InfoSecurity PROFESSIONAL®

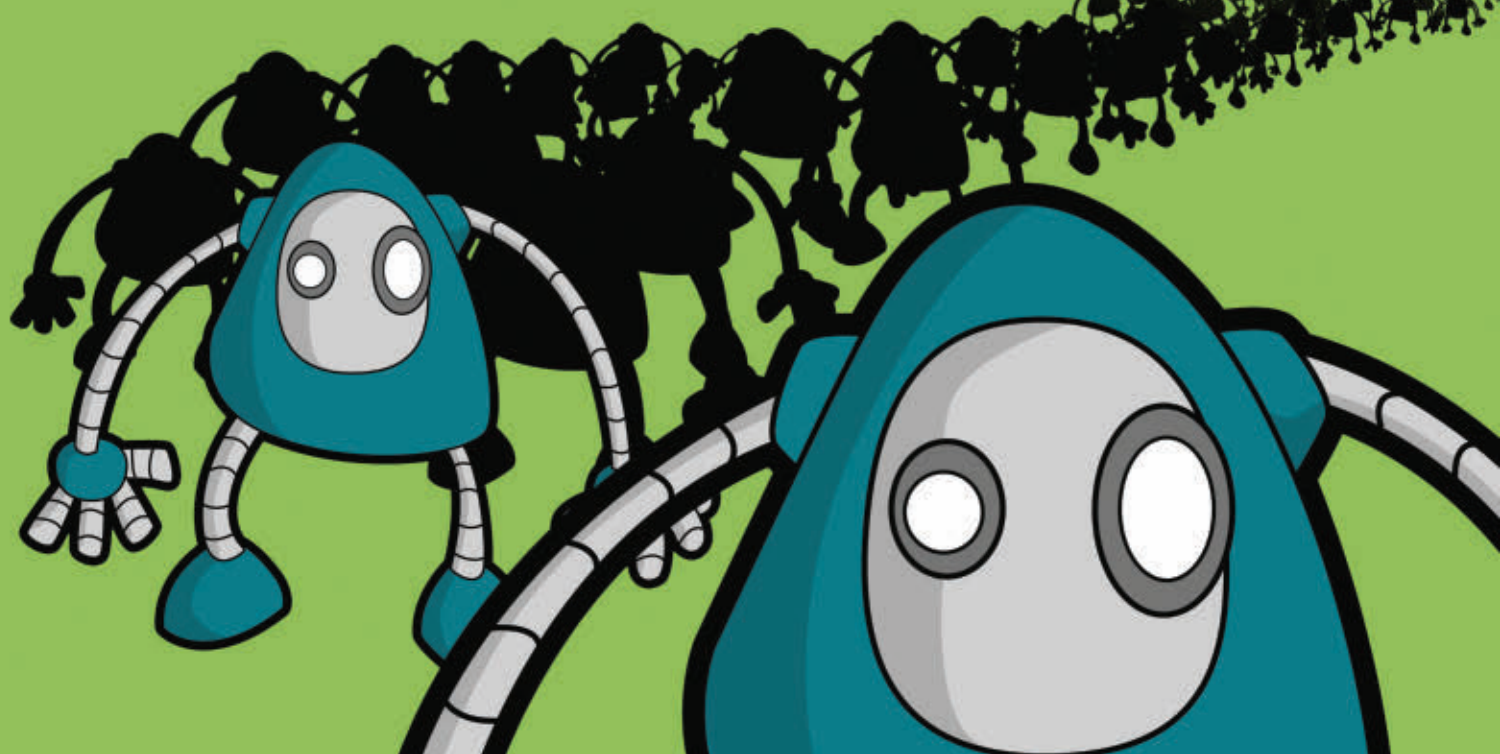
AUTUMN 2008

An (ISC)² Digital Publication

www.isc2.org

Battling Botnets

HOW TO PROTECT YOUR CORPORATE DATA



autumn

2008
VOLUME 1 NUMBER 3

18

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

features

also inside

InfoSecurity Professional is published by CXO Media, an IDG company, 492 Old Connecticut Path, Framingham, MA 01701 (phone: 508-935-4796).

COVER ILLUSTRATION BY PHOTODISC

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

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

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

For more information call 1.866.736.1755 or visit www.capella.edu/isc2

CAPELLA UNIVERSITY

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

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

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

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

* ACCREDITATION
Capella University is accredited by The Higher Learning Commission and is a member of the North Central Association of Colleges and Schools (NCA), www.ncahlc.org.

CAPELLA UNIVERSITY
225 South Sixth Street, Ninth Floor, Minneapolis, MN 55402,
1.888.CAPELLA (227.3552), www.capella.edu

executive letter

FROM THE DESK OF THE EXECUTIVE DIRECTOR

Breaking New Ground

BUILDING ON RECENT ACCOMPLISHMENTS, (ISC)² PLANS TO LAUNCH A NEW CREDENTIAL

YOU HAVE PROBABLY NOTICED that changes are underway here at (ISC)². Let me take this opportunity to say that I'm pleased to assume the executive director role for the organization, and I'm proud to lead such a great group of people.

Some of the immediate issues that I'm tackling include finding areas where we can expand support and bring the utmost value to our members. We have already made accomplishments in this regard with:

- The successful launch of our Member Services Contact Center, a one-stop shop where you can log questions, requests and problems related to your membership and credentials;
- Our revamped Website, including a new look, new functionalities, easier navigation and fresh content. If you haven't had a chance to visit the site yet, please make sure you do and send your comments to editor@isc2.org;
- Planning 2009 events and e-Symposiums to give you more CPE opportunities.

And I'm thrilled to be onboard as (ISC)² enters new territory in addressing critical security concerns around the world with the introduction of a new credential: the Certified Secure Software Lifecycle Professional (CSSLP[cm]). It is geared toward professionals involved in the software lifecycle—including, but not limited to, developers, software engineers, project managers and software architects.

The CSSLP will take a best practices approach, ensuring that holders can mitigate the security concerns every organization has regarding application design, development, deployment and disposal. The first professional assessment of the CSSLP is underway. To see if you qualify, go to www.isc2.org/CSSLP.

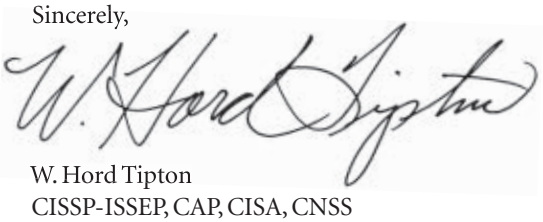
And while you're at the Website, visit the Cyber Exchange. As you know, October is Cyber Security Awareness Month, and part of our job is to make the cyber world a safer place. Read more about it on page 6. We urge you to find ways to participate in your organization and community.

In this age of increased cyber threats, we must educate ourselves about the risks as much as possible. This issue's cover story (page 10) about botnets—a serious danger to the corporate world and end users—offers an overview and suggestions for protecting your organization.

Also in this issue, we're introducing new features: (ISC)² member news (page 6), a career advice column (page 22) and a global view editorial (page 23).

We continue to receive great suggestions and feedback about this magazine. If you have comments that you would like to share, please send an email to infosecproeditor@isc2.org. Thank you, and I look forward to serving all of you.

Sincerely,



W. Hord Tipton
CISSP-ISSEP, CAP, CISA, CNSS
Executive Director

PHOTO BY ALEX McKNIGHT

Find the tools and guidance you need for a well-guarded network at microsoft.com/security/MSAT

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

Microsoft®

inbox

READER FEEDBACK AND SUGGESTIONS


Mentoring

"ONE-ON-ONE INTERACTION HELPS PUT SPECIFIC EXPERIENCES AND KNOWLEDGE SETS TOGETHER IN A WAY WE OTHERWISE CANNOT EXPECT."
—TONY BARATTA, (ISC)² DIRECTOR OF PROFESSIONAL PROGRAMS

It Takes 2

Mentoring provides career rewards for both mentors and mentees, which is why (ISC)² is rolling out a pilot program. by Peter Fretty

The [mentoring] program sounds like a great idea (*"It Takes 2," Summer 2008, page 16*). I have one question or rather a recommendation.

The article quotes Tony Baratta as saying "less experienced CISSPs have often asked where they can go for help, and this arrangement should provide that opportunity."

In that scenario, would it not make sense to provide one CPE per hour credit to the mentee, just as the mentor is getting? The mentee is furthering his/her knowledge in security, which is the point of the CPE. This would also provide a check and balance on CPE submission from the two different CISSPs.

Just a thought. Excellent job on the magazine, by the way.

STEVEN KELLER, CISSP
INFORMATION SECURITY ARCHITECT
WEBSTER, MA, U.S.

(ISC)² responds: *We did not intend to keep the mentees, who are broadening their knowledge base, out of the equation. We like your check and balance idea, but implementing it may be a bit cumbersome. We cannot guarantee that all mentees will be lesser experienced CISSPs. They may be students who haven't gotten the certification yet. We appreciate your suggestion and will look further into the details of this matter.*

I am truly excited to learn that (ISC)² has published a magazine focused primarily on security-related concerns. I'm currently reading the second edition, and thought it would be great to have a section dedicated to Governance, Risk and Compliance. What do you think?

ROOSEVELT REYNOLDS, CISSP
INFORMATION SECURITY OFFICER
ATLANTA, GA, U.S.

(ISC)² responds: *In upcoming issues, we plan to include articles that touch on the GRC topic. And hopefully, as our magazine grows, we'll have the space to give it a whole section.*

We welcome reader feedback and suggestions, and publish letters as space allows. Please send an email to: infosecproeditor@isc2.org

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

Marcia Thorpe
Senior Manager of Member Services
727 785-0189 x219
mthorpe@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

Kim Han
Senior Designer

CSO
Custom Solutions Group

[fyi]

(ISC)² MEMBER NEWS

PHOTO BY GABE PALMER/CORBIS

Get Your Cyber Safety Resources Online

FOR THE SECOND YEAR RUNNING, (ISC)² is championing Cyber Security Awareness Month, an initiative that aims to heighten public awareness about the importance of protecting information and implementing online safety programs at home, work and school. While cyber security is critical all year-round, with children back in school, October is the opportune time to focus on education and promotion.

As an (ISC)² member, it's easy to take part: visit the Cyber Exchange (http://cyberexchange.isc2.org) and submit valuable awareness resources the public can use, including videos, presentations and posters. You can, for example, share these materials with your local schools, or ask your organization to endorse the initiative to show that it cares about cyber safety.

As you know, (ISC)² has been running a Cyber Exchange contest for members, with the top five most downloaded materials winning $1,000 each. The contest runs through Oct. 31. (ISC)² wishes to thank all those members who have already contributed materials. You will be able to read about the winners in early November on the Cyber Exchange site.

Form 3 students from the Buddhist Sin Tak College in Hong Kong participate in the Youngsters Information Security Awareness Program, led by (ISC)² members.

Hong Kong Members Volunteer in Youngsters Awareness Program

(ISC)² MEMBERS ARE getting involved in worldwide initiatives to increase knowledge and awareness about information security among children. One opportunity is Cyber Security Awareness Month (see Cyber Safety Resources on page 6). Another initiative in which (ISC)² members can participate is the Youngsters Information Security Awareness Program (YISAP).

The project started in Hong Kong this past school year, where more than 6,000 primary and secondary students attended special events and presentations given by (ISC)² members to help the children understand the importance of information security.

Launched in conjunction with the Hong Kong Office of Government Chief Information Officer, Hong Kong Police and the (ISC)² ALIG-Professional Information Security Association, YISAP is expected to grow and expand to more school districts in this coming year. If you are interested in starting such a program in your area of the Asia-Pacific region, or if you live in Hong Kong and want to volunteer, please contact kchung@isc2.org.

and the winners are

SEVEN STUDENTS, most of whom are (ISC)² members, have been awarded scholarships for their research in information security. Congratulations to the winners, who will each receive between $11,000 and $12,500, depending on their research budgets, to fund studies in areas such as access control, intrusion detection systems, wireless mesh networks, risk analysis and software security. To view the press release with a full list of the scholarship winners, visit www.isc2.org/pressreleases.

(ISC)² Partners With Childnet Charity

IN THE UNITED KINGDOM, (ISC)² members are participating in the Safe and Secure Online initiative, a program developed by (ISC)² and Childnet International, a charity dedicated to making the Internet a safe place for children. Trained volunteers go into classrooms and discuss areas of growing Internet concern, such as social networking and cyber bullying, with 11 to 14 year olds.

The program has educated more than 7,000 students since the 2006 launch. Feedback from the children and their teachers has been overwhelmingly positive, with many students saying they would change their Internet behaviors having learned of the potential effects.

If you live in the U.K. and would like to participate, send an email to lturley@isc2.org.

There are plans to bring the Safe and Secure Online initiative to the U.S., with a pilot program now being developed in Seattle, Wash.

PHOTO COURTESY OF KITTY CHUNG/(ISC)²

events

EDUCATION OPPORTUNITIES

Upcoming conferences, seminars, workshops and trade shows for information security professionals to continue their education and earn CPE credits.

EVENT	DATE	LOCATION	FOR MORE INFO
Yuzawa Information Security	October 8-10	Yuzawa, Niigata Prefecture	*www.yuzawaonsen.gr.jp/conf*
SecureIndianapolis	October 16	Carmel, IN	*https://www.isc2.org/events*
SecureDallas	October 21	Dallas, TX	*https://www.isc2.org/events*
(ISC)² e-Symposium	October 21	Online	*http://isc2.brighttalk.com/upcoming-events*
SecureLondon	October 21	London, England	*https://www.isc2.org/events*
Systems	October 21-24	Munich, Germany	*www.systems.de/en*
RSA Europe	October 27-29	London, England	*www.rsaconference/2008/Europe*
ChicagoCon	Oct. 27–Nov. 1	Chicago, IL	*www.chicagocon.com*
SecureAsia	October 29-30	Seoul, South Korea	*https://www.isc2.org/events*
(ISC)² e-Symposium	November 11	Online	*http://isc2.brighttalk.com/upcoming-events*
SecureCharlotte	November 12	Charlotte, NC	*https://www.isc2.org/events*
Infosecurity Netherlands	November 12-13	Utrecht, The Netherlands	*www.tinyurl.com/3psnku*
CSI 2008	November 15-21	Washington, DC	*www.csiannual.com*
Infosecurity France	November 19-20	Paris, France	*www.tinyurl.com/3t7gzo*
SecureDubai	December 4	United Arab Emirates	*https://www.isc2.org/events*
(ISC)² e-Symposium	December 9	Online	*http://isc2.brighttalk.com/upcoming-events*
SecureLosAngeles	December 9	Los Angeles, CA	*https://www.isc2.org/events*
SC World Congress	December 9-10	New York City, NY	*www.tinyurl.com/4szptp*

ADVERTISER INDEX

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://mediazone.brighttalk.com/comm/ISC2/22a3caf27b-9876-1674-1

PHOTO BY GREG PEASE

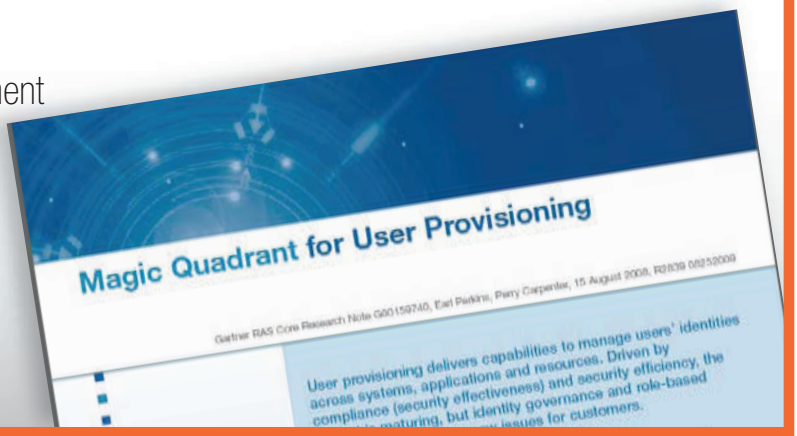
courion®

Courion Positioned in the Leader's Quadrant of Gartner's Magic Quadrant for User Provisioning

Access a copy of the 2008 Magic Quadrant compliments of Courion.

Learn why Courion's Enterprise Provisioning Suite™ solution helps companies achieve measurable business results by:

- Streamlining User Provisioning
- Simplifying Role Lifecycle Management
- Managing Access Compliance
- Automating Password Management



Visit our website to learn why companies worldwide are choosing Courion.

Read how our customers achieve success with Courion solutions.

Learn how we have enabled our clients to cost-effectively and securely automate the delivery of IT access to their users.

- Children's Hospital Boston ▸
- Regional Utilities Company ▸
- SunTrust Banks ▸

Learn why Courion is the solution of choice for fastest time to value.

The Courion Enterprise Provisioning Suite Jump Start Options received a perfect 5 out of 5 stars from SC Magazine.

SC MAGAZINE RECOMMENDED ★★★★★

Read the review ▸

Experience Courion through industry events, product demos and white papers.

See for yourself how Courion solutions can address your needs.

- Industry Events ▸
- Product Demos ▸
- White Papers ▸

[Cover Story]

BATTLING

BOTNETS

BOTNETS ARE BECOMING A BIG PROBLEM–SPREADING MALWARE AND STEALING SENSITIVE PERSONAL AND CORPORATE INFORMATION.

SAMUEL GREENGARD EXAMINES THE BATTLE LINES.

Hardly a day goes by without news of a breakdown or meltdown due to hacking, vandalism, outright data theft or, in the case of the Russia-Georgia conflict this past summer, cyberwar. In most cases, these incidents are the result of botnets—a collection of software robots, or bots, that run autonomously and automatically.

"They are a huge and growing problem," says Adam Meyers, principal of the information assurance division at SRA International, a global IT services firm headquartered in Fairfax, Va., specializing in national security, civil government and global health.

Ranging from a few hundred to a few thousand bytes, botnets can be used to infiltrate computer networks, causing the machines on them to perform a host of annoying—and often malicious—tasks. These include stealing passwords and identities, keystroke logging, spamming, producing adware and generating distributed denial of service (DDoS) attacks. The hijacked computers, referred to as

ILLUSTRATION BY PHOTODISC

"zombie" systems, lie dormant until the perpetrator of the attacks, a.k.a. the "botmaster," decides to unleash them. Then, with stealthy abandon, they pursue their mission—without the user's knowledge.

"These types of programs surreptitiously spread themselves and create networks that are far more powerful than groups of independently infected systems," says Ira Winkler, president of the Internet Security Advisors Group and author of *Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day*.

To make matters worse, botnets are growing more powerful and destructive. Too often, end users lack adequate protection, corporations fail to notice signs of a problem, and universities and government agencies are slow to react to infected systems. The largest botnets commandeer hundreds of thousands to well over a million computers. "They are a devastating force," Winkler says.

Carole Theriault, senior security consultant for Sophos, an IT security and control firm headquartered in Boston, U.S. and near Oxford, U.K., says that as long as the computers are online and vulnerable in some way, they can be absorbed into a botnet. "Interestingly, our research shows us that the U.S. is the number-one country for compromised machines being used for nefarious purposes, such as DDoS attacks and spam relaying, accounting for about 15 percent. Russia is at number two, accounting for 7.5 percent and Turkey is number three with 6.8 percent."

BOT ARMIES GENERATE 80% OF THE SPAM THAT HITS INBOXES AROUND THE WORLD.

Computing Under Attack

One thing that makes botnets so deadly is that the code can sit on a system for weeks or months before being activated. Computers carrying bot code initiate communication, usually through an IRC channel or open Internet protocol, and register themselves on the network. Then, at some point, these massively parallel systems receive a command to initiate an attack—subsequently shutting down major Websites, mining passwords or churning out mountains of untraceable spam.

Merrick Furst, associate dean at Georgia Tech's College of Computing, estimates that bot armies generate 80 percent of the spam that hits inboxes around the world. Some botmasters have gone so far as to use Google AdWords and banner ads to entice surfers to follow links or visit URLs that download bot code to their computer. As quickly as organizations like Google snuff out the fake ads, new ones pop up.

Traditionally, botnets have been the result of spam messages, browser hijackings through Javascript or Active X components, and peer-to-peer networking applications. Several botnets have gained notoriety over the last few years, including Kraken and Storm. Security specialists say that the former spews upwards of 9 million spam messages per day from more than 1 million infected computers worldwide, while the latter churns out spam, steals email addresses, spreads viruses and generates DDoS attacks. In fact, the Storm botnet, first identified in early 2007, at one time accounted for 8 percent of all malware on Microsoft Windows computers.

At this point, few organizations and site operators are immune. In September 2007, hackers took over the U.S. Republican Party's Website, circulating fake products and offerings that spread the Storm bot. A month later, online video site YouTube was hit with a bot. Social engineering often revolves around greeting cards, special deals and pornography, enticing recipients to click through to a Website from which bot code is automatically downloaded.

"The attacks themselves are fairly simple and straightforward," Winkler says. "The biggest problem is that people don't take precautions such as installing and updating antivirus software, using personal firewalls to block unsolicited inbound traffic, and installing host-based intrusion detection."

However, corporations and organizations are increasingly at risk, as end users download infected files—frequently through free music or games—or click on links to Websites that surreptitiously download bots, often through phishing techniques.

Another problem is that many enterprises leave port 25—the default port used to connect to email servers and to send email—open and unprotected, thus allowing unknown traffic to travel across the server. Ultimately, an SMTP mail server sends email but also spreads malware threats, says Tony Bradley, a consultant and co-author of *Hacker's Challenge 3*. Locking down port 25, he says, can go a long way toward preventing and blocking bots—and avoiding collateral damage.

Winkler believes that botnets have grown into the largest threat facing the Internet. Botnet operators often rake in significant sums of money while facing a minimal risk of capture. Some operate independently; many work in organized rings. "It's not organized crime in the way one might think of the Mafia. It may simply be a group of young men and women—often based in former Soviet bloc countries—who collaborate for basic criminal purposes," he notes.

In some cases, the activity can extend beyond spamming and phishing and into the world of extortion. Some online gambling sites, for example, have found themselves facing a DDoS attack the night before a major sporting event, unless they pay a ransom to groups operating a botnet. "It's nothing less than an online protection scheme," Winkler explains. "Oftentimes, it's easier to pay and not worry about getting shut down than it is to deal with an attack."

Defense Mechanisms

When 3Com Corp.'s TippingPoint Technologies division identified 25,000 systems infected with the Kraken bot in April 2008, executives pondered snatching control back, according to a *Computerworld* magazine article. Researchers infiltrated

the botnet by setting up a phony command-and-control server after reverse engineering a list of domain names found in a captured bot. They even wrote a piece of code that could remove the bot. Ultimately, however, officials opted to avoid any involvement for fear of liability. The U.S. Computer Fraud and Abuse Act prohibits unauthorized access to PCs, regardless of the purpose.

The rare individuals who are caught typically face relatively light penalties. For instance, when Robert Matthew Bentley of Panama City, Fla. was caught and convicted of operating a bot network this past March, he was sentenced to 41 months in prison and a $65,000 fine. And in January 2007, a court in the Netherlands sentenced two men to 24 and 18 months in prison (served retroactively) along with $11,700 and $5,200 fines for commandeering millions of computers and running Toxbot, which hijacked systems in order to steal credit card numbers and other personal data from eBay and PayPal. The pair also blackmailed online businesses by threatening to take down their Websites.

More daunting than capturing botnet creators is shutting down the botnets themselves. Because there's no single point of control, new PCs are constantly infected as their owners deploy antivirus software or when their systems go offline. More sophisticated polymorphic bots can change and evolve to escape detection—and some can tell when they're being probed or investigated and will fight back with a DDoS attack. Others are sophisticated enough to disable antivirus software, says SRA's Meyers. Still, others use rootkit technology to hide within other programs. "They are getting harder and harder to detect and eradicate," Meyers says.

Counterattack

There are ways to protect your organization; education is an important one. Employees should receive training about the dangers of botnets and the need to avoid potentially harmful email messages and links.

Some companies use "fire drills" to identify employees who are likely to click on bad links. In these scenarios, the IT department sends an email with a phony link and anyone who replies is flagged to receive further education and training on security issues. Some analysts have also suggested that companies should track employee responses to these test messages and use the data to guide employee evaluations.

From a technology standpoint, it's critical to have good antivirus software and update it regularly, says Andre DiMino, CISSP, co-founder and director of the Shadowserver Foundation, an all-volunteer watchdog group of security professionals who gather, track and report on malware, botnets and electronic fraud.

"You also need a centrally managed antivirus system that rolls out to every client [computer], so that anyone who attaches to the network must be scanned before getting in to the network," DiMino says. He also recommends having intrusion detection systems at the host and network level, and checking DNS logs for anomalies. "Botnets always change domain name pairings, so look for strange domain names—especially out of China and Russia," he adds.

Browser designers such as Microsoft and Mozilla are getting into the act by building anti-phishing technology directly into their browsers. The software identifies and blocks known malware sites. Another add-on tool, McAfee Site Advisor, displays green, yellow and red signs while searching on major search engines, including Google. Popup boxes display more detailed information about potentially dangerous sites.

On a Broader Scale

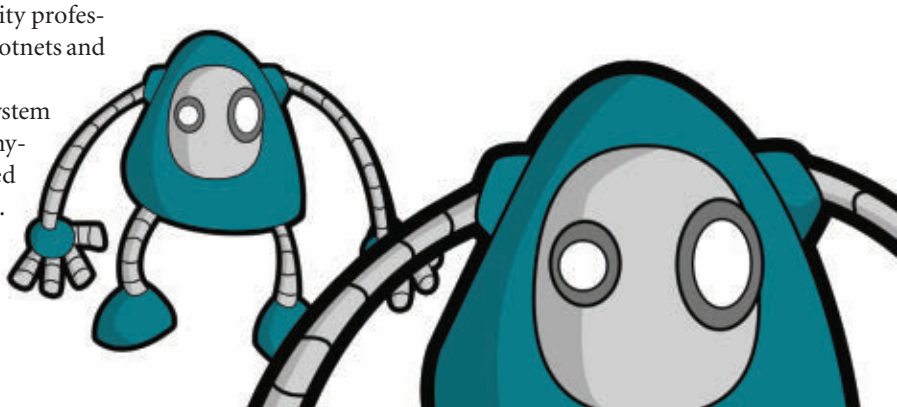
Most experts say that while there are certain steps you can take to protect your organization, ultimately, more stringent regulations are necessary. "If you are going to be on the Internet, you need to be running some basic security software and make sure it is updated," Winkler says. "It's really no different than operating a motor vehicle. You can be cited for a nonfunctioning headlight or a broken mirror." Likewise, he says, ISPs must identify and stop computers that spew millions of data packets resulting in spam.

DiMino agrees. "ISPs have to get onboard with the problem. Right now, they see it as a necessary cost of business. They need to cooperate with each other and with law enforcement."

The Messaging Anti-Abuse Working Group (MAAWG) hopes to clamp down on spammers by having ISPs block all machines on dynamic IP addresses that send email on port 25 outside their own network—unless there are special, legitimate reasons for doing so. In addition, rather than blocking relaying outright (and thus blocking legitimate users who forward email through their ISP's mail server), ISPs can fix the problem by using separate servers to receive and forward email messages.

Yet despite such advances—and new ideas and approaches—botnets aren't going to vanish anytime soon. And all the technology and brainpower in the world isn't likely to wipe them out. "We are seeing billions of dollars of losses as a result of botnets," Winkler says. "And we will continue to see billions of dollars of losses until individuals, corporations, universities and government becomes personally responsible for it. It's a problem that everyone needs to take a lot more seriously." (ISC)²

Samuel Greengard is a freelance technology journalist based in Oregon, U.S.



BETTER SAFE THAN SORRY

Why you need an information security strategy, and how to build one. By Nalneesh Gaur and Mike Heindl

Last year, a business disaster of the worst kind—the loss of information kind—struck TJX Companies. When the Framingham, Mass.-based parent of discount retail store chains reported that 45 million of its customers' credit and debit card account numbers had been stolen, it spent more than US$180 million to settle with consumers, banks and network associations. It was an expensive bandage for a wound that could have been easily prevented.

Of course, TJX isn't alone. As reported in "Data Breach: Creating an Organizational Strategy" (*InfoSecurity Professional, Summer 2008, page 6*), there have been numerous data breaches worldwide. These incidents have brought to light the importance of information security.

Still, businesses remain reactive, responding by allocating valuable resources to tactical measures and standalone compliance efforts. Over time, quick fixes and point solutions become costly and difficult to manage due to the complexity of multiple and redundant solutions. What organizations need is a clear and consistent information security strategy.

New Threats, New Regulations

Globalization makes it easier to conduct commerce anywhere, anytime. It's what *New York Times* columnist Thomas Friedman refers to as the "flattening of the world." No one could have imagined that this phenomenon would lead to increased crime and cyberterrorism and yet, that's exactly what has happened. Today's flat world is characterized by distributed operations and complex relationships between businesses and providers, all of which makes it difficult to distinguish between internal and external threats.

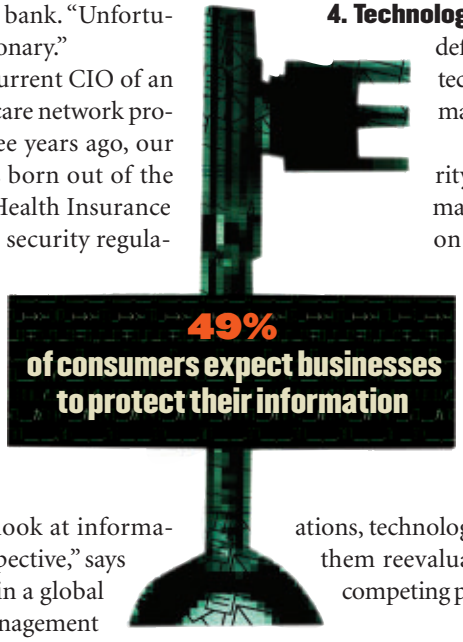
Still, consumers are increasingly aware of privacy issues and expect businesses to guard their personal data. In fact, 49

percent of consumers expect businesses to protect their information, according to Ponemon Institute's 2007 Consumer Survey on Data Security.

Government expects it, too. In the current environment, lawmakers and industry consortiums have been steadfast in passing regulations that bring information security and privacy best practices to bear. Because many of those regulations require greater accountability on the part of senior management, auditors have become more concerned than ever with verifying compliance. As a result, corporate boards in every industry are getting involved, holding senior executives responsible for security compliance and breaches.

"Today, information security is event-driven by regulatory pressures and the threat of breaches," says the former CISO of a large U.S.-based regional bank. "Unfortunately, most organizations are reactionary."

Another former CISO and the current CIO of an Oklahoma-based non-profit healthcare network provider agrees and says: "Almost three years ago, our information security program was born out of the necessity to comply with HIPAA [Health Insurance Portability and Accountability Act] security regulations. However, our executives were not content with simply complying with HIPAA; we wanted to adopt information security best practices to comply with any future regulations."



There is no doubt that compliance is a global driver for information security. "We predominantly look at information security from a regulatory perspective," says the head of IT operations risk within a global financial institution's investment management practice. "But our culture, which is driven by a preventative mindset, is another key catalyst for our information security program."

The Four Pillars of an Information Security Strategy

An information security strategy—and, indeed, a preventative mindset—is essential to modern-day business success because it allows businesses to prioritize their resources when addressing risks. In other words, it gives companies that have invested in various security tools and the tactics with which to use them.

Indeed, while many companies rely solely on technology to confront information risks, doing so can prove inefficient and even harmful. That's because a tools-only approach addresses threats in a piecemeal manner, which may amplify future problems. In the interest of solving problems more holistically, businesses should develop action tactics that are driven by the value of business assets and the probability of business risks, including their likelihood and their potential impact.

Leading global organizations believe that meeting information risks head-on requires an emphasis in four key tactical areas:

1. Strategic and Business Alignment: Businesses must identify information security drivers like applicable regulations, fraud and customer privacy, and then identify business assets, including their respective threats and vulnerabilities. Additionally, companies should review their existing information security initiatives, technologies and trust relationships.

2. Organization and Culture: A successful strategy must incorporate the executive tone; organizational and partner awareness; training needs, skills and competencies; and administrative and functional reporting structures.

3. Management and Governance: Management must focus on how the organization develops policies and standards, manages projects and programs, makes decisions and funds information security programs.

4. Technology: Organizations must establish a precise definition of information security that includes technology needs and standards, and how information security technology is managed.

Developing an effective information security strategy requires creating a long-term roadmap with milestones that are prioritized based on risk, compliance needs and cost. Further, a comprehensive effort requires establishing a program management office (PMO) to lead planning and execution, says the former bank CISO.

Planning gives businesses a better understanding of scope, dependencies, costs and needs. It also helps them budget resources across different groups—for example, operations, technology and information security. Finally, it helps them reevaluate implementation activities according to competing priorities.

Transforming Information Security

Although planning your information security roadmap is important, acting on it is critical. After all, to pick the fruits of its strategic labor, your business must move immediately to capitalize on the momentum of its efforts.

To successfully do that, start with right-sizing the scope of your project. Most information security managers mistakenly "over-scope" their initiatives when they ought to be looking for quick wins. Tackle urgent and basic problems before addressing more complex ones. For example, address pending compliance and audit issues on significant systems only before initiating an organization-wide rollout of your solution.

Following your security roadmap will inevitably require change. To help employees and executives cope, consider establishing cultural initiatives to educate and train them on new policies and revised procedures. Where necessary, implement structural changes, which may require recruiting new talent or pooling related job functions to make employees more effective and efficient. Regardless of the changes you make, understanding how your business needs will evolve is essential in leveraging new information security solutions.

Process changes that transcend all initiatives are common,

so affected processes must be identified and modified appropriately to ensure that initiatives succeed.

Also critical to success is executive involvement, which requires facilitating an operational relationship between the PMO and the executives who oversee it. "Having executive management on board is paramount to the success of any information security program," says the former bank CISO. "We provided quarterly updates to the board by answering questions such as, 'Are we protected?' and, 'What are the major issues?'"

The CIO of the healthcare network gained executive support with a three-pronged approach that first involved conducting an information security assessment, then implementing the resulting recommendations and finally, educating executive and division heads on information security's strategic nature. "Education came easy in the form of two information security breaches that were small enough to raise awareness but not cause any serious damage to our organization," says the CIO. "We now meet on a quarterly basis with the board and update them with a perspective on the state of information security. We provide them with information security metrics, including a global map that depicts where our threats came from in the last three months, as well as the number of employees, contractors and partners who have successfully passed the information security training."

The head of IT operations risk adds: "We work with the business, legal, compliance, audit, operations and IT groups to articulate the vision and benefits of the information security function. Stakeholder and steering committee meetings serve as the venue, where we share the progress of information security projects, key metrics, risks and issues."

Like all strategies, an information security strategy must be regularly revisited and revised so that it addresses your company's changing business needs, as well as evolving threats and technology advances. "We periodically review the initiatives and are prepared to correct course as needed," says the former bank CISO. "This is necessary to account for budgets and the evolving threats in the business environment. For example, we created and communicated a process to respond to what was, at the time, the emerging threat of phishing."

Unfortunately, information security transformation cannot be achieved overnight; it requires an ongoing commitment, as well as the willingness to persevere through change and resistance. Not ready for the work? Consider the alternative: a costly security breach or debilitating fraud that will bring your company to its knees. (ISC)²

Nalneesh Gaur, CISSP, is a principal, and Mike Heindl is a partner at Diamond Management & Technology Consultants, a consultancy firm with offices in the U.S., India and the U.K.

Don’t make your dog’s name your password

(and other tips on making Cyberspace a safer place.)

(ISC)²® members are among the most elite, knowledgeable information security professionals in the world. So we’re asking you to share your experience, knowledge and creativity at Cyber Exchange, (ISC)²’s new Website for trading ideas and expertise. Submit fresh videos, informational pieces, presentations and other cyber security materials to our Cyber Exchange Site in celebration of Cyber Security Awareness Month

It’s a dog-eat-dog world out there, full of cyber threats. Help promote Internet safety within your organization or community by uploading or downloading materials at (ISC)²’s Cyber Exchange today at **https://cyberexchange.isc2.org**!

October is Cyber Security Awareness Month. Go Fetch.

cyber exchange by (ISC)²

Social networking sites offer career, business and social advantages, reports Elisabeth Horwitt

MAKING connections

ONLINE SOCIAL NETWORKING SITES AREN'T JUST FOR TEENAGERS ANYMORE. Working professionals are increasingly using them to stay in touch with colleagues, share and acquire information, recruit talent and—most importantly—reach out to people who might hire them or otherwise further their careers.

Individuals in the information technology fields are in the vanguard of this trend. A December 2007 *NetworkWorld* survey of 663 IT professionals found that more than two-thirds of them are using social networking sites—42 percent primarily for business reasons. Sixty-eight percent of the respondents who use social networks visit them at least once a week, while 16 percent visit daily.

Information security professionals in particular have found online social networking platforms to be of great value in furthering their business and career goals. "Those with security skills to offer, and those in need of such skills, have an interest in creating a more transparent marketplace," says Peter Berlich, CISSP-ISSMP, CISA, CISM, founder of Swiss-based Birchtree Consulting and an (ISC)² board member.

SOCIAL NETWORKING WITH A BUSINESS SLANT

While many online communities are dedicated primarily to social activities, popular sites such as Facebook and MySpace are starting to target business professionals. Facebook provides a business page with features that professionals might find useful, including a tool for polling target audiences.

Some information security professionals, however, are leery of using general social networking sites for business interaction. They worry that discussion may gravitate to non-work-related issues, says Robert Beggs, CISSP, CISA, president of Toronto-based security services firm DigitalDefence and co-administrator of the Ethical Hackers group on LinkedIn. A substantial number of security professionals have gravitated to business-oriented social networking sites including LinkedIn, Xing, Plaxo and Ryze.

Such sites utilize the basic social networking concept but are for professionals only and include a number of features and tools designed specifically for career-building. For example, when Berlich was looking for a project partner with a specific skill set, he contacted his immediate Xing connections, obtained a couple of names, and looked up their profiles. Using the network reduced the cost and time required to find a certified professional with the right skills, he says.

Another way to form valuable connections is by joining groups or forums within a social networking

ILLUSTRATION BY DAN PAGE/THE ISPOT

A Global Review of Social Networking

Here are some testimonials to the business and career benefits of social networking from an international sampling of security professionals:

[ISRAEL]

ALON REFAELI, CEO AND CO-FOUNDER OF SECUREDZONES TECHNOLOGIES:

"I've used LinkedIn to find employees and contractors, and to get answers to security questions either by posting on the site or asking my connections."

[SWITZERLAND]

PETER BERLICH, CISSP-ISSMP, CISA, CISM, PRESIDENT OF BIRCHTREE CONSULTING AND AN (ISC)² BOARD MEMBER:

"As a freelancer, I want to know what people are up to, what clients they've worked with recently. Xing lets me do this without sending numerous emails."

[CANADA]

ANDREW HAY, CISSP, CCSE PLUS, RHCE, INTEGRATED SERVICES PROGRAM MANAGER AT THE FREDERICTON, NEW BRUNSWICK R&D FACILITY OF Q1 LABS:

"I use LinkedIn to get introduced to my counterparts at various vendors. Building my network of security contacts has really helped me get the information and contacts I need to get the job done."

[CANADA]

ROBERT BEGGS, CISSP, CISA, PRESIDENT, DIGITAL DEFENCE, TORONTO:

"LinkedIn is probably the best advertising tool I've got. Out of my last 10 jobs, six or seven clients used my LinkedIn profile to determine my suitability for hire. And when I'm looking to hire someone, it's the first place I go."

[UNITED STATES]

RICHARD STIENNON, CEO OF SECCOM GLOBAL:

"LinkedIn replaces the Rolodex. People keep updating their profiles, so if they move, you don't lose them forever. I have big plans for the Security Leaders group I founded; we're adding 30 people a day. There's the potential at RSA or another security conference to say, 'Let's meet at a restaurant and get to know each other.'"

[BRAZIL]

ED WILSON MENEZES, CSO AT REDECARD S.A., AND OWNER OF EWE TECHNOLOGIES:

"I decided to join LinkedIn because I can exchange knowledge with peers all around the world, and it's focused on professional relationships. I have received job proposals—some interesting, some not. I think the most valuable benefit that LinkedIn brings to users is that you can post questions to experts all around the world and get several points of view. Then you can compile the answers and make the best decision."

site. Some groups focus on specific issues, such as security metrics or ethical hacking. Others are defined by geographic location, job title or credentials; for example, there is an (ISC)²-sponsored site at LinkedIn that is for CISSPs only.

Members can also use keyword searches to locate other members with specific attributes, such as an HR employee at a certain company, or a CISSP in a particular industry or location.

GET NOTICED, GET HIRED

Social networks take advantage of the "six degrees of separation" theory that you can reach just about anybody through a branching network of friends and friends of friends. "If you can contact someone at an organization you want to work for through an intermediary you know instead of cold-calling HR, that's super valuable," notes Richard Stiennon, CEO of security service provider Seccom Global.

Once you reach a critical mass of 300 to 400 connections, "momentum builds," says Beggs, who now has about 800 contacts on LinkedIn. This can be both exhilarating and useful. "People keep tripping over me," says Beggs, "and because they do, they assume I'm worth knowing, that I can introduce them to other people. So they ask me to join their groups."

How do you build up to that critical mass? The first step is to ask your friends for introductions, especially the "spiders in the web—the ones in your industry who have lots of connections," Beggs advises.

Answering questions posted on the site or in community forums also gets you noticed. LinkedIn ranks "Top Experts" who answer the most questions in a given week. "If you see a lot of questions about PCI compliance, just by responding, you position yourself as an expert in that area," says Beggs.

He also recommends linking your profile to your Website and blog. "When potential clients go to my Website to check me out, immediately my LinkedIn profile pops up, with longstanding referrals from clients and links to my industry contacts," says Beggs.

Creating and leading a group is another means of making friends and establishing yourself in an online community. Stiennon created the Security Leaders group on LinkedIn, which recently exceeded 1,000 members, he reports.

IT'S GOOD TO BE SELECTIVE

Some information security professionals belong to half a dozen sites in order to ensure optimal coverage of issues and connections in their fields of interest. For example, Peter Wood, CISSP, COO of U.K.-based First Base Technologies, is a member of LinkedIn, Plaxo and Facebook, and participates to a lesser extent in Naymz, Spock and Spoke.

[JOIN IN]

► To become a member of **LINKEDIN** for CISSPs, email linkedin@isc2.org and you will be sent instructions to join. If you are a member of LinkedIn, you can join the CISSP network by simply updating contact preferences on your LinkedIn profile.

► To join the CISSP group on **XING**, go to https://www.xing.com/net/cissp. You will need to sign up if you're not already a member, then follow the registration instructions for the group.

Wood says these sites are useful "as a marketing tool for my business and keeping in touch with clients and peers," as well as "reminding people of our services."

When choosing a social network, one factor to consider is whether it has a significant population of members in your field and areas of specialization. For example, Alon Refaeli, CEO and co-founder of SecuredZones Technologies in Israel, says he has found business connections and resources by joining the following LinkedIn groups: Business Continuity, Information Security Assurance and Compliance Management; CISO: Meaningful Metrics; Certified Information Security Managers; ISACA Professionals; and IT Security Experts.

Geographic presence is another important criterion. Online security groups "tend to be very connection-focused, without physical boundaries," says Beggs. "People want to connect with anyone who does a particular type of job, regardless of nationality. I found that some people in the U.S. knew more CISSPs in Canada than I did."

Not all social networking sites have an equally strong presence in all countries or regions. Facebook and MySpace are still primarily U.S.-based, although both are aggressively expanding their overseas memberships. Xing has strong representation in Germany, where it originated, as well as in Italy and Spain.

Obviously, security is of primary importance to information security professionals. Business-oriented sites such as LinkedIn and Xing are particularly careful about keeping members' information private. Participants can choose which elements of their profiles are accessible to other members, and which are invitation-only. Beggs says he has tested LinkedIn's security by creating an account with fake information. After six months, he reports, he received no spam or unsolicited emails through that account. "They abide by their policy of not sharing (client) information, which is great."

Apart from the business and career-building advantages, information security professionals say they value the social aspects of such sites, including the ability to easily stay in touch with friends and colleagues. "I can maintain social relations with about 200 people," Berlich estimates. "This opens up the world to me. Why do we form social relationships? For safety, security, resources and for company, and to feel like we're part of something. This is one of the chief values that networking groups provide: I'm a part of something bigger." (ISC)²

Elisabeth Horwitt is a freelance business and technology journalist based in Boston, Mass.

Defining Qualities

DO YOU HAVE WHAT IT TAKES TO BE AN INFORMATION SECURITY "ROCK STAR"? BY JEFF COMBS

IT WAS A DEMANDING ASSIGNMENT. The client was an exciting startup company with an exceptional management team and very tough hiring standards. I was tasked with finding and recruiting the perfect person to fit this company's culture, someone who could quickly join and build the firm's global services function from the ground up. The client told me what they ultimately wanted was a "rock star" information security professional: someone with the credentials, skills and experience to meet the firm's expectations and impress the team.

My biggest challenge was clearly defining what "rock star" meant. Fortunately, the client was fully committed to the search—we spoke every day for a week to develop and refine the profile before the sourcing even started. Here are some tips on the qualities that make an information security professional a rock star, at least in the eyes of a hiring manager:

- **Character:** someone with integrity, values, intellect and personality
- **A winner:** someone who expects to succeed and won't settle for less
- **A strong track record:** someone who has worked for companies with good reputations
- **An achiever:** someone who strives to be his or her best, both in terms of work and personal accomplishments

In addition, rock stars have a solid sense of career direction, drive and a commitment to their profession. They exhibit ambition, growth potential and charisma—and, of course, demonstrate leadership qualities and exceptional communication skills. While not everyone in the information security industry is interested in being a high-powered executive, these qualities are examples of what separates a good candidate from an exceptional one.

In a competitive employment market, being good at one's job isn't enough to stand out. Candidates must differentiate themselves. While the term "rock star" may be a cliché, it characterizes individuals who have gone the extra mile and have the high-quality skills and expertise it takes to rise to the top.

In the end, it comes down to maintaining a high level of integrity, doing the best job you can at all times and being committed to the development of the information security profession—all of which, by the way, align with the (ISC)² Code of Ethics. (ISC)²

Jeff Combs is the practice lead of security and IT risk recruiting at Alta Associates, a Flemington, N.J.-based recruiting firm that specializes in information security, IT risk management and privacy. He also speaks at industry events and contributes to trade publications.

PHOTO TOP BY MOODBOARD/CORBIS

Smarter Security Spending

HOW TO BUDGET FOR SECURITY DURING AN ECONOMIC SLOWDOWN BY JOHN COLLEY

MANY PARTS OF THE WORLD are gearing up for an economic slowdown, if not a full-blown recession. In such a climate, it is natural for information security teams to assess security budget cuts. This comes at a time when pressure—from consumers, partners and business-to-business customers—to ensure responsible, secure business practice is mounting. And many organizations are dealing with regulations from government entities or the financial institutions that handle their business transactions.

Looking at the results of our own research into the concerns of the industry has led me to believe that companies will continue to take action rather than cut back on their investments. The 2008 (ISC)² Global Information Security Workforce Study* revealed an emerging parallel between assessing risk and confidence in the organization. Issues included improving customer and employee awareness, protecting the corporate brand and concerns over privacy violations.

As a result, a strong outlook is predicted for growth and professional development in the sector, with most respondents expecting either stability or an increase in personnel and training budgets. Expected workforce growth remains strong at 10 percent globally, the same as the previous study released in 2006, despite concerns in the 2008 report of an economic slowdown in many areas of the world. Europe, one of the regions predicted to experience an economic slowdown, was identified as the fastest-growing at 13 percent.

Regardless of the optimistic outlook, we must continue to sharpen our ability to justify what we spend. Security is increasingly viewed as a cost of doing business—similar to health and safety or well-being. While this may protect overall investment in security, more and more departments are sharing accountability and competing for budget funds.

Security costs fall into several categories: the cost of fixing things that go wrong through improper security measures; the cost of software, hardware and people involved in protecting the organization; or the "lost opportunity" cost if an organization isn't able to implement an initiative because it's hampered by insufficient security. The best way to justify the case for security is to have a coherent security business strategy that addresses costs in alignment with the overall business strategy. If it's developed in conjunction with business managers, you're more likely to get acceptance and foster a broader understanding of the benefits.

Security may be the safest item on operational budgets. However, this does not mean it is immune from justification. As good business managers, we should always be looking for ways to help tighten the corporate belt. Tough economic times should make us better at what we do by forcing smarter—and, I would like to think, more collaborative—thinking across the organization. (ISC)²

John Colley, CISSP, is (ISC)²'s managing director for EMEA and co-chair of (ISC)²'s European Advisory Board. He has more than 15 years of experience in information security.

PHOTO TOP BY GEORGE DIEBOLD

*Download the Study at https://www.isc2.org/download/2008_Global_WF_Study.pdf

insight

"SUCCESSFUL IMPLEMENTERS APPROACH THE PROJECT WITH PEOPLE IN MIND."

The DNA of ISO Achievers

CERTAIN CHARACTERISTICS LEAD ORGANIZATIONS TO ISO 27001 IMPLEMENTATION SUCCESS. BY SEKAR SETHURAMAN

Sekar Sethuraman, CISSP, CGEIT, CISM, CISA, PMP, CSQA, is the head of IT security in Greater Asia for LexisNexis. He has more than 25 years of experience in the industry, having held roles such as head of IT infrastructure and information security, CTO, CIO and advisor/consultant.

OBTAINING THE ISO 27001 CERTIFICATION is increasingly perceived as a competitive advantage. Earning this standard demonstrates that there is a solid baseline in information security management, and it proves to customers and vendors that the certified organization has ensured the appropriate protection for information assets, in line with potential risks.

It's quite common and popular among organizations in India to implement an information security management system (ISMS) and get it certified against the ISO 27001. These certifications have been earned by companies in widely diverse industries including software, business process outsourcing, manufacturing, banking and financial services, telecommunications and pharmaceuticals. Because of this diversity, many information security professionals have been engaged in ISMS-related projects, and ISO 27001-related courses are among the most sought-after training courses.

Having been associated with many ISO 27001 implementations, I have found that successful organizations have certain characteristics that seem to be part of their DNA:

1. Business alignment. Successful implementers have the ability to see the ISO 27001 project as an essential part of their organization's key business objectives. As a result, the project gets a high business priority and organization-wide participation.

2. Right size and right time. Experts in these implementations choose a scope that best fits the organization, which enables better focus and business benefits. These implementers also evaluate specific details of the ISO 27001 project, then time the implementation according to the maturity and abilities of the organization.

3. Culture. A passion for certifications is a part of the organizational culture. You will often see that they have pursued and earned other certifications—such as ISO 9001, SEI-CMMI, P-CMMI, ISO 20000—and many of their staff members have security certifications themselves. As a result, the organizations and the individuals have a greater awareness of the mandatory processes required.

4. Management commitment. Senior management participates extensively in these projects. This type of commitment is necessary for ISO 27001 implementations.

5. People-centric implementations. Successful implementers approach the project with people in mind and usually provide extensive awareness, training and development programs.

6. Ability to collaborate. Projects are carried out with significant collaboration at all levels and involve appropriate consultants as necessary.

7. Monitoring and course corrections. Strong monitoring processes—such as internal audit and measuring—are established, enabling the implementers to make timely course corrections when necessary.

Organizations should consider the above characteristics as they work to achieve success in their ISO 27001 implementations. (ISC)²

ISACA Now Offering a New Certification in IT Governance

CGEIT™
CERTIFIED IN THE GOVERNANCE OF ENTERPRISE IT™

Certified in the Governance of Enterprise IT™ (CGEIT™) recognizes IT professionals who have the knowledge, personal skill and business experience to maximize IT's contribution to enterprise success while managing and mitigating the risks posed by IT.

- Supports the growing business demands related to IT governance
- Increases the awareness and importance of IT governance good practices and issues
- Defines the roles and responsibilities of the professionals performing IT governance work

Early Registration Deadline: **11 February 2009**
Final Registration Deadline: **8 April 2009**
Exam Date: **13 June 2009**

Grandfathering Program Now Available!

Apply for certification without taking the CGEIT exam through **31 October 2008**.

Visit ***www.isaca.org/cgeit*** for more information.

SecureAsia@Seoul Conference

An (ISC)²® Security Leadership Event

29-30 Oct 2008
Asem Hall, COEX Convention Center
Seoul, Korea

SecureAsia is the region's premier 2-day conference in information security. Now in its third year, the Seoul event will focus on "New Technologies and Regulatory Compliance" and bring together information security experts from the U.S., Europe and the Asia-Pacific region to discuss emerging threats, risks and strategies on how best to mitigate them.

In conjunction with SecureAsia, (ISC)² is hosting its second annual Information Security Leadership Achievements (ISLA) Gala Dinner on 28 Oct, 2008 that recognizes the outstanding contributions and achievements of information security professionals in the workforce. Limited seats are offered to SecureAsia Conference registrants on a first come first serve basis.

KEYNOTE SPEAKERS :

Hwang Joong-Yeon
President, Korea Information Security Agency, Korea

Dr. Jae-Woo Lee
PhD, Honorary CISSP, CISA, CISM, Chair Professor, Graduate School of International Affairs and Information, Dongguk University, Korea

John Meakin
Group Head of Information Security, Standard Chartered Bank, UK

Prof. Howard A. Schmidt
(ISC)² Security Strategist and Newly Appointed President of Information Security Forum (ISF)

Prof. Corey Schou
Honorary CISSP
University Professor of Informatics, and Associate Dean, College of Business, Idaho State University, USA

Dr. Shin Soo-jung
Ph.D, CISSP, PMP, CISA
Executive Vice President
Infosec Co Ltd, Korea

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

Mark your diary and register at www.informationsecurityasia.com