projects. Above all, understand where the business is going, what the challenges are and the outlook for the next 12 months. (ISC)²

Ionut Ionescu, CISSP, CISM, GSEC, is based in Germany and works for Nortel Global Services as director of security services, Europe, Middle East and Africa. He is a member of the (ISC)² European Advisory Board.

SECURITY VULNERABILITIES ARE RARELY DUE TO A SINGLE, CARELESS MISTAKE.

Accident or Incident?

RESIDUAL SECURITY RISKS ARE INHERENT IN ANY SYSTEM. STUFF HAPPENS. **BY FRANK KOERNER**

THE WORD "ACCIDENT" IS RARELY USED with regard to computer security problems; the word "consequence" is more appropriate. Accidents happen due to unforeseeable, unpreventable events. Consequences are the logical results of certain actions, and consequences are preventable. To measure a system's security is to answer this question: With respect to what? You must ensure that the system complies with its associated security policy and requirements.

Despite this roadmap, security incidents regularly occur. One reason often given is that development using plug-and-play components occurred before security policies and requirements were defined. Or there wasn't enough time or money to "do it right." Neither explanation is correct. Security incidents are the preventable result—or consequence—of a string of bad human choices that disregard classic principles of sound engineering judgment.

Security vulnerabilities are rarely due to a single, careless mistake; they are often the result of a confluence of circumstances. This makes 100 percent secure systems impossible to attain. There are always residual risks. Stuff happens.

The complexity of security choices is exacerbated by the overlapping nature of security disciplines, which consist of the protections of hardware, software and firmware remedies, which consist of communications, physical security, operations, emanations, personnel and administrative measures. Each discipline is incorporated into a system's security design; the art of security lies within their interrelationships. For example, technical remedies might have an administrative or procedural element or vice versa. A minor IT weakness might have major emanations, or their separate, major impacts might nullify each other.

That is why across-the-board analysis needs to be enforced at every system decision point. Each point doesn't come labeled with warnings such as, "If mixed with elements B and C, this will become a major security vulnerability."

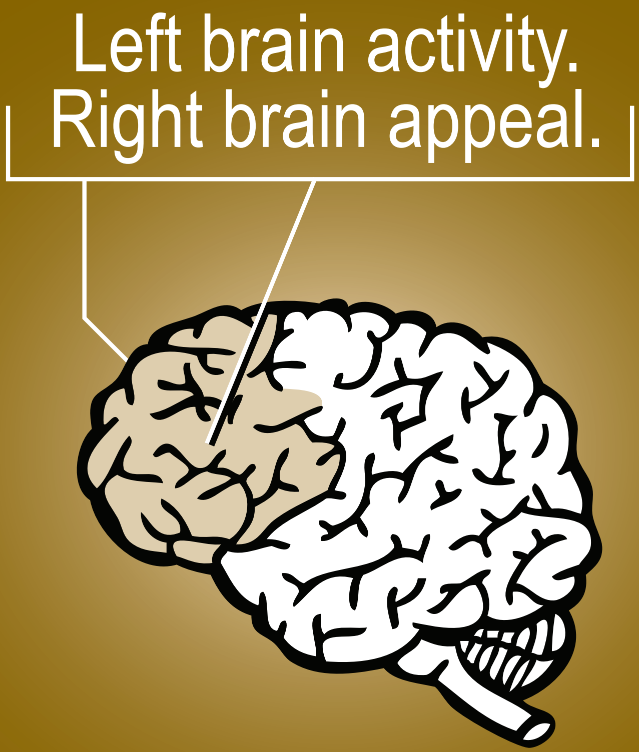
The elements of a security incident may appear insignificant when viewed individually, but they take on new meaning when looked at as potential links in an inherently unpredictable chain of causation. This chain is often buried among the post-incident debris, becoming visible only after extensive analysis. Our reasoning process must be inductive as well as deductive—that is, we must ask questions such as, "How did we get here?" and "Where do we go from here?"

It's been said that the road to hell is paved with good intentions. The road to security incidents is often paved with them as well, along with engineering judgments that in isolation look acceptable. Only by fully examining such incidents can we determine if they are accidents—unforeseeable and unpreventable—or the consequence of a system engineering process gone awry. (ISC)²

Frank Koerner, CISSP, is a senior security engineer at Science Applications International Corp., based in California. He is a member of the Health Systems Business Unit, Healthcare Systems Integration, IT Support and Field Operations Group.

ILLUSTRATION BY CAMPBELL LAIRD/VEER

Social skills and the ability to play well with others.


Left brain activity.
Right brain appeal.