

Info Security

PROFESSIONAL®

ISSUE NUMBER 7

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



Ethical Choices

A code of ethics guides information security professionals in the protection of data

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.



where secure minds meet

issue 7

2009 VOLUME 3

12

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

[features]

8 **Ethical Choices**

Information security professionals must be aware of their ethical role in the protection of data.

BY EFRAIN VISCAROLASAGA

12 **Hard Targets in Software**

Fundamental problems within the software development lifecycle are causing holes in applications.

BY JOHN SOAT

16 **Professional, Beware!**

Read up on the latest trends in financial high-tech crimes.

BY RAJ GOEL

[also inside]

2 **Inbox**

Feedback and Suggestions Readers share their thoughts and suggestions.

3 **Raising Awareness**

Executive Letter From the desk of (ISC)²'s executive director. BY W. HORD TIPTON

5 **FYI**

Member News Read up on what (ISC)² members worldwide and the organization itself are doing.

18 **Reasons for Change**

Career Corner Advice from a recruitment professional toward furthering your career. BY BARCLAY SIMPSON

20 **Securing Cyberspace**

Global Insight International perspective on the pressures facing today's information security professionals. BY ALBERT LEWIS





Letters to the Editor

A part of my duties in the company is security awareness. I read an article in *InfoSecurity Professional* titled "Googling Security and Privacy" (p. 16, Issue 6), written by Raj Goel. I'm interested in taking some parts of the article, translating to Spanish and using it for part of our security awareness program.

Please let me know if it is possible.

EMILIO CASTILLO, CISSP
LEADERSHIP RISK ASSESSMENT
MEXICO CITY, MEXICO

(ISC)² responds: Thank you for wanting to share this information with your colleagues. We do allow our members to use information from this magazine

for these purposes. We ask that you use proper attribution and please let us know how it will be used.

I just found these magazines and like what I have seen so far. I just got an iPhone at work and having these magazines available in eReader or ePub format would be a huge value add!

ED DAVISON, CISSP
MANAGED NETWORK SECURITY
TEXAS, USA

(ISC)² responds: To view the magazine on your mobile device, go to www.isc2.org, login with your member ID, then click on the magazine issue link. You will be taken to the online platform where you can read InfoSecurity Professional on your mobile device.

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

Mary Lester
Executive Director, Art and Design

Kim Han
Art Director

Lisa Stevenson
Associate Production Manager

CSO
Custom Solutions Group

ADVERTISER INDEX

CA	p. 4
IEEE	p. 10
ISACA.....	C4
(ISC) ²	C2, 7, C3
Norwich University.....	p. 14
SCIPP.....	p. 19

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

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

<http://tinyurl.com/mcplxb>

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

executive letter

FROM THE DESK OF THE (ISC)² EXECUTIVE DIRECTOR

Raising Awareness

(ISC)² CALLS FOR ITS MEMBERS TO BECOME AMBASSADORS OF CYBERSECURITY AWARENESS.

AS INFORMATION SECURITY PROFESSIONALS, we deal with security issues from the top to the bottom of our organizations. So it's no surprise to hear that more than half of all security threats come from insiders and end users—often unintentionally—who inadvertently visit unsafe Websites, open emails with viruses and so on.

These threats can quickly cause big headaches in terms of financial and legal liabilities. They also increase the risk of data breaches, as well as the amount of work that must be done to repair damage and absolve vulnerabilities.

Based on our education and expertise as information security professionals, we have a wealth of knowledge about these issues and the potential problems these threats cause. That's why it is imperative that we become ambassadors for information security. We need to reach out to children, adults and everyone in our local communities to bring a message of information security awareness.

(ISC)² takes this responsibility seriously. We have undertaken several public awareness initiatives—for example, Safe and Secure Online (a program aimed at keeping children safe online) in the United States and United Kingdom, and a similar program, along with police training, in Hong Kong.

We encourage you to get involved! There's no

better time than now, as October marks National Cyber Security Awareness Month. It was begun in the United States in 2001, and (ISC)² celebrates it globally.

We've recently revamped our Cyber Exchange (<https://cyberexchange.isc2.org>), an online portal where you will find free valuable resources—posters, presentations and videos—that you can share with your local community. This site now encompasses our overarching public awareness efforts, including (ISC)²'s Safe and Secure Online program, where our expert members can volunteer to educate children ages 11 to 14 about the importance of protecting themselves online.

Finally, we hope all members will participate in our 2009 board of directors elections. Voting begins on November

16, so please take a few minutes of your time to have a say in (ISC)²'s direction and leadership.

Sincerely,



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



**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.

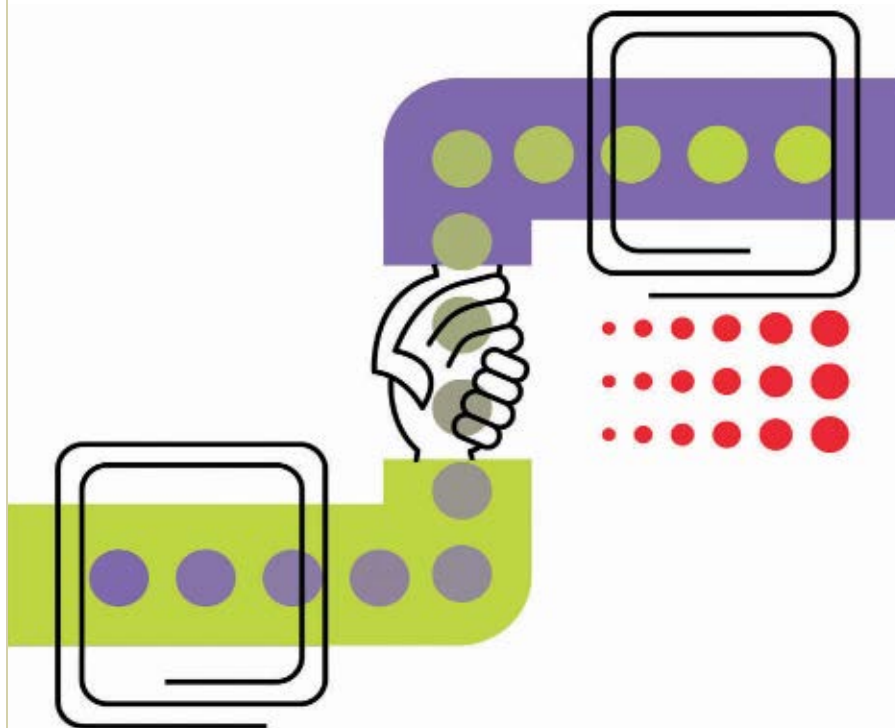
Learn more at ca.com/security

Copyright © 2009 CA. All rights reserved.





(ISC)²
MEMBER
NEWS



Shake Hands Around the World

(ISC)² HAS launched its own professional networking site, called InterSeC. The site has been designed for (ISC)² members; however, eventually it will be open to professional members of the whole information security community and associated disciplines.

InterSeC offers opportunities to share knowledge and build virtual groups based on your needs, interests and capabilities.

(ISC)² members have requested chapters for quite some time. With the recent social networking boom, we have created a virtual outlet that

we hope will be a welcome substitute for official chapters.

You'll find it easy to use and intuitive. Although all social networking sites work in a similar fashion, this site is designed so that users can easily find other professionals with similar interests—by topic, geography, vertical markets and so on—and facilitate interaction and collaboration. We hope you'll take advantage of this new member benefit!

To join the site, go to the (ISC)² member home page (<http://members.isc2.org>) and click on the InterSeC logo.

Raising Awareness

EVERY OCTOBER is National Cyber Security Awareness Month in the United States, yet we celebrate it globally at (ISC)². This year's theme is "Our Shared Responsibility." To help drive this message home, (ISC)² ran its annual Cyber Exchange contest. Thanks to those of you who participated this year. The winners will be announced at the end of September on the member Website.

The Cyber Exchange (<http://cyberexchange.isc2.org>) houses materials that you—the preeminent information security experts of the world—donated for the public good. Anyone can download these materials for free and use them in their local communities.

Even though the contest is over, you can share security awareness resources and help spread the word that information security is everybody's business and responsibility. At any time, you can upload your expert, original cybersecurity awareness presentations, flyers, posters, etc.

2009 Asia-Pacific ISLA Program a Success

THE (ISC)² Asia-Pacific Information Security Leadership Achievements (ISLA) program annually recognizes outstanding leadership and achievements in the workforce improvement of IT security professionals throughout the Asia-Pacific region in three distinct categories. This year's ISLA ceremony was held on July 8, in conjunction with the Malaysia Cyber Security Awards in Kuala Lumpur, Malaysia, where 21 honorees were recognized for their contributions to the advancement of the IT security profession. Three in particular were showcased:



IT Security Practitioner: HyunCheol Jeong, CISSP, Director of the Security Technology Department at the Korea Information Security Agency. Jeong is in charge of the development of information security technology, domestic and international standardization business, and the study and distribution of

encryption technology. He is also in charge of standardizing cyber security in Korea by acting as chair of the Telecommunications Technology Association. Jeong was recognized for developing the first security program in Korea and for encouraging his team members to be innovative leaders.



Senior Non-IT Security Professional: Gerard Tan, Partner-Advisory, PriceWaterhouseCoopers LLP in Singapore. Tan has 30 years of experience in financial and technology audit and advisory services. He leads the System and Process Assurance and Business Continuity Planning practices for PwC

Singapore. He is currently the president of the Association of Information Security Professionals (AISP). The ISLA program recognized him for this honor because he leads by example and encourages people to work together as a team to achieve a common goal. Tan took on the role of president for AISP at the most critical moment during its formation and molded the interim executive council into a cohesive, working unit and defined its roles and responsibilities.



Senior IT Security Professional: Retired Lt. Col. (R) Husin bin Jazri, CISSP, CEO of CyberSecurity Malaysia. Husin Jazri has more than 20 years of experience in information and communication systems security obtained from military service, working with research institutions and the government agencies

of Malaysia. He has been a visiting lecturer on the subject of information security at the University of Technology, Malaysia, since 2004. He was honored for his dedication to cyber security and for elevating the profile of CyberSecurity Malaysia to be the one-stop coordination center for all national cybersecurity initiatives in Malaysia.

We congratulate all current and past honorees of the ISLA program. For more information, visit www.isc2.org/isla.

Remember to Vote

VOTING for the (ISC)² Board of Directors will take place in November. Members in good standing as of July 16, 2009, will be able to cast their votes from Nov. 16 to Nov. 30. Results will be announced in December.

(ISC)² is a global not-for-profit organization governed by a member-elected Board of Directors. The Board consists of top information security professionals representing a wide variety of countries and organizations. Board members provide strategic governance and direction for the organization.

Your participation in this board election influences the direction and leadership of (ISC)², so please be sure to vote. For more information, visit <https://www.isc2.org/board-election-process.aspx> or contact bodelections@isc2.org.



ISACA recently recognized (ISC)² with a Partner Organization Award.



**Mother Nature doesn't
take security lightly
and neither do you.**



In the software world, our creations are vulnerable and the threats are just as real. Give your software some teeth and be ready for any attack. Take the lead in making sure security's built into every stage of the software lifecycle by becoming an (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP^{CM}). Learn how security should be baked into the software lifecycle – attend a CSSLP Education Seminar. It'll cover how to build security into each phase. Mother Nature gives every member of the animal kingdom ways to protect itself. Every stakeholder in the SDLC needs to do the same. **Become a CSSLP today!**

**Register for
the CSSLP
Education Program**

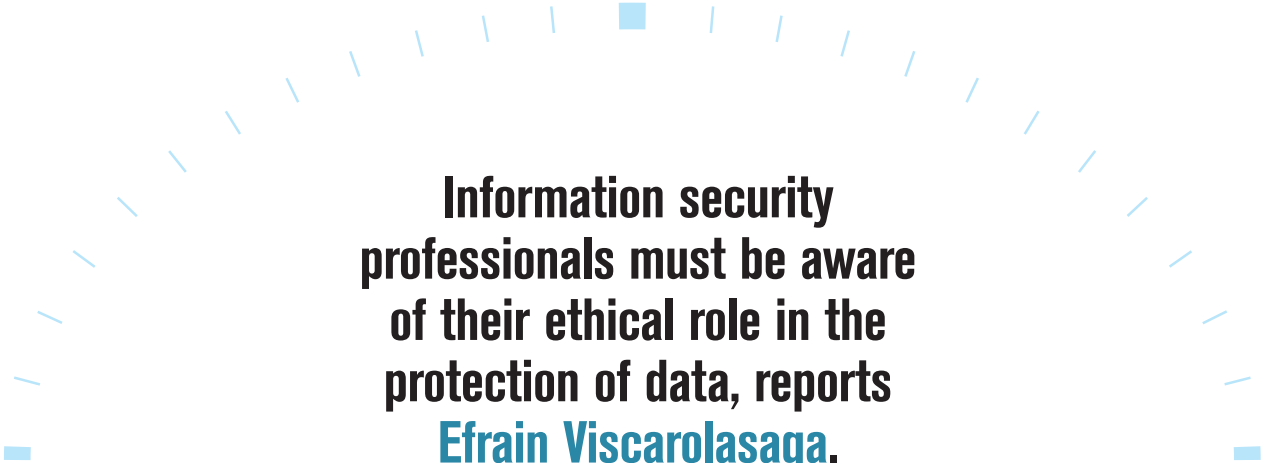
Start Here.

www.isc2.org/csslpedu

ETHICAL CHOICES

WRONG | | | | RIGHT





Information security professionals must be aware of their ethical role in the protection of data, reports Efrain Viscarolasaga.

Ethics plays a crucial role in many industries where professionals deal with sensitive information, from doctors and lawyers to journalists and engineers. But while the basic tenet of ethical codes—“do the right thing”—is universally accepted, each discipline brings countless variables and details specific to its particular industry, requiring unique and evolving guidelines to ensure that the interests of all parties, including society at large, are protected.

The information technology field is no different. Data has become a crucial element of society’s day-to-day operations, making it paramount that information security professionals behave ethically.

The IT industry’s ethical operations are similar to those of more traditional engineering practices, says Stuart Shapiro, CIPP/G, principal information privacy and security engineer at government nonprofit technology organization MITRE Corp. in Massachusetts.

“If you look at formal codes of ethics, I don’t see the field of information security as being that different from other engineering fields,” he said. “You see codes of ethics in other engineering fields, and they have similar premises: responsibility to privacy, responsibility to the client, responsibility to the employer and responsibility to society at large.”

WHAT IS ETHICAL?

While “do the right thing” serves as a starting point for ethical behavior in any environment, it’s more appropriate to discuss what *isn’t* ethical behavior.

According to W. Hord Tipton, CISSP-ISSEP, CAP, CISA and executive director of (ISC)², examples of unethical activities in information security include attaching a weak system

to the public network, associating with individuals whose practices may harm the industry or lying about the details of a security breach.

Tipton recounts the story of an information security professional hired to perform an audit of a company’s security infrastructure. During the audit, the individual found some problems and reported them to the client. However, the client liaison was unwilling to pass the information along to superiors, clearly a breach of ethical conduct. Eventually, the professional disclosed the problems to the appropriate personnel.

While the primary function of information security professionals is to build and maintain a secure digital environment and protect the company from attack, they are also responsible for the data residing on those networks. According to Larry Ponemon, CIPP and founder of digital privacy research group Ponemon Institute, the responsibility of maintaining ethical standards when managing digital data falls on the shoulders of a company’s digital security leader.

“Your job is not only to ensure your company holds a good security posture but that it is not taking advantage of the data it has on hand,” says Ponemon.

Ethical problems arise when the interests of one or more of those constituents come into conflict with each other. The

difference in the information security industry, he says, is that in many cases, the IT industry deals with abstractions and does not have the history of hard data to refer to; this places more significance on the ethical decisions of security professionals.

Shapiro uses the construction of a bridge as an example. If an engineer wants to build a bridge one way and the client wants it built a different way, one that the engineer believes is unsafe, the engineer has the entire history of bridge building to cite, as well as the laws of physics, to support his decision. In the information security industry, the lines are not as clear-cut.

“We are developing that body of evidence, but we’ll never have something as concrete as the laws of physics,” he said. “Ultimately, it is going to be the individual engineer or professional faced with taking a particular course of action, and it will end up being that person’s decision that will tell the tale at the end of the day.”

THE CODE

By and large, information security professionals are guided by the Code of Ethics developed by (ISC)². No one can be certified by the organization without studying and understanding the organization’s code of ethics, which cites four tenets:

1. Protect society, the commonwealth and the infrastructure;
2. Act honorably, honestly, justly, responsibly and legally;
3. Provide diligent and competent services to principals; and
4. Advance and protect the profession.

(ISC)² also has a procedure for filing and judging complaints against individuals and companies who violate the Code and fail to act in the best interests of the information security industry. Punishment under (ISC)²’s guidelines can range from a letter of reprimand to the wholesale revoking of certification.

But while Tipton and (ISC)² point to these tenets as a foundation for ethical behavior, they acknowledge that no such code can cover all the possible conflicts. In the end, an organization’s adherence to ethical standards lies in the trust it puts in its information security professionals.

“You can have conflicting objectives from different areas. Accounting may want one thing, while engineering may want another,” says Dorsey Morrow, CISSP-ISSMP, general counsel for (ISC)². “Those kinds of dilemmas and those kinds of priorities need to be made by a qualified IT security professional in whom the organization has placed its trust.”

Morrow also points out that the Code is not meant to create or even guarantee ethical behavior but to solidify it to provide professionals with a reference point when problems arise.



Have you gained access to Biometrics Certification?

Access is now being granted to qualified Biometrics Professionals.

IEEE, along with some of the world’s leading biometrics experts, has developed a new certification and training program for biometrics professionals and their organizations. The IEEE Certified Biometrics Professional™ (CBP) program focuses on the relevant knowledge and skills needed to apply biometrics to real-world challenges and applications.

- **Certification:** Earning the IEEE CBP designation allows biometrics professionals to demonstrate proficiency and establish credibility.
- **Training:** The IEEE CBP Learning System combines print materials and interactive online software – ideal for job training, professional development, or preparing for the CBP exam.

To gain access to more details, visit
www.IEEEBiometricsCertification.org.



WHERE ETHICS MEETS PRIVACY AND SECURITY

Ethics in information security deals with everything from managing physical infrastructure to accurately disclosing security breaches. But when it comes to dealing with individuals' personal data, ethics becomes intertwined with privacy.

According to Peter Kosmala, CIPP and assistant director of the International Association of Privacy Professionals (IAPP), ethics and privacy may cover different areas and operate a bit differently, but each relies on the other to maintain security.

"There is this inherent ethical component that goes with privacy," he says. "Privacy goes to the deepest level of the actual holding of information, while ethics layers over both security and privacy."

As the use of private data has grown exponentially, an array of governmental agencies and industry organizations have developed new laws, codes and rules for ensuring individuals a certain level of privacy pertaining to personal electronic information. While specifics vary from region to region, it is generally accepted that three concepts hold true throughout the privacy world: notice, consent and access.

NOTICE: Users and consumers should be given clear notice about how their personal information will be used when a company requests such information.

CONSENT: Users must be asked for, and give, their consent for their information to be used for secondary purposes. Consent is the basic tenet behind opt-in/opt-out rules.

ACCESS: Individuals must be able to access or view their information and to dispute that data's accuracy and completeness.

A final tenet is data security, which refers to the integrity of the data management system and the ethical behavior of its professionals.

"The guidelines themselves are a framework from which the laws are built," says Kosmala, whose organization has certified more than 6,300 privacy professionals worldwide.

But with the basic principles in place, the specifics are constantly evolving. For example, earlier this summer, digital privacy advocate Larry Ponemon met with security and privacy industry members and drafted what is tentatively called the "Archer-Ponemon Treaty for Data Governance," with the goal of creating an industrywide treatise for information privacy.

While Ponemon's document is still in its draft form at the time of this writing, he is asking for industry comments. The document can be seen in its entirety on his blog at www.ponemon.org/blog/post/archer-ponemon-treaty-for-data-governance.

In addition, companies can add another layer of detail by incorporating their own guidelines for ethical behavior. MITRE, for example, has implemented a series of ethical guidelines for its IT and information security professionals, according to Shapiro. Many of them drill into the specifics of how data is handled in the organization, including when data is in transit and guidelines around access control.

"If you put these to any information security professional, they are going to say, 'Of course you do that,'" says Shapiro. "But we think it's important to have them codified so that as you go about

your day-to-day work, you have a point of reference to guide your choices."

THE FUTURE

With rapidly rising volumes of data, increasing numbers of malicious attacks and the rise of new online environments such as social networks, the role of ethical principles in the day-to-day operations of information security professionals is becoming more crucial. However, while the complexity is changing, the basic ethical issues remain similar, and that is keeping the (ISC)²'s Code intact.

"With the rapid growth of our group

and our monitoring of ethical standards, the ethical questions we run into have not changed as much as the number of people and organizations we are overseeing," says Tipton.

Tipton also points out that increasing globalization is putting its own stresses on the ethics of IT. Regions such as China and India come to the table with different cultures, adding confusion to the perception of right and wrong. (ISC)² is reviewing such issues and will address them specifically in the future.

As a result of the industry's expansion and increasing concern with security, individuals who were once focused solely on the technology side of security are finding themselves more involved in the corporate policy side of business. MITRE's Shapiro, who previously taught computer ethics at universities, says this is a good thing.

"What you get when you don't have this kind of [ethics] training is people who enter the workforce and believe, or can end up believing, that ethical and policy questions are not their domain," he says. "But policy is not just someone else's problem. Part of being a professional is that you are aware of and think about the context in which you work. I feel strongly that any IT curriculum is lacking something if it doesn't have some kind of course on ethics—not just computer ethics that revolve around hacking and intellectual property rights, but the ethical behavior of an IT professional."

Ethics training and the parameters laid out by (ISC)²'s Code of Ethics are valuable tools in helping information security professionals do the right thing. Ultimately, the choice is up to you. (ISC)²

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

Further Reading

To read more about the general spirit of "doing the right thing," read Bruce Weinstein's book *Life Principles: Feeling Good by Doing Good*, which explores the principles of ethics, sample ethical conflicts and solutions to common problems.

HARD TARGETS in Software

IN THE EARLY 1990s, when Jim Molini was the computer security coordinator for the space shuttle's onboard flight software development team, he and his NASA colleagues came to the conclusion that the application modules they were working on didn't need extensive security measures because they existed "in a controlled environment." Instead, explains Molini, CISSP, CSSLP, now senior program manager in the identity and security division at Microsoft, they built security "all around that environment."

Today, the controlled interior of the space shuttle may be the only place where application security doesn't need to be a priority. Retail businesses, government agencies, financial firms, media companies and even non-profits are under attack. Security experts, research groups, standards bodies, professional organizations, consultants and vendors all point to application security as a problem for any organization doing business on the Internet. Translation: All organizations need to be concerned.

FINDING VULNERABILITIES

Information security professionals have spent years locking down networks with firewalls and intrusion-prevention technology. Even desktops have been secured with anti-virus and anti-malware software. The next logical area for hackers to pursue was the application layer.

"Over the last 15 years, we've spent a lot on improving infrastructure," says Joseph Feiman, a research vice president at research firm Gartner, who specializes in application security. "Hackers have raised their level of attacks to the application level."

There's also the money factor: Web applications are often the gateway to customer data or corporate intellectual property. "It's the most profitable way for hackers to make money," Feiman says.

Vulnerabilities in Web applications make up the vast majority—75 to 80 percent, according to security services firm Cenx Inc.—of the security flaws on the Internet.

And according to the most recent top 10 lists by the Open Web Application Security Project (OWASP), the three most prevalent Web application security problems are:

cross-site scripting (XSS)—allows an attacker to execute script in a victim's browser;

Hackers are exploiting
holes in software
applications because there
are fundamental problems
within the software
development lifecycle.
John Soat investigates
solutions to this problem.



injection flaws, in particular SQL injections, whereby an outsider inserts data into a database query; **malicious file execution**, which embeds and executes hostile code on a vulnerable Website.

SUBTLE DISTINCTIONS

These days “very few applications are not Web applications,” says Mandeep Khera, chief marketing officer at CenZic. As more commercial interactions and business processes move to the Internet, more software is being hard-coded with Web connections. “All applications are becoming HTTP enabled,” he explains.

This distinction also can be expressed as the difference between internal-facing and external-facing applications. E-commerce applications are external-facing, as are most systems that support customers, partners and suppliers. Internal-facing applications are the HR and financial systems that companies use to support employees and pay bills. Generally speaking, external-facing apps are more likely to be targeted by outsiders seeking to gain access to valuable data or electronic real estate.

So does that mean the accounting application tucked away in a back office is immune from security problems? It used to, but not anymore, says John Dickson, CISSP, owner and principal of Denim Group, a security consulting firm. That’s because devious or malcontent employees are as malicious as external ones, if not more so. Internal databases contain proprietary customer or employee data that has value in the thriving black market for personally identifiable information.

Another subtle distinction involves the difference between application security and software security. The former refers to discovering and dealing with problems in applications that are deployed and in production; it involves tactics such as risk assessment and remediation. Software security speaks directly to people involved in the software development lifecycle.

The fact that universities and their computer science departments aren’t teaching the fundamentals of secure application development is a common refrain among industry insiders. In a

blog last April titled “The Supply Chain Problem,” Mary Ann Davidson (<http://blogs.oracle.com/maryann davidson/2008/04/08/>), chief security officer for Oracle, wrote: “There is no ‘secure development lifecycle’ in the vast majority of universities’ degree programs—security is not ‘baked into’ graduates of relevant programs (e.g., computer science) throughout their degree programs. And that is a problem, perhaps *the* problem plaguing the software industry.”

The good news is that the biggest change regarding application security is awareness, says Mike Puglia, director of product marketing for Veracode, a security services company. The bad news, he says: “Awareness is a lagging indicator of the problem.”

TAKING RESPONSIBILITY

Most IT professionals know that there are security vulnerabilities in the applications their organizations purchase. For



USE YOUR CISSP TO SAVE TIME AND MONEY.

Qualify and redeem one seminar waiver for a savings of approximately \$5,000. This program can be completed in as little as 15 months.

Developed and taught by leaders in the field and backed by 189 years of academic heritage, this program enhances your technical and business management expertise as you gain consultancy experience through an organization-wide integrated information security project. Customize your degree with a specialization in either Business Continuity Management or Managing Cyber Crime and Digital Incidents.

Norwich University was among the first 23 institutions to receive the National Security Agency’s designation as a Center of Academic Excellence in Information Assurance Education.

To learn more please visit
www.msia.norwich.edu/isc



NORWICH
UNIVERSITY™

Expect Challenge. Achieve Distinction.



“There are things you can find with a tool and things you can’t. At the end of the day, that tool is not going to completely safeguard your organization.”

— TOM BRENNAN, CISSP, WHITEHAT SECURITY

example, many network managers and systems administrators mark the second Tuesday of every month on their calendars as Microsoft’s “Patch Tuesday.”

Information security professionals must ask vendors the hard questions. “Ask what their security development lifecycle is,” Molini says. “Ask what kind of security mechanisms they include with their software. Ask if they can provide an integrated and hacker-resistant authentication system for the software.”

Apply that same level of scrutiny to open-source software or shareware tools. This is especially true if open-source software is incorporated into products marketed to customers. Inadvertently incorporating application vulnerabilities could open companies to liability issues.

As for in-house-developed software, information security professionals must get a handle on potential vulnerabilities in applications their organizations have in production. Security managers should embrace “an approach based on risk,” says Denim Group’s Dickson. “Fix what you can and remediate what you can, if you can afford to do it.” Though it is costly and disruptive to yank applications if they are security risks, companies have to do something about them. “Consider end-of-life-ing certain ones,” he says, or at least “accelerating the decommissioning” of those applications.

INCREASING EMPHASIS

There is a growing market for technology that addresses problems with application security, aided by an increasing emphasis on the part of regulators. For instance, some regulatory bodies, such as the Payment Card Industry Security Standards Council, recommend the use of Web application firewalls.

A Web application firewall, also called an application-level firewall, sits in front of an application and enforces security policies to block potential attacks. It can come in the form of software, or as a hardware or software appliance. Web application firewalls are particularly

effective as a tactical way to address potential vulnerabilities. “If you already have an application in place and people are using it, you can’t shut it down,” says Anshuman Singh, product manager for the Web application firewalls at Barracuda Networks.

An emerging product category is application hardening and shielding. A set of technologies from either a single vendor or vendors in partnership, it inserts security functions such as sophisticated encryption and obfuscation directly into applications, generally after coding is complete but before deployment.

Some application security service providers market a variety of services, from risk assessment and remediation to training and staff augmentation. Most also offer application testing and code reviews to determine where security vulnerabilities exist. These tests can be conducted on applications that are idle, known as static application security testing, or those that are running or in production, called dynamic application security testing.

Still, take caution: “A fool with a tool is still a fool,” says Tom Brennan, CISSP, security strategist with WhiteHat Security and a global board member of OWASP. Brennan’s company offers a testing tool of its own, along with other security services, so he’s criticizing not the technology but the potential for too much reliance on it. “There are things you can find with a tool and things you can’t,” he says. “At the end of the day, that tool is not going to completely safeguard your organization.”

PROCESS CHANGE

The bottom line is, software development has to adapt. Organizations must examine and in many cases alter their software development practices with application security in mind.

To that end, (ISC)² offers a software security certification, the Certified Secure Software Lifecycle Professional (CSSLP^{CM}), which is intended for people involved in the software development

lifecycle. The program addresses security concepts related to all aspects of software development: requirements, design, implementation, testing, acceptance, deployment and maintenance.

Information security professionals should encourage secure software development practices. If that means partnering with the company’s code experts, do it. Also, familiarize yourself with the rudiments of application development. “Knowing the nomenclature is important,” says Dickson, as well as “knowing what meetings to get invited to.” The earliest design meetings are the most important, he says; there you can discuss security compliance on a strategic level.

“Someone has to break down that barrier between development and security,” says Microsoft’s Molini, who helped develop the CSSLP and was the first recipient of the credential. “The software they’re developing is more at risk today than it was five years ago because attacks are being focused on that software.”

For information resources concerning Web application security, a good place to start is OWASP (www.owasp.org), which describes itself as a free and open community focused on improving the security of application software. “OWASP is making great strides in getting vendor-agnostic material injected into educational institutions,” board member Brennan says.

The current problems with application security are indicative of a necessary change in security thinking, from a defensive posture to a proactive and strategic stance. “We spent 15 years in the wilderness following the hacker mentality,” Molini says. “That was the wrong way to go about it.” (ISC)²

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

For valuable insights and interesting discussions about security issues, visit Jim Molini’s blog: www.codeguard.org/blog.

MALICIOUS ATTACKS ON DATABASES and incidents of online and other tech-related thefts continue to evolve in number and manner—leaving both consumers and businesses scrambling to pay for the damage to their reputations and bottom lines. The Identity Theft Resource Center reports that in the first half of 2009, 18.4 percent of all breaches were from insider theft. That's up from 15 percent in 2008 and 6 percent in 2007. During the same period, the ITRC reports that hacking totaled 18 percent

of all data breaches, compared with 11.7 percent in 2008. Combined, these malicious attacks are up more than 10 percent in 2009, with data breaches and insider theft accounting for 36 percent of the 250 reported breaches this year.

Information security experts, including ITRC, say companies must implement effective data-protection policies and

pant because so much of the information required to commit ID theft is available online due to inadequate controls, data leaks or human behavior.

For instance, ITRC reports that as of June 15, 2009, only 0.4 percent of all breaches involving laptops or other portable storage devices had encryption or other strong protection methods in use. Another 7.2 percent of reported breaches had data password protection. That leaves 92.4 percent of sensitive data with no protection at all. And ITRC reports that many of these breaches are

ITRC suggests any entity that requests personal information should have the technology and policies in place to limit access of sensitive information. For instance, companies can set up verification systems so that a consumer should not be asked for his or her Social Security number to view, for instance, a current balance.

GLOBAL SUPPLY CHAIN RISKS

Fake receipts and counterfeit gear are just a couple of examples of crimes that have swept through global supply chains. Fake receipts include everything from fake ticket stubs and railway passes sold online by unscrupulous companies to fake restaurant or taxi receipts turned in by unscrupulous employees looking to pad expenses.

One recent business scammer fraudulently raised \$50 million from local investors by using fake receipts to support a lie about the number of existing U.S. customers signed on with his business. In another case, Chinese authorities reported seizing several warehouses



PROFESSIONAL,

High-tech professional criminals are getting ever more clever, says **Raj Goel.**

systems to safeguard their businesses and customers. Knowing what you are up against is a solid start in planning a defense against would-be thieves—from both inside and outside your company.

What follows are some of the latest trends in information security breaches and technology-related theft examples that hold valuable lessons for information security professionals.

IDENTIFICATION THEFT

Identification theft continues to run ram-

peated events affecting the same company or agency.

PrivacyRights.org reports that between 2005 and 2009, companies reported losing more than 431 million data records, primarily those of U.S. citizens. Stolen personal information has, in turn, created a vast black market for hijacked credit card numbers and bank account credentials. As of April 2009, Symantec reports that hijacked credit card numbers were being sold for as little as 6 cents per card in lots of 10,000.

full of fake receipts worth an estimated \$147.3 billion dollars.

Another booming criminal business is the production and sale of counterfeit technology. For instance, the U.S. Federal Bureau of Investigation recently discovered nearly \$2 million in counterfeit Cisco Systems gear that leading private companies and leading government agencies were using unknowingly.

Government investigators and industry experts say the Cisco example highlights a need for companies' IP protec-

tion teams, resellers, law enforcement liaisons and customer service teams to stay in touch and be aware of red flags such as customer complaints.

ONLINE BANKING AND MORTGAGE FRAUD

Banks across the globe have spent billions of dollars over the past few years encouraging consumers to shift to online banking. And businesses everywhere

of criminals targeting owners of rental properties or second homes with attractive refinancing offers are on the rise. Using data supplied by the victims, the criminals forge credentials, refinance properties and abscond with the funds.

And when risky business practices in the subprime loan and mortgage market played out as a leading cause of the global financial meltdown, many people were surprised to find out just how many

(MAAWG), 12 percent of Internet users admitted clicking on spam because they were interested in the product or service offered. Eighty percent said they didn't believe they were at risk from malware when doing so.

And it's not just criminals who are peddling fake antivirus software or bogus spyware, or botnet herders hijacking machines. For instance, the New York attorney general's office in 2007 fined Priceline, Travelocity and Cingular for using adware programs to market their products.

Meanwhile, insecure or bad coding—whether it's a flaw in APIs from the same vendor that has acquired other companies or multiple companies agreeing on the same insecure standards or single-vendor flaws—is likely here to stay.

For instance, HIPAA is touted as a good first step in protecting the electronic storage of medical data, but it only applies to doctors, hospitals, insurance companies and the government. It excludes pharmaceutical companies and services to which consumers voluntarily give their health information. Industry watchers say new online health concerns, such as Google Health, Microsoft Health and other services that are exempt from HIPAA-required controls, will lead to further privacy erosions due to flaws in their APIs or third-party APIs.

THE BOTTOM LINE

The Ponemon Institute reports that in 2005, the cost for companies that lost 10,000 records or more was \$138 per record to clean up. By 2008, the cost per lost record rose to \$202. Multiply that by 10,000 records and it skyrockets to more than \$2 million.

Security experts say the best defense is to learn from trends in crimes, and use the knowledge to revise and build better policies and systems in cooperation with industry peers and government agencies—because you will be targeted again. (ISC)

Raj Goel, CISSP, is chief technology officer of Brainlink International, an IT services firm. He is located in New York and can be reached at raj@brainlink.com.

BEWARE!

Here are the latest trends in financial crimes. ■

have implemented more and more self-serve transaction methods—online and in person.

However, not all security ramifications have been thought out. For instance, if a customer logs into her bank account and a piece of malware transfers funds out of her account, who is liable?

In the U.S. home mortgage industry, meanwhile, reports

banks and lenders had inadequate internal digital controls.

In one sample case, a vocational nurse violated HIPAA's provisions and stole the identification of a 72-year-old woman. The nurse and three accomplices were able to cash out \$165,000 of the woman's home equity.

SPAM, MALWARE AND INSECURE CODING

According to a new survey by the Mesaging Anti-Abuse Working Group



Reasons for Change

INFORMATION SECURITY PROFESSIONALS CITE THE FACTORS THEY CONSIDER BEFORE CHANGING JOBS.



THE NUMBER-ONE FACTOR considered by information security professionals when deciding whether to switch jobs is a company's culture and values, according to a recent survey conducted by Barclay

Simpson, an international recruitment company. The poll was conducted on LinkedIn among 180 members of the Information Risk & Security Job Forum.

Other top factors include salary and benefits, promotional opportunities, company market position, and training or qualification support.

In practice, a decision to change jobs is most often a composite of all these factors. It is therefore likely that if the company's culture and the proposed salary are suitable, information security professionals will most likely accept an offered position. If these are not acceptable, pro-

motional opportunities, market position and training are unlikely to make up the difference.

Other interesting insights can be gleaned when you look at how age, gender and company size contribute to the results. For example, 50 percent of the respondents put themselves in the 25-to-34 age range. People in this group are usually the most active in the recruitment market and most likely to change jobs; these respondents say salary is most important. Perhaps not surprisingly, the younger age group, 18 to 24, are most interested in training and development.

While only 10 percent of the

respondents were female, the percentage matches the number of women working in the information security field. Surprisingly, 55 percent of the women cited salary as the most important factor in their decision to change employers, compared with 28 percent of men. In addition, women generally were more interested in qualitative than quantitative factors. The reverse tends to be true for men.

Unlike age and gender, the size of the company appears to have less influence on the value placed on various benefits of working for another employer. Market trends typically indicate that fewer information security professionals work for small companies: Those information security professionals working for enterprise companies represented the largest proportion of respondents (46 percent), while only 27 percent said they worked for small companies. (ISC)

Barclay Simpson is an international recruitment company specializing in corporate governance, audit, risk, compliance, information security and legal jobs. It recently opened a Hong Kong office to cover the Asia-Pacific region. For more information on that office, please contact Russell Bunker at rb@barclaysimpson.com.

Can You Tell What's Missing?

Security Awareness Begins and Ends with YOU!

A single user can make even the most fortified networks vulnerable. Your people ("you") are ultimately the most important line of defense against potential network exposure and at the same time, they are the most overlooked asset in any company.

Information Security is not a game, it is an attitude. EVERYONE in an organization plays a vital role. Email, instant messaging, fire walls, encryption and authentication systems are just a sample of the many commonly used business tools that should be considered in a company's overall security culture. A



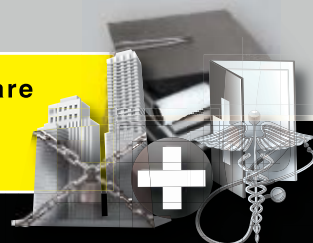
solid security awareness program will support a more secure posture and satisfy mandates and industry standards for information security.

Enter SCIPP's world-class End-User Security Awareness (EUSA) course. Easy to brand, and even easier to deploy, this web-based course is based on the SCIPP GAP™ (Generally Accepted Practices) and can be combined with industry specific modules created to comply with training mandates, such as FISMA, FERC, NERC, SOX, GLBA, FERPA, HIPAA, PCI and others.

EASILY CUSTOMIZE YOUR PROGRAM WITH SCIPP'S INDUSTRY SPECIFIC LEARNING MODULES



Financial Services (FFIEC) | Energy (FERC/NERC) | Healthcare (HIPAA) | Education (FERPA) | US Government (FISMA) | Retail (PCI-DSS) | Workforce Safety & Security



Securing Cyberspace

THE WORLDWIDE ECONOMIC DOWNTURN MAKES THIS EFFORT MORE IMPORTANT THAN EVER, SAYS ALBERT LEWIS.



BETWEEN THE SHORES OF LAKE GENEVA and the Alps rests the medieval castle of Chillon, erected by the Swiss in the 12th century to control the strategic passage between northern and southern Europe. A formidable fortress with watchtowers, ramparts, moats and turrets, it proved a fitting setting for a recent security conference. Here I had the opportunity to meet with CISOs, CSOs and other security professionals from around the globe to discuss common threats and challenges.

Many I spoke with were concerned about the impact of the global economic downturn on their ability to fund programs, while others spoke of the dire need for an international public-private sector partnership to coordinate against cyber attacks. In every case, they shared a global perspective on cyber security and recognized that cyber terrorism continues to be a real and pervasive threat to business and government. Both the European Union and U.S. government have recently announced plans to name cybersecurity czars to coordinate digital infrastructure defense, but public-private coordination for cyber security on an international scale remains elusive.

A global economy in crisis is the perfect outlet for cyber terrorists. With executives in government

and business focused on financial survival, inevitable budget cuts in cybersecurity programs will eventually lead to serious vulnerabilities in our critical cyber infrastructure. In this climate, a well-coordinated cyber attack by our enemies could cause further economic—and possibly political—destabilization for the West. The specter of global terrorism, including cyber warfare, is real and threatens the viability of vital financial and government systems. Now is the time when we can least afford to fail at protecting our critical digital infrastructure.

Today, the increasingly complex threat landscape requires systems and people that are proactive, flexible and able to do more than simply mount a reactive defense. Similarly, as cybersecurity leaders, we must adapt to a changing landscape of economic realities that threaten to negatively impact our programs.

The challenge is to recognize that most executives continue to view cybersecurity expenditures as overhead rather than a necessity. We need to make the business case that the firm's economic survival is directly tied to the strength of the organization's cybersecurity posture.

Most of us in cybersecurity leadership roles entered the field as engineers, but being a technical cyber genius is no longer enough. We must also be good communicators, adept at building coalitions and fostering relationships across our organizations. Today's successful cybersecurity leaders must learn to not only to effectively manage cyber risk, but also the economic risks that threaten the successful execution of our mission. (ISC)¹



Albert Lewis, CISSP-ISSMP, CISM, CGEIT, is a cybersecurity strategist and consultant to government and industry. Among his clients have been the U.S. Supreme Court, the FBI and the Department of Energy. He resides in the Washington, D.C., area.

There are plenty of fish in the sea.

Which is fine, if you're looking
for an ordinary fish.



Hire the Extraordinary

How do you make sure you land the perfect candidate? With (ISC)²[®], our members are pre-qualified because they hold an (ISC)² credential. This means they have been recommended and endorsed by professionals in their field and have subscribed to our Code of Ethics.

Make the Right Catch

(ISC)² Career Tools offers hiring managers the ability to review resumes of qualified, certified information security professionals around the globe and post multiple job openings for FREE! There's only one catch...the position must require or prefer the candidate holds an (ISC)² credential. It's all about looking in the right place, so tap into a pool of qualified professionals with (ISC)² Career Tools.

Learn more at www.isc2.org/careers

(ISC)²[®]
CAREER TOOLS

How do you translate

SUCCESS?

ISACA® Certifications

Certified Information Systems Auditor™ (CISA®)

Certified Information Security Manager® (CISM®)

Certified in the Governance of Enterprise IT® (CGEIT®)

As an IT professional, being a
CISA®, CISM® and/or CGEIT®:

- Counts in the hiring process
- Boosts your earning potential
- Enhances your credibility and recognition

Registered for an exam?

Get exam preparation materials and online review courses directly from ISACA.

For more information visit www.isaca.org/rgcertification.

