InfoSecurity PROFESSIONAL®

ISSUE NUMBER 6
An (ISC)² Digital Publication
www.isc2.org

Anti-Social Behavior

The use of social-networking platforms is on the rise, increasing the risk of data leaks

Mother Nature understands the importance of building in security. Just like you.

CSSLP[CM]

Certified Secure Software Lifecycle Professional

You know malicious attackers are intentionally seeking out software vulnerabilities! Threats to application security have become more prevalent in an increasingly interconnected world. You must devise ways to ensure your applications are built securely. You're already a leader in information security, now take the lead in building security into every aspect of the software lifecycle by becoming an (ISC)²® Certified Secure Software Lifecycle Professional (CSSLP[CM]). You'll prove your knowledge on how security should be applied. No one understands the critical nature of security like Mother Nature. We couldn't ask for a better teacher. **Become a CSSLP today!**

Take the CSSLP Exam today!

Start Here.

www.isc2.org/csslp-register

20 (ISC)² years of excellence

issue 6

2009 VOLUME 2

8

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

COVER ILLUSTRATION BY KEN ORVIDAS/VEER. ILLUSTRATION ABOVE BY MICHAEL MORGENSTERN/VEER

features

also inside

InfoSecurity Professional is published by CXO Media, an IDG company, 492 Old Connecticut Path, Framingham, MA 01701 (phone: 508 935-4087). The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)² on the issues discussed as of the date of publication.

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

http://tinyurl.com/nkgq9u

InfoSecurity PROFESSIONAL

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

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

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

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

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

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

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

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

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

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

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

CXO Media Team
Matt Avery
Vice President, Custom Solutions Group

Amy Freeman
Project Manager ■ afreeman@isc2.org

Anne Taylor
Managing Editor ■ ataylor@isc2.org

Mary Lester
Executive Director, Art and Design

Terri Haas
Art Director

Lisa Stevenson
Associate Production Manager

CSO
Custom Solutions Group

ADVERTISER INDEX

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

executive letter

FROM THE DESK OF THE (ISC)² BOARD CHAIRPERSON

Reason to Celebrate

DESPITE A DIFFICULT ECONOMY, IT'S IMPORTANT TO RECOGNIZE SUCCESSES AND REMAIN POSITIVE.

THE SLIGHT IMPROVEMENTS WE'RE SEEING in the global economic picture bring much-needed relief from the constant, tumultuous media headlines. During these unprecedented economic times, we have sometimes wondered whether it's the right time to celebrate (ISC)²'s birthday or whether we should wait for better days that must be just ahead. Expressions of appreciation that recognize our volunteers for their unselfish support of the profession and the association are always appropriate.

Both in good times and during our struggles, giving thanks lifts our spirits and lets us focus, if just for a moment, on the accomplishments of the revered ones in our midst. In this case, they are all those individuals who were honored for their roles over the past two decades in the establishment and early development of the first information security credential—the Certified Information Systems Security Professional (CISSP®)—and our professional association, (ISC)².

At an April gathering in San Francisco, 80-plus founders and special guests came together to honor and be honored as pioneers and visionaries. Through their determination and sacrifices, they have been major contributors to the profession almost since our inception. We are grateful because without them, there would be no birthday to celebrate.

Looking ahead, our future is bright. As the economy sees some initial sparks of recovery, at (ISC)² we're seeing areas of growth, too. The new Certified Secure Software Lifecycle Professional (CSSLP℠) certification is generating tremendous response. As this issue of the magazine goes to press, the first set of candidates will be taking this exam.

We're also growing and expanding our membership in geographical terms. (ISC)² has seen interest in expanding our presence to India and further into Latin America. You can read about this growth as well as other areas where we're breaking new ground in our latest annual report, which you can find at www.isc2.org/aboutus/default.aspx.

As we look forward to new opportunities and celebrate what we have achieved, I wish to thank all of our members for the many ways that you contribute to our success. Your suggestions and participation in (ISC)² are incredibly valuable to maintaining the success of our organization. Keep sending us your ideas and feedback.

I also encourage you to volunteer in our programs, such as Safe and Secure Online (www.isc2.org/awareness), and make your voice heard by voting in the annual (ISC)² election in October—you'll read more about that in the next issue of *InfoSecurity Professional*.

Thank you for being a part of (ISC)².

Best regards,

Patricia A. Myers

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

(ISC)² MEMBER NEWS

[fyi]

A Matter of Federal Security

CISOs IN THE U.S. government sector believe the global economic crisis will increase information risks, according to a comprehensive "State of Cybersecurity" survey sponsored in part by (ISC)². And as a result of these growing threats, federal CISOs say there is pressure to quickly implement security solutions, which should result in the ability to retain critical security employees.

The study, the first of its kind among U.S. federal government agencies and bureaus, gives insightful overviews of how these groups go about their work. It takes a look at security tools and technologies being used; success of information programs and initiatives; and agencies' ability to recruit and retain personnel.

Other survey highlights:

- 48 percent believe that external threats resulting in data loss are the greatest risk to the federal government, followed by insider threats and software vulnerabilities.
- CISOs' top three priorities are: addressing threats to government data and information systems; improving cybersecurity governance; and meeting compliance objectives.
- The top three technology tools CISOs need are stronger intrusion detection and prevention; stronger authentication; and encryption.

For a copy of the report, visit www.isc2.org/ciso.

ILLUSTRATION BY MICHAEL KLEIN/VEER

fyi

An Awarding Evening

TO COINCIDE WITH (ISC)²'s 20th anniversary, a special awards ceremony and members' reception was held in April at the RSA conference in San Francisco. Founders as well as longtime and continued contributors and supporters of (ISC)² were recognized during this event.

At the annual RSA member reception, original (ISC)² founder Sandra M. Lambert and past board chair Randolph N. Sanovic were honored with the 2009 Harold F. Tipton Award and 2008 James R. Wade (ISC)² Service Award, respectively.

Other award recipients included:

- **Benjamin H. Gaddy Jr.**, 2009 James R. Wade (ISC)² Service Award
- **Prof. Howard A. Schmidt**, Fellow of (ISC)²
- **Dr. Whitfield Diffie**, Fellow of (ISC)²

For more information about the awards, visit www.isc2.org/PressReleaseDetails.aspx?id=4164.

(ISC)² HONORED SEVERAL INDIVIDUALS WITH AWARDS DURING ITS 20TH ANNIVERSARY MEMBER RECEPTION, WHICH WAS HELD ON APRIL 22 IN CONJUNCTION WITH THE RSA CONFERENCE IN SAN FRANCISCO. THE RECEPTION WAS ATTENDED BY MEMBERS, (ISC)² FOUNDERS AND CONTRIBUTORS.

A Secure Place for Kids

FOLLOWING THE SUCCESS of (ISC)²'s Safe and Secure Online program in the United Kingdom and Hong Kong, (ISC)² is proud to launch the program in the United States.

With the mission of educating schoolchildren ages 11 to 14, Safe and Secure Online is now under way in the Seattle area, led by (ISC)² member volunteer Richard Harrison, CISSP. The program combines classroom presentation materials, including a video about cyberbullying, with practical advice given by (ISC)² professionals. Topics include social networking, viral emails, spam, identity theft and more.

The program was initiated by (ISC)² with support from Childnet International, a charity that aims to make the Internet a safe place for children. First introduced in the United Kingdom in 2006, it was expanded to Hong Kong in 2007 and has reached more than 15,000 children in those regions. The program is designed to address the gap in security advice that exists in children's safety outreach efforts.

If you would like more information or are interested in becoming a volunteer and establishing the program in your area, please visit www.isc2.org/awareness.

FOUND TREASURE

(ISC)² HAD A GREAT response to the word hunt in its redesigned Website. Members who found the hidden words to create the sentence "Check out (ISC)²'s newest credential–CSSLP!" were entered in a contest to win a GPS. The winners included:

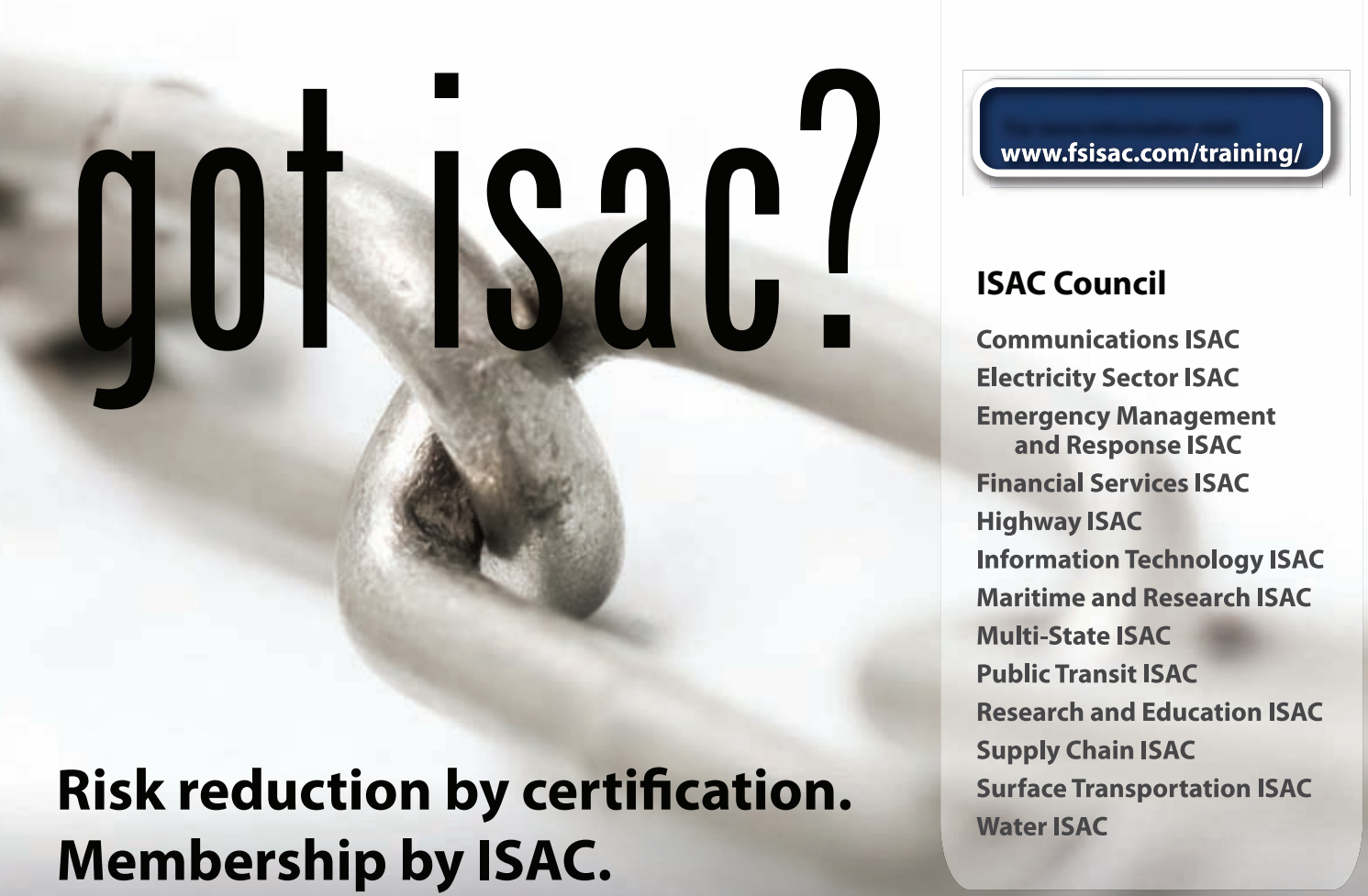
Jerome Radcliff (USA)
Betsy Mugo (USA)
Ken Cornies (Canada)
Guy Deacon (U.K.)
Rajesh Patel (U.K.)
Frank Spoelman (Netherlands)
Brian D'Cruz (Singapore)
Peter Bujnak (Australia)
Maisy Ching (Hong Kong)

Policy Change

AS OF JUNE 1, (ISC)² has made a change in its Continuing Professional Education (CPE) credits policy and will no longer post CPE credits on behalf of its members; members will be responsible for posting their own CPEs.

Also, CPEs earned for e-Symposia and for passing the *InfoSecurity Professional* magazine quiz are now subject to random audits.

For more information, please visit www.isc2.org/credentials/default.aspx.



got isac?

www.fsisac.com/training/

ISAC Council

- Communications ISAC
- Electricity Sector ISAC
- Emergency Management and Response ISAC
- Financial Services ISAC
- Highway ISAC
- Information Technology ISAC
- Maritime and Research ISAC
- Multi-State ISAC
- Public Transit ISAC
- Research and Education ISAC
- Supply Chain ISAC
- Surface Transportation ISAC
- Water ISAC

Risk reduction by certification. Membership by ISAC.

The secret to building and maintaining a resilient supply chain is professionalization of your key personnel - IT Security; Software Developers, Designers and Architects; Business Continuity Planners; and even your End-Users.

All Information Sharing and Analysis Center (ISAC) members are eligible to take advantage of HUGE discounts on world-class professional education and certification from the Business Continuity Institute, the IEEE Computer Society, (ISC)², and SCIPP International.

bci Business Continuity Institute

IEEE computer society

(ISC)² 20 years of excellence

SCIPP International™ The Security Awareness Certification Company

"Information Sharing and Analysis Centers were born out of the December 2003 presidential directive-07. These 'ISACs' were not only envisioned as sharing threat, vulnerability, incident and response/solution information within sectors, but also serving as interlocked components of a national critical infrastructure protection system. In such a system, cross-sector and sector-to-government communications could make possible a true national threat, alert and response system that can mitigate significant risk."

1999-2009 ITPG

10 years of innovation in education

THE COMPANY BEHIND THE COMPANY

powered by ITPG, www.ITPG.org

UNDERSCORING **CLOUD SECURITY** ISSUES

Cloud computing offers many benefits, but it's important to be aware of the security risks. Troy Giefer explains.

Cloud computing has quickly transformed from the latest buzzword to a trend that some of the IT industry's biggest players are taking seriously and a service in which they are investing serious resources.

However, cloud computing has some significant security risks that commercial and government users must address before they commit to relocating their organizations' data, applications and services. Information security professionals need to understand these risks as well as the potential benefits and the impact that cloud computing may have on traditional security tasks and roles within the organization.

But first things first: What is cloud computing? In a traditional IT environment, services, data and applications are typically located on the end user's machine or on servers within the corporate infrastructure. This infrastructure may be centralized or distributed; however, the organization typically owns and controls access to the majority of the computing resources and services.

In cloud environments, organizations relocate resources such as data, applications and services to computing facilities outside the corporate firewall, which the end user then accesses via the Internet. The cloud computing environment also provides organizations access to new services and applications, increased processing capacity, collaborative capabilities and managed services such as data backup and restoration,

ILLUSTRATION BY MICHAEL MORGENSTERN/THEISPOT

SC WorldCongress

ENTERPRISE DATA SECURITY 2009
CONFERENCE & EXPO

REGISTER NOW FOR SUPER EARLY BIRD SAVINGS
www.scworldcongress.com

INCOMPARABLE

SC World Congress provides the most security education bang for your buck (whatever the currency) of any event on the planet.

COMPELLING

Every session is packed with actionable information conveyed by experts in innovative formats.

REACH

A global network provided by more than 75 media partners is unsurpassed in the industry.

LOCATION

SC World Congress moves to the heart of the world's business capital in a new, high-quality hotel environment.

Sheraton New York Hotel & Towers

OCT.

13 TUESDAY

14 WEDNESDAY

Announcing your best value proposition in information security education & networking

SC World Congress 2008

Cybersecurity threats are recession-proof. Increasingly sophisticated attacks on your organization's vital IT infrastructure occur 24/7. Cost-effective strategies are required to meet these challenges. You'll get them at the second annual SC World Congress.

Emphasizing quality content, innovative formats, global perspectives and ROI, you can't afford to miss this event.

To register and for information, visit www.scworldcongress.com.

To exhibit or sponsor, contact Mike Alessie at 646-638-6002 or mike.alessie@haymarketmedia.com.

The breadth and depth of security topics covered at the SC World Congress 2008 was fantastic. Experts from government, banking, academia and more offered cutting-edge insights. I highly recommend attending."

– Dan Lohrmann, chief technology officer, state of Michigan

and security—all on demand and at costs often below what individual organizations can achieve.

Cloud environments typically consist of enormous data centers operated by industry-leading organizations—Amazon, Microsoft, Google, for example—with resources that may be distributed globally. They often offer massive economies of scale, services over the Internet, pay-as-you-go cost models, multi-tenancy and the use of virtualization technologies.

THE RISKS

Information security professionals need to understand the potential security risks associated with cloud computing early in the planning stages to best mitigate the risks.

Security was rated as the top concern for organizations considering a cloud computing strategy in a September 2008 *InformationWeek* survey of 456 business technology professionals. Respondents also identified security as the second most important element when choosing a cloud vendor.

So, what are some of the specific security risks that organizations will have to deal with when moving to a cloud computing environment?

- **Protection of data in transit.** Organizations must be sure that their proprietary data is adequately protected as it is transferred between the end user and the cloud data center. While interception of data in transit should be of concern to every organization, the risk is much greater for organizations utilizing a cloud computing model, where data is transmitted over the Internet. Unsecured data is susceptible to interception and compromise during transmission.

Hackers can use packet sniffers to monitor traffic passing through nodes between the sender and the receiver, or intercept improperly secured wireless communications to conduct session hijacking and man-in-the-middle attacks. The good news is that most cloud vendors use secure socket layer (SSL) or similar encryption protocols to secure data in transit.

- **Securing data at rest.** In a cloud computing environment, data from different organizations at different protection levels may be stored in a shared environment. Providers must address the unique challenges this brings and demonstrate to clients their solutions to these challenges. Cloud providers are responsible for maintaining separation of data as they promote the sharing of cloud applications and hardware hosted on virtualized images.

The very act of storing data in the cloud to improve availability and access from anywhere in the world substantially increases the number and types of threats to that data. Organizations should ask their cloud provider what controls have been implemented to defend against threats such as hackers, online crime, viruses and spyware.

Some cloud vendors leave the decision to encrypt and the method of encryption up to the user, while others maintain their own encryption-key infrastructure. Possible solutions that the end user can implement are authentication technologies, such as digital certificates and biometrics, while cloud providers could separate a customer's data into individual instances of applications—such as databases—or partition

> Organizations must be sure that their proprietary data is adequately **PROTECTED** as it is **TRANSFERRED** between the end user and the cloud data center.

specific areas of a cloud for information at different classification levels, or for military or government use only.

- **Maintaining compliance.** Public and private organizations have regulations and standards that must be adhered to with regard to data privacy and protection. The data owner must take appropriate actions to ensure the security and integrity of the data—such as developing a security policy, auditing, ensuring that proper controls are in place and performing risk assessments. Organizations considering a cloud vendor must be sure the provider understands the role it plays in assisting customers in meeting and maintaining compliance with governmental and commercial data protection and privacy laws.
- **Data privacy.** It is possible that a cloud provider has data centers in foreign countries, where data privacy and security laws differ, and that allow cloud administrators and law-enforcement officials full access and control of end-user data. Data privacy risks also come into play during investigative and forensic efforts. Ask the cloud provider where your data will reside and the role it plays in incidents such as data spills.
- **Data availability and recovery.** Ensuring data availability and recovery is arguably the most difficult of the security risks to mitigate because of the use of the Internet as the backbone between your local infrastructure and the cloud provider. Connectivity issues may arise due to peaks in network usage along any point across the Internet over which neither your organization nor your cloud provider has control. Internet outages caused by denial-of-service (DoS) attacks, natural disasters or technical problems at an ISP will have a negative impact on your ability to access data and services.

Although cloud providers offer service-level agreements to protect against substandard performance, these agreements will apply only to vendor-controlled services, not Internet or ISP performance. Also, while a contract with your cloud provider may guarantee payment for vendor outages, what is the impact to your business if your data is not accessible?

Both cloud users and providers must be responsible for maintaining adequate Internet access; this involves dual-homed ISPs and putting proper protections in place to deal

with vulnerabilities. Although cloud providers have data backup and recovery procedures, an organization should maintain local backups of critical data in case of a temporary loss of connectivity or, even worse, provider bankruptcy.

SECURITY BENEFITS

Although there are inherent security risks to cloud computing, there are many security benefits that may drive your organization to adopt a cloud computing model.

First, cloud providers can afford to implement and maintain best-of-industry security solutions and hire industry-leading experts because they have paying clients. This is in contrast to the battle raging in most organizations, where IT and security departments fight over a limited budget and critical security solutions get left on the negotiating table.

> Information security professionals and IT leadership should understand the **IMPACT** that moving data, applications and services to the cloud will have on security and traditional security roles.

Additionally, large cloud providers often have the ability to detect and defend against new malware and hacker attacks sooner than smaller, individual organizations. Cloud providers process millions of transactions each day that originate from users globally, giving them global threat visibility and zero-hour malware detection capability.

The large-scale capacity and infrastructure offered by cloud vendors is an exceptional environment for fighting off major threats such as distributed DoS attacks. The virtualized environments deployed by most cloud vendors offer the flexibility to isolate portions of the cloud under attack and quickly relocate services to avoid outages.

Another cloud benefit is that organizations can avoid large investments in security resources by transferring some security responsibility to cloud providers. Cloud vendors can provide 24/7 services such as firewall monitoring, intrusion detection and prevention, email filtering and patch management. The vendor may also provide in-house forensic support.

Providers can distribute antivirus software, personal firewall applications, and whole-disk encryption technology to mobile users on demand or as required in specific situations—such as at initial connection to the cloud environment. They can also evaluate devices each time they connect to ensure that they have applied all security patches and fixes prior to accessing the cloud infrastructure. It is important to understand, however, that outsourcing key security services does not completely relieve the security department from managing and maintaining security for the local infrastructure.

Data backup in the cloud is an optimal solution for organizations with limited data center space or when there is a temporary need for access to increased amounts of data storage. One word of caution: Costs should be carefully weighed, as most vendors charge for transfer of data into and out of their data centers. This makes cloud computing best suited for storage of static data accessed infrequently.

Finally, organizations stand to benefit from a reduced risk of data loss by storing corporate data in one central location that is accessible from anywhere in the world with Internet access. This minimizes the need to store local copies of data on fixed or mobile devices and reduces the risk of loss or theft.

IMPACT TO THE ORGANIZATION

Information security professionals and IT leadership should understand the impact that moving data, applications and services to the cloud will have on security and traditional security roles. For example, organizational security policy will need to be updated to account for third-party services offered by cloud providers; system boundaries will expand to include the architecture and services of cloud computing environments; security and IT staff will be freed from routine administrative or security tasks that are outsourced to cloud providers.

Likewise, the decision to move to a cloud computing architecture may impact traditional security roles within the organization. Security leadership should focus on enterprise security outside the firewall and manage relationships with primary cloud providers and subvendors. And security staff may spend less time on routine administrative tasks such as virus defense, patch management and email filtering, and more time managing security solutions as cloud vendors provide managed security services.

Information security professionals should become familiar with technologies used by cloud providers, such as virtualization and APIs, and the particular security strengths and weaknesses of these technologies. They should increase their focus on areas such as protection of data in transit and the unique privacy and compliance issues raised by cloud computing versus in-house security concerns. (ISC)²

Troy Giefer, CISSP, is an information assurance consultant for an international consulting firm based in Virginia. He is involved in cloud computing research and the development of cloud computing security offerings for the government market.

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

data leaks

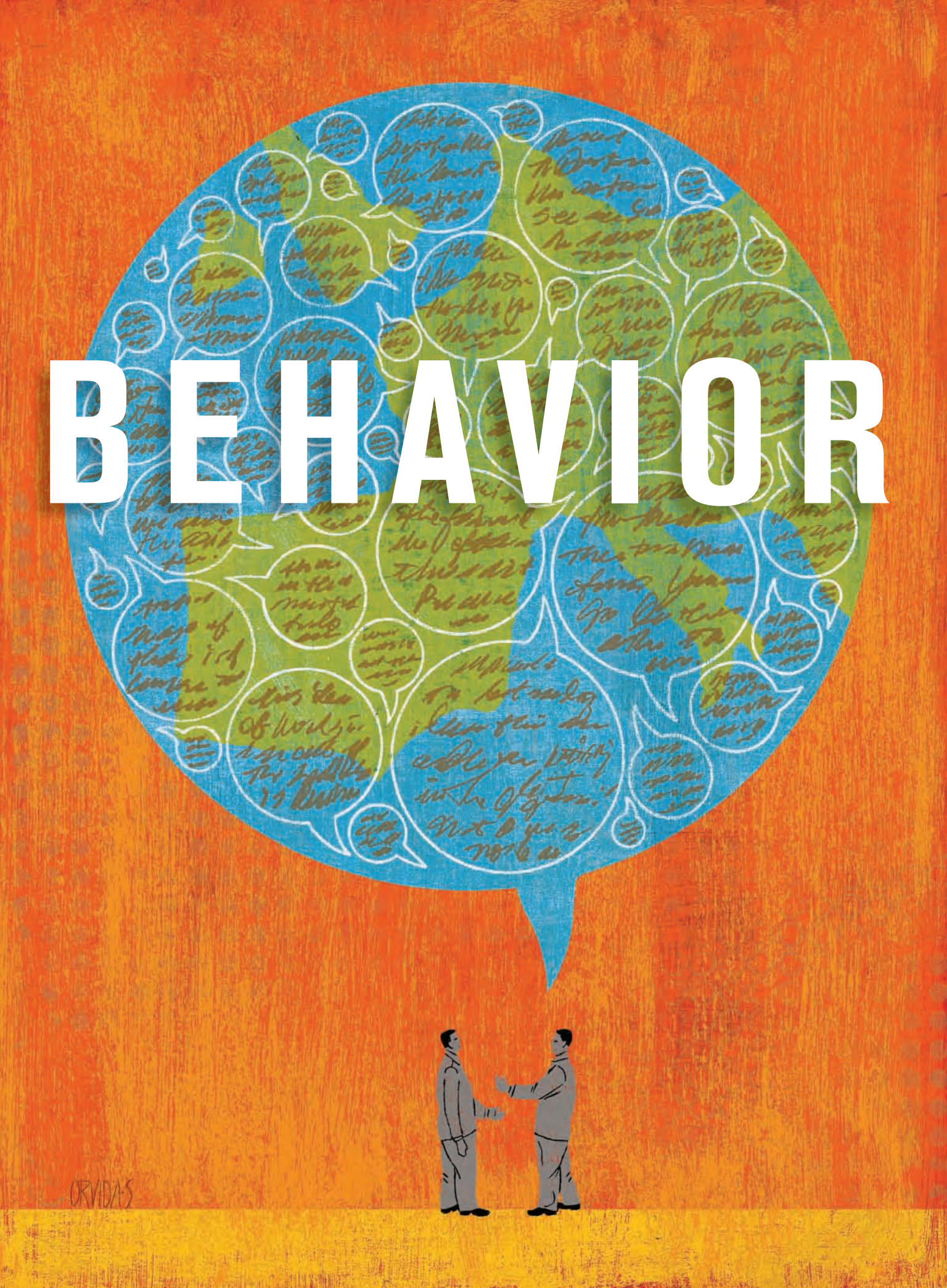
ANTI-SOCIAL

The threat level of social-networking platforms is rising fast, writes John Soat.

Drip, drip, drip… That's the sound of confidential corporate data leaking out onto the Web through social-media sites. Information security professionals can't ignore it any longer.

The Brits love a good scandal, and this was a good one. In April, a senior aide to England's Prime Minister Gordon Brown was forced to resign after emails written by him purportedly detailing plans to humiliate his political rivals were made public. In his resignation statement, Damian McBride wrote: "I am shocked and appalled that, however they were obtained, these e-mails have been put into the public domain."

ILLUSTRATION BY KEN ORVIDAS/VEER


BEHAVIOR
ORVIDAS

However, it isn't only politicians' information that is being leaked to the public. In a study called "Risky Business: Reputations Online," public-relations firm Weber Shandwick surveyed more than 700 senior executives last year. Respondents ranked "confidential or leaked info will appear online" as being the top online risk to their companies' reputations.

Confidential corporate data finding its way onto the Web isn't new. But the rapid proliferation and popularization of interactive online platforms such as blogs, wikis, chat rooms and messaging sites such as Twitter—collectively known as social media—have upped those stakes significantly for information security professionals.

Experts say a comprehensive IT security strategy must incorporate the use of social media, and that this demands a reorientation to the Internet. Security managers must stop thinking of Internet access in on/off, all-or-nothing terms and instead look on it as a series of conversations to be monitored in real time and in context, with effective rules being applied.

Just as important, information security professionals must ensure that their organizations' written security policies spell out the appropriate use of social media and that employees are well-aware of consequences for not following those rules.

DESIGNED TO LEAK

The problem is straightforward. "Social media [platforms] are designed to leak," says Mark Rasch, a consultant with Secure IT Experts and the former head of the U.S. Department of Justice's computer crime unit. The casual nature of communication in social media and its immediacy and informality, combined with the global reach of the Internet, contributes to making social networks "the world's largest coffee klatch," he says.

It's a klatch that's growing. Time spent on social-networking sites has eclipsed time spent on email, according to a recent survey by market research firm Nielsen Online. And that includes

Googling Security and Privacy

The search giant saves a lot of information. Here's what you should know.

It's no secret that Google retains search data and metadata regarding searches—in fact, it's quite open about doing so. What's unsure, though, is the long-term threat to information security and privacy.

Let's review Google's elements.

Google Search: This search engine is gathering many types of information about online activities. Its future products will include data gathering and targeting as a primary business goal.

All of Google's properties—including Google Search, Gmail, Orkut and Google Desktop—have deeply linked cookies that will expire in 2038. Each of these cookies has a globally unique identifier (GUID) and can store search queries every time you search the Web. Google does not delete any information from these cookies.

Therefore, if a list of search terms is given, Google can produce a list of people who searched for that term, which is identified either by IP address or Google cookie value. Conversely, if an IP address or Google cookie value is given, Google can also produce a list of the terms searched by the user of that IP address or cookie value.

Orkut: Google's social-networking site contains confidential information such as name, email address, phone number, age, postal address, relationship status, number of children, religion and hobbies. In accordance with its terms of service, submitting, posting or displaying any information on or through the Orkut.com service automatically grants Orkut a worldwide, nonexclusive, sublicensable, transferable, royalty-free, perpetual, irrevocable right to copy, distribute, create derivative works of, and publicly perform and display such data.

Gmail: The primary risk in using Gmail lies in the fact that most users give their consent to make Gmail more than an email-delivery service and enable features such as searching, storage and shopping. This correlation of search and mail can lead to potential privacy risks. For example, email stored on third-party servers for more than 180 days is no longer protected by the Electronic Communications Privacy Act, which declares email a private means of communication.

Gmail Mobile: Mobile phones are increasingly being sold with Gmail built in, and if not, it can be downloaded. The questions to ask: How uniquely does your mobile phone identify you as the user, and when was the last time you changed your phone and your identifiers?

Gmail Patents: Gmail's Patent #20040059712 emphasizes "Serving advertisements using information associated with email." This allows Google to create profiles based on a variety of information derived from emails related to senders, recipients, address books, subject-line texts, path name of attachments and so on.

Google Desktop: Google Desktop allows users to search their desktops using a Google-like interface. All word-based documents, spreadsheets, emails and images on a computer are instantly searchable. Index information is stored on the local computer. Google Desk-

the corporate environment. Many companies are beginning to realize how valuable social media can be in terms of brand management and product marketing—and, in particular, for customer service—as a way to establish close relations with valuable constituencies. On top of that, social networking is a way of life for most of the emerging workforce, guaranteeing its expanding use.

Data leaks in social media often are inadvertent: a salesperson posting a tweet about a new sales prospect or a developer sharing details on an industry blog. Or they can be intentional. The Website WikiLeaks (wikileaks.org), which has as its tagline "We help you safely get the truth out," provides an online platform for sensitive corporate data. "Whistleblowers can submit documents anonymously and untraceably," according to the site's FAQ list.

> "Social media [platforms] are designed to leak."
>
> – MARK RASCH, SECURE IT EXPERTS

Social networks have opened a whole new vector of attack for hackers and criminals. Kaspersky Lab's most recent malware study finds that malicious code distributed via social-networking sites is 10 times more effective than that spread in email. The reason: trust. Facebook users are more likely to open an attachment they think is from someone in their group.

Just as insidious, says Paul Roberts, enterprise security analyst with The 451 Group, is the potential for social engineering. "Employees might inadvertently expose data via their Facebook walls that the company doesn't want exposed," he says. "Even innocuous stuff, like naming your boss, or where you

top 3 allows users to search across multiple computers. GD3 stores index and copies of files on Google's servers for nearly a month.

Chrome: Chrome is Google's browser. It's available for download today and will eventually be installed on new PCs. Some of the risks it poses include:

- Every URL visited gets logged by Google
- Every word, partial word or phrase typed into the location bar, even if you don't click the Enter/Return button, gets logged by Google
- Chrome sends an automatic cookie with every automatic search it performs in the location bar.

Android: Android is Google's operating system for cell phones. It retains information about dialed phone numbers, received phone-call numbers, Web searches, emails and geographic locations at which the phone was used.

Google Health: This product allows consumers—such as employees, coworkers and customers—to store their health records with Google. Recently, CVS Caremark, along with Walgreens and Longs Drugs in the United States, agreed to allow Google Health users to import their pharmacy records.

Organizational Threats

Uninstalling these products or using competitive tools can mitigate many of these threats. But what about the dangers to your organization? One example is Google Search with its Google Flu Trends (www.google.org/flutrends).

Google has correlated flu data from the U.S. Centers for Disease Control (CDC) from 2003 to the present with its own search data. Spikes in users' searches about flu treatments correlated tightly with the CDC data. Flu Trends has demonstrated Google's ability to analyze search data for a specific term or set of terms. And it can retain this data and where it came from because Google in its privacy policies states that it records IP addresses.

So, what's to stop Google from analyzing all search data from your organization's networks? What's the difference between analyzing flu trends and "Top 100 search terms from XYZ Corp."? Or what if a company were to correlate regional threats from swine flu with search data from Google Health/Prescription data and then analyze the health of its employees and detect long-term effects?

Overall, the most critical threat is reliance on Gmail—whether the setting is universities, cities, companies or countries switching to Gmail en masse, or the newest employees in the organization using Gmail as their primary or sole email platform.

Questions to ask your security team: How big is the organization's email archive? How many years of emails are saved? If your organization switches its email hosting service to Google Gmail, what happens to the privacy and confidentiality clauses in your employee and customer contracts?

Another area of concern for hosted email is the potential of having to turn that data over to the government. Google, Yahoo and Microsoft have a history of complying with the United States' and foreign governments' requests for information. If such data is turned over, how much corporate security is being eroded?

Consider the amount of money and manpower dedicated to handling Microsoft Windows patches, viruses, spyware and botnet detection. Imagine the impact that reliance on Google products could have on corporate privacy and security.

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@goel.com.

work or the name of the project you're working on" can be compiled and used by hackers to gain access to a facility or to an individual's PC, he says.

Mobile technology also is problematic. Access to social networks via mobile devices nearly tripled last year, according to Nielsen. Twitter, with its 140-character limit, is the perfect platform for cell-phone users. The photo and video capability of mobile phones represents a potential avenue to exposing proprietary corporate data, both purposeful and inadvertent.

> "Employees might inadvertently expose data via their Facebook walls that the company doesn't want exposed."
>
> – PAUL ROBERTS, THE 451 GROUP

WHAT'S BEING SAID

Addressing this security challenge involves knowing what's going out of your organization as well as what's coming in, says Rasch. Instead of simply blocking Websites, companies must be "appropriately monitoring what's going out of the corporation and what's being said by people in the company," he says.

There are a growing number of technology solutions attempting to address this problem, says The 451 Group's Roberts: "It's a very hot area right now." Most solutions have secure gateways that monitor Web traffic and keep track of social media as it evolves. "Our core capability is our ability to understand several thousand applications at the egress level," says Kailash Ambwani, CEO of FaceTime Communications, which markets a Web monitoring and content management system.

Part of the problem is that Facebook, MySpace and Twitter are only the best-known names in the social media; there are many more, with a variety of purposes, such as Delicious, FriendFeed, Picasa, StumbleUpon, Tribe.net and Viddler—to mention a few. Google, with its brand extensions, presents its own set of problems in how data finds its way onto the public Internet (see sidebar, "Googling Security and Privacy," page 16).

That's why context is so important. The idea is to "create rules around the type of content [employees] can see or engage with," says Dave Meizlik, director of product marketing at Websense, a Web monitoring and content management vendor. There are three important contextual indicators, he explains. "When you understand the user, the data and the destination, you can set policy around those," Meizlik says. "That allows you to set business intelligence controls but still enable business."

Also, companies should track social-media sites for potentially compromising content. Rasch calls this "open-source monitoring," and there are several products and services that can follow every mention of a company's brand or logo in the blogosphere. Usually these are marketing tools, but information security professionals might want to employ them, for instance, to seek wayward intellectual property. This effort can be accomplished with tools as simple as Google Alerts or Yahoo Pipes.

POLICY MATTERS

Still, vendors themselves admit that technology alone won't solve the problem. "Technology is an enabler for good policy," says Meizlik.

Companies must update their security policies to address the use of social media. But what such a policy might entail depends, to a certain degree, on the culture of the company. At a high level, though, a social-media policy is simple: Don't be stupid. Employees must use their heads when they're social networking, especially as representatives of their organizations.

FaceTime has a clearly spelled out Web 2.0 policy, says CEO Ambwani. At a strategic level it goes like this: "Be mindful of what you're communicating." At a tactical level, salespeople can't talk about specific customers they're working with and developers can't talk about particular projects or features they're working on, he says.

A factor that should not be underestimated is employee satisfaction. Security professionals should encourage their companies to conduct employee-satisfaction surveys and to take them seriously. Satisfied employees can be strong advocates for their companies in the social media; unhappy employees are social-media time bombs.

Information security professionals can't ignore the growing use of social media and the increasing threat level it represents. The security risks related to peer-to-peer networks are well-documented, yet many people might be surprised to find out how prevalent P2P is in the corporate environment. FaceTime regularly polls the gateway devices installed at its customers' sites. In its most recent survey of the 80 locations represented, 94 percent have at least one P2P end-point.

In terms of social-networking sites, that number is 100 percent. And that's a lot of egress points. (ISC)²

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

The one security blanket you won't be embarrassed to take to work.

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

CISA wins *SC Magazine's* Best Professional Certification

CISM named finalist for *SC Magazine's* Best Certification Program

ISACA® Certifications

ISACA certifications increase your value to employers and clients.

Being a CISA®, CISM® and/or CGEIT®:

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

Secure Your Career: Get Certified.

Visit *www.isaca.org/rgcertification.*

ISACA® Since 1969 40th Anniversary

Serving IT Governance Professionals

Stepping

OVER THE COURSE OF **20 YEARS**, (ISC)² HAS ACHIEVED A SERIES

AS (ISC)² CELEBRATES ITS 20TH ANNIVERSARY, it's time to reflect on the achievements of the original founders and members and how they've shaped the information security profession.

What started with a handful of passionate volunteers and 500 applicants for the first CISSP® credential exam, has grown to an organization with a professional staff serving more than 60,000 members worldwide from Antigua to Zimbabwe.

(ISC)² has become synonymous with the people part of the information security equation, and its certifications have become the highest in demand around the world. The organization has accomplished a great deal over the past 20 years, thanks to those professionals who have dedicated their time and knowledge.

On this page and the next, you'll see how (ISC)² has grown and changed, including the major milestones achieved.

20 (ISC)² years of excellence

1988

- "The Consortium" was formed among several professional organizations to create a global information security certification process for professionals and address the need for standardized curriculum for the burgeoning profession. A series of strategy and planning meetings were held at Idaho State University and in Salt Lake City starting in November.

1989

- (ISC)² was established as a nonprofit corporation
- First president of the Consortium was named
- The first CBK® prototype was completed

1990

- The first CBK working committee was formed

1992

- The CBK committee finalized creation of the CBK's general contents

1994

- CISSP® credential established and first exam launched
- U.S. Postal Service was the first organization to contract with (ISC)² for its certification services

1997

- (ISC)² board began overseeing all operations

PHOTOS BY ISTOCK

Stones

OF MILESTONES THAT ADD UP TO A HIGHLY SUCCESSFUL ORGANIZATION.

2000

- Hired a professional management team
- Hired first managing director

2001

- Established its European headquarters in London
- Harold F. Tipton Award was established
- Launched the SSCP® credential

2002

- Opened its Asia-Pacific office in Hong Kong
- (ISC)² Institute was established
- Featured on the cover of *CIO* magazine
- Recognized its 10,000th member
- Expanded information security education to Europe and Asia

2003

- Recognized as one of the industry's top IT certifications in *Certification* magazine
- Launched the Associate of (ISC)² and CISSP concentrations
- Formed the first Advisory Boards
- (ISC)² Press was launched
- Established the Information Security Scholarship

2004

- Opened an office in Tokyo
- Released inaugural publication of *Information Systems Security*, *The (ISC)² Journal*
- CISSP earns ANSI accreditation for ISO/IEC Standard 17024
- Developed the Security Leadership Conference Series
- (ISC)² corporate headquarters moved to Palm Harbor, Florida
- Launched first (ISC)² *Resource Guide for Today's Information Security Professional*
- Released inaugural "Global Information Security Workforce Study"

2005

- CAP® credential was launched
- Declared 2005 the Year of the Information Security Professional
- Established the Affiliated Local Interest Group program
- Published the *Career Guide to Information Security Profession*

2006

- SSCP received ANSI accreditation for ISO/IEC 17024
- Launched Safe and Secure Online program with Childnet in the United Kingdom
- Received inaugural *SC Magazine* award for Best Professional Training Program

2007

- Launched (ISC)² e-Symposium Webcast under the (ISC)² Security Leadership Series as an exclusive member benefit
- Won *SC Magazine* award for Best Professional Training Program for second consecutive year

2008

- Launched the *InfoSecurity Professional* magazine to its membership
- Published the *Hiring Guide to the Information Security Profession*
- The CSSLP℠ was launched
- Won inaugural *SC Magazine* award for Best Professional Certification Program
- Launched the (ISC)² Security Blog

2009

- The *(ISC)² Online Resource Guide* is launched to the public
- Launched the (ISC)² ThinkTank—a Security Leadership Roundtable
- (ISC)²'s membership today consists of over 60,000 members in more than 130 countries

www.AltaAssociates.com

Alta ASSOCIATES
specialists in executive recruiting

We get people...

...we know who they are, what you need & how they fit.

We recruit people who strengthen organizations

With over 20 years of building world class teams and promoting diversity, Alta is proud to host

The 7th Annual
EXECUTIVE WOMEN'S FORUM
National Conference

September 23-25, 2009

Hyatt Regency at Gainey Ranch

Scottsdale, AZ

This year's theme–
Pragmatic Risk Solutions for Changing Times:
Achieving More with Less

*The EWF brings together **more than 200 executive women of influence, power and intelligence** within the Information Securtiy, Privacy and Risk Management arenas.*

To partner with Alta Associates, please visit
www.AltaAssociates.com

For more information on the EWF or to register, please visit: **www.ewf-usa.com**

Today's Essential Skills

FROM CERTIFICATIONS TO SPECIFIC SECURITY SKILL SETS, LOUISE HARRIS REPORTS WHAT'S IN DEMAND.

A SURVEY BY the Computing Technology Industry Association found that expertise in security, firewalls and data privacy are considered the most important skills for IT staff.

The survey, conducted worldwide last year with more than 3,500 respondents in 14 countries, found that security is clearly a key skill for IT professionals. But what are the most sought-after skills and qualifications in the security sector?

Information security generalists who have come up through the experience-only route are best advised to gain a recognized information security qualification before looking for their next job. The further up the career ladder these professionals climb, the higher the expectation will be that they hold one or multiple certifications. The most commonly sought-after qualifications are the CISSP®, CISA and CISM—with employers most frequently requesting the CISSP.

Less-experienced candidates who show dedication and motivation in gaining qualifications are well-regarded by potential employers and are likely to have an edge over applicants who haven't started down the certification route. Seize the time to enhance or attain credentials wherever possible.

Information security specialists, most notably penetration testers and forensics analysts, are continually in demand by employers. In these cases, while relevant certifications and qualifications are desirable, solid experience tends to hold more power.

Another area of expertise in demand is for Payment Card Industry Data Security Standard specialists. There is a strong demand for experience in taking companies through the compliance process, provided that salary expectations are not unrealistic. Companies that need quality employees to deliver consultancy to corporate clients in this area generally seek individuals who have gained these skills perhaps as part of a broader role and are willing to specialize.

Finally, skills that never go out of fashion are soft skills. The ability to communicate and interact with people of all levels, getting them to recognize risk and own the goals of an information security program, often requires a high level of diplomacy. All the qualifications around are no substitute for the right interpersonal skills. Information security professionals must strengthen their abilities and recognize that doing so is as much a vital part of professional development as the next certification. (ISC)²

Louise Harris is the director of Alderbridge Network Recruitment, which has been providing specialist information security recruitment services across Europe for more than 10 years.

PHOTO TOP BY MOODBOARD/CORBIS

Similar and Yet the Same

THOUGH EACH GEOGRAPHY HAS ITS SECURITY ISSUES, THERE ARE MANY AREAS OF OVERLAP, WRITES PETE ALGAR

INFORMATION SECURITY HAS TO BE ONE of the most interesting and diverse professions to work in right now. I see many differences, but there's an increasing convergence as our profession matures. The global nature of security adds further diversity with the inherent differences in language, culture and regulation.

All Regulation Is Not Created Equal

Regulation has been one of the key drivers in developing information security in recent years. There are obvious geographical differences in regulation with limited application globally. The United States has developed regulatory legislation such as the Sarbanes-Oxley Act and the Healthcare Insurance Portability and Accountability Act (HIPAA).

Europe has strong privacy and data protection regulations, but even these are not consistently applied across the continent. Some regulations are applied outside of their region of origin, others are purely local. These differing regulations sometimes present contradicting requirements in different territories. Thus it is often difficult for the information security professional to get it right every time.

The recent escalation in terrorism has been another key driver in some parts of the world. However, this risk is perceived differently in different parts of the globe. In some localities, terrorist threats to security systems are new; in others it has been seen as a new variant of a previous threat.

Censorship, media regulation, industry self-regulation and government regulations are also handled differently in various parts of the world.

Sharing Common Ground

Yet with all these differences, there are many things information security professionals have in common. We are in an uphill struggle to protect our organization's data, and we're constantly trying to understand and predict the ever more ingenious ways the "bad guys" invent to attack our information resources.

We are beginning to see some global standards being adopted—for example, Payment Card Industry Data Security Standard for credit card payments. Also, the ISO 27000 series of standards is becoming established as an integrated criterion for information security as well as for related areas such as business continuity and risk management.

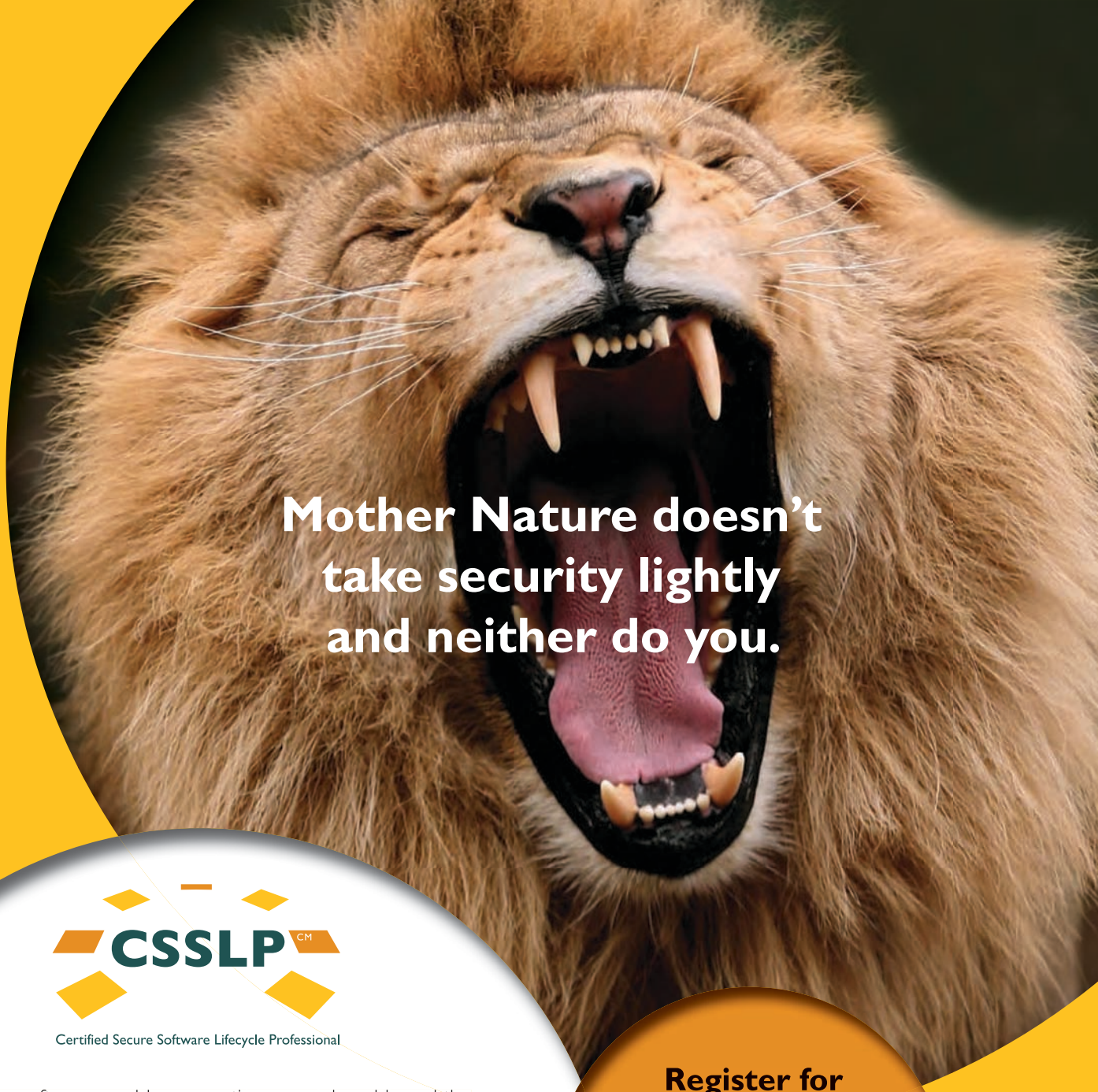
What's Next?

I believe we will see a move from specific regulations toward overall standards as the information security sector continues to mature. There will continue to be specific local needs, and language and cultural differences will continue to provide new views into handling security.

It's interesting and rewarding to work in a profession that is still defining itself and its place in the world. (ISC)²

Pete Algar Dos Santos, CISSP, is a business security manager for a large financial services and insurance provider. He is located in Bristol, U.K.

PHOTO TOP BY GEORGE DIEBOLD



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

CSSLP[CM]

Certified Secure Software Lifecycle Professional

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

20 (ISC)² years of excellence

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®