InfoSecurity PROFESSIONAL®

ISSUE NUMBER 12

An (ISC)² Digital Publication

www.isc2.org

Building Credibility with the Business

It's critical to understand what the business wants to hear before making security investments.

INTER SEC

where secure minds meet

Join InterSeC!

www.isc2intersec.com

The community where secure minds meet.

Don't miss out on the conversation. Collaborate with other security professionals for career advice, projects, best practices through groups, wiki's, blogs, etc.

LATEST NEWS

Stay updated with the latest from others on InterSeC.

GROUPS

Join one of the 100's of groups on InterSeC. You can also start a group, post discussions and upload files.

STAY CONNECTED

Access InterSeC from anywhere in the world on your iPhone. Go to **www.isc2intersec.com** on your iPhone.

NETWORK WITH THOUSANDS OF SECURITY PROFESSIONALS AROUND THE GLOBE.

(ISC)²®

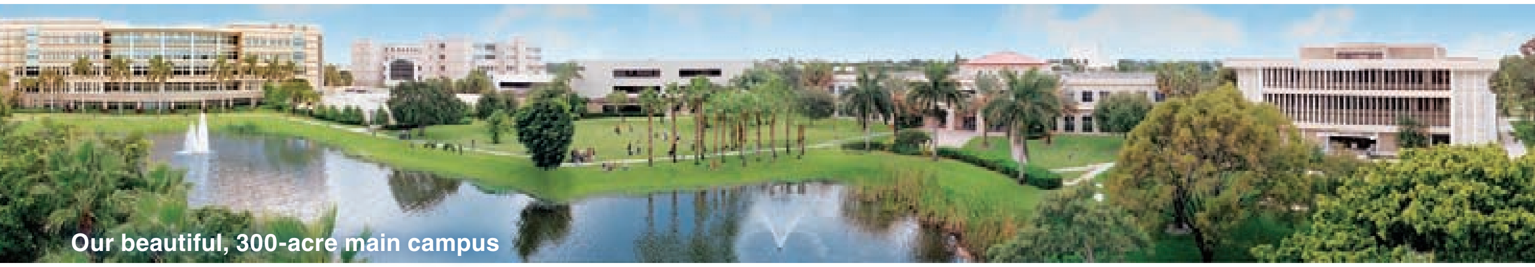
issue 12

2010 VOLUME 4

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

COVER PHOTO BY SIMON POTTER/CULTURA/CORBIS; ABOVE PHOTO BY ANDREY TSIDVINTSEV

InfoSecurity Professional is published by IDG Enterprise Custom Solutions Group, 492 Old Connecticut Path, Framingham, MA 01701 (phone: 508 935-4796). The information contained in this publication represents the views and opinions of the respective authors and may not represent the views and opinions of (ISC)² on the issues discussed as of the date of publication. No part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of (ISC)². (ISC)², the (ISC)² digital logo and all other (ISC)² product, service or certification names are registered marks or trademarks of the International Information Systems Security Certification Consortium, Incorporated, in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. For subscription information or to change your address, please visit www.isc2.org. To order additional copies or obtain permission to reprint materials, please email infosecproeditor@isc2.org. To request advertising information, please email tgaron@isc2.org. © 2010 (ISC)² Incorporated. All rights reserved.


Our beautiful, 300-acre main campus

executive letter

FROM THE DESK OF THE (ISC)^2 BOARD CHAIRPERSON

Moving Forward

WITH THE INSTITUTION OF A NEW CHARITABLE FOUNDATION, (ISC)^2 SETS ITS SIGHTS ON THE FUTURE.

MOST ORGANIZATIONS are now closing the books on 2010 and are looking forward to the new year. We, too, at (ISC)^2 are focusing on new horizons—not just for 2011, but also for the coming decades and generations of members.

(ISC)^2's mission is to make society safer by improving the productivity, efficiency and resilience of information-dependent economies through information education and certification. We are constantly seeking ways to enable our members to improve safety in their communities, while also enhancing their own skills and expertise.

That's why we are pleased to announce the creation of the (ISC)^2 Foundation. (ISC)^2 has for many years provided funding and resources for goodwill initiatives around the world. Based on overwhelmingly positive member feedback, we have decided to formalize these efforts by establishing a structured, non-profit entity. This entity will ensure that (ISC)^2 remains committed to and financially supportive of goodwill initiatives.

In many cases, this foundation will enhance and move forward projects we have already established—including the Safe and Secure Online program and scholarship program.

In addition, the foundation will enable us to better identify and provide resources for avenues that improve the safety of our communities and foster the growth of the information security profession. We'll update you on our progress and ways that you can get involved.

As we close the year, I want to acknowledge our passionate, dedicated volunteers around the world. From item writers to exam proctors and supervisors to Safe and Secure Online presenters, I want to thank you for the difference you're making not only in the lives of your peers but also of the people in your community.

There is certainly cause for excitement as we move into 2011 and the new decade. As always, we are committed to providing you, our members, with tools and resources to ensure that you remain competitive in your careers. We welcome your feedback and suggestions on how we can improve your membership experience.

Happy New Year!

Diana-Lynn Contesti
CISSP-ISSAP, ISSMP, CSSLP, SSCP
Board Chairperson, (ISC)^2

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
Corporate Communications Specialist
727 785-0189 x242
adalessandro@isc2.org

Sarah Bohne
Senior Communications Manager
616 719-9113 ▪ sbohne@isc2.org

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

Sales Team

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

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

Mike Walker
Regional Sales Manager
U.S. West Coast and Asia
213 896-9210 ▪ mwalker@isc2.org

IDG Media Team

Charles Lee
Vice President, Custom Solutions Group

Amy Freeman
Project Manager ▪ afreeman@isc2.org

Anne Taylor
Managing Editor ▪ ataylor@isc2.org

Kim Han
Art Director

Lisa Stevenson
Production Manager

CSO
Custom Solutions Group

ADVERTISER INDEX

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

[fyi]

(ISC)² MEMBER NEWS

(ISC)² Executive Director W. Hord Tipton welcomes Ireland State Minister John Curran TD to the first Irish member reception this past October.

A First in Ireland

(ISC)² kicked off the first Irish member reception in Dublin, Ireland on Oct. 14 with a special guest speaker: John Curran TD, Minister of State at the Departments of the Taoiseach and Defence with special responsibility as Government Chief Whip.

Setting a Benchmark

CSSLP®

Certified Secure Software Lifecycle Professional

ANSI

ISO/IEC 17024

THE CERTIFIED SECURE SOFTWARE LIFECYCLE PROFESSIONAL (CSSLP®) credential has been accredited by the American National Standards Institute (ANSI) and the International Organization for Standardization (ISO).

Being accredited under ANSI/ISO/IEC Standard 17024 establishes the CSSLP as a global benchmark for information security.

"As the first information security certification organization to have a credential—the CISSP, accredited under ANSI/ISO/IEC Standard 17024—we are proud to again be recognized for our dedication to providing information security professionals the gold standard in credentials," says W. Hord Tipton, executive director of (ISC)².

Leaders Honored

(ISC)² RECENTLY ANNOUNCED the winners of its seventh annual U.S. Government Information Security Leadership Awards (GISLAs). Winners are recognized for their initiatives to significantly enhance the security posture of a department, agency or the entire federal government.

CATEGORY: **Federal Contractor**

Individual Award: Kenneth A. Buszta, CISSP-ISSMP, federal contractor with Integrity Applications Inc.

Team Award: The Military Satellite Communications Systems Wing Certification and Accreditation team, comprised of 15 highly trained and certified professionals.

CATEGORY: **Workforce Improvement**

Individual Award: Thomas W. Schankweiler III, CISSP, chief information security officer, Office of the Secretary, Department of Health and Human Services.

Team Award: The National Defense University "Assuring the Information Infrastructure" team, under the leadership of professor Mark Duke.

CATEGORY: **Technology Improvement**

Individual Award: Kenneth Kurz, CISSP, chief of the National Cryptographic Solutions Management Office, National Security Agency Information Assurance Directorate.

Team Award: The Lightweight Portable Security team at the U.S. Air Force, led by senior software protection engineer Rich Kutter, inventor and lead developer of the Lightweight Portable Security (LPS) security solution.

CATEGORY: **Community Awareness**

Individual Award: Erich Fronck, SSCP, Network ISO at the Department of Veterans Affairs.

Team Award: The Global Cyber Security Management team at the U.S. Department of Homeland Security.

CATEGORY: **Process/Policy Improvement**

Individual Award: April Giles, CISSP, program manager and chief architect of the General Services Administration's FIPS 201 Evaluation Program.

Team Award: The Defense Business Systems Acquisition Executive team at the Business Transformation Agency for the Department of Defense.

Discover each individual's and team's achievements at **www.isc2.org/gisla**. Photos are available on (ISC)²'s Facebook fan page (www.facebook.com/home.php?#!/isc2fb), and video interviews are on YouTube (www.youtube.com/isc2tv).

Director's Notice

EVERY YEAR, (ISC)² RECOGNIZES volunteers for their contributions to the organization through (ISC)² President's Awards. This year's recipients include:

- James Molini, CISSP, CSSLP
- Art Friedman, CISSP
- Devon Bryan, CISSP
- Richard Harrison, CISSP
- Phil Lamb, CISSP
- Kevin Gourlay, CISSP
- Eamonn McCoy, CISSP
- Tim Wilson, CISSP
- Steve Hindle, CISSP
- Martin Reynolds, CISSP
- Wo Sang Young, CISSP
- Henry Ng, CISSP-ISSAP
- Howard Lau, CISSP
- Mano Paul, CSSLP
- Dr. Meng Chow Kang, CISSP
- Anthony Lim, CSSLP
- Edmund Chua, CISSP

Awarding Sustained Contributions

(ISC)²'S HIGHEST HONOR, the Harold F. Tipton Lifetime Achievement Award, has been given to Lt. Col. Husin bin Jazri, CISSP.

The award is given annually to recognize an individual who is dedicated to carrying on Tipton's tradition of passionately promoting and enhancing the information security profession. Husin has raised security awareness throughout Malaysia and set a benchmark for cyber security, including the establishment of a national cyber security hotline.

In addition to the Tipton award, (ISC)² recently recognized Richard Nealon, CISSP, SSCP, with the 2010 (ISC)² James R. Wade Service Award, which acknowledges volunteers who have made a sustained and valuable contribution to the organization. As one of the first CISSPs in Ireland, Nealon has been a significant test development contributor and member of the (ISC)² Board of Directors and European Advisory Board.

For more information, visit: **www.isc2.org/awards**.

(ISC)²'s Information Security Scholarship Program Returns

(ISC)² HAS EXPANDED its Information Security Scholarship Program and now offers more than 35 opportunities worth a total of up to US$100,000 for scholars attending and faculty members teaching at regionally accredited academic institutions around the world. It includes four grant categories:

- **Travel Grants for Research Presented at Conferences:** for qualifying scholarship recipients to present their research papers at information security conferences (up to US $3,000 per recipient)
- **Faculty Certification Exam Vouchers:** vouchers for one CISSP or CSSLP® exam and, upon certification, the first year of annual maintenance fees to qualifying faculty members
- **Graduate Research Project(s):** for qualifying junior faculty members and doctoral students conducting research of significance to the industry and society (up to US$3,000 per recipient)
- **Graduate Research Equipment Grant:** for one qualifying full-time Ph.D. student or a faculty/academic staff member (up to US$30,000 within their first five years of graduation to fund purchase of equipment for their university that is not currently available to them and needed for established research)

Please note that the scholarship application period closed on Oct. 31 for all categories except Travel Grants, which is open year-round. Scholarship recipients will be announced soon. For more details, visit **https://www.isc2.org/scholarship**.

Don't forget to take the quiz and earn CPEs:
http://bit.ly/dCpsbG

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

Moderator's Corner

BY BRANDON DUNLAP

WE HAVE BEEN RUNNING the ThinkT@nk series over the past six months, which has generated a great deal of interest in managing security requirements between traditional IT and cloud-based solutions. There is a fracturing of the data center, driven by economic and business requirements, and yet for many organizations, security requirements are still catching up. To address the concerns of (ISC)² members, we decided to tackle this topic from a few different angles.

In June, we kicked off with a discussion on "Managing Split Security in Cloud Services and the Data Center." The archived file can be found at http://bit.ly/ameExR. In this Web roundtable, panelists discussed the ways in which many security monitoring and assessment functions in the cloud aren't meeting the same level of rigor as those in data centers. We explored strategies for addressing these concerns and improving the visibility necessary in these hosted environments.

The conversation shifted to managing identities across the fractured data center in the October roundtable (archived version at http://bit.ly/bxb597). Presenters shared their insights into bridging identities and access controls between the enterprise and the cloud environment. One of the panelists, Matt Chiodi of Deloitte Consulting, recommended a presentation his colleagues put together on this topic. (ISC)² members can view it at http://slidesha.re/9srzPo.

As we near the end of 2010 and the beginning of 2011, watch for additional discussions and knowledge sharing about the fractured data center—including how to prioritize business needs while maintaining security requirements.

I look forward to hearing what new topics you would like to see included in the events calendar, as well as your insights into the information security profession.

Best wishes,
Brandon Dunlap
Managing Director of Research, Brightfly
bsdunlap@brightfly.com

BALANCE
Risk with Reward

TURBULENCE in the Clouds

There are compliance and risk management dangers in cloud computing.

Cloud services are gaining in popularity thanks to business benefits including cost savings, improved time to market and the ability to speed up innovation. However, few standards exist (the Cloud Security Alliance, a worldwide nonprofit organization that promotes best practices in security assurance in cloud computing, is making strides toward establishing industry-wide standards—but they're not there yet), and that presents a considerable problem for information security professionals looking to implement and maintain cloud services.

PHOTO BY ANDREY TSIDVINTSEV

Security experts warn of data compliance and risk management dangers when procuring cloud services, reports Peter Fretty

Cloud Definitions*

Private cloud: infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Public cloud: infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud: infrastructure is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

* as defined by the National Institute of Standards and Technology IT Lab

TRANSPARENCY IS A MUST

Businesses must take precautions when entering into cloud-based service agreements. They need visibility into cloud providers' processes and systems to maintain necessary IT governance, says Jim Reavis, executive director of the Cloud Security Alliance. "You cannot outsource governance, risk and compliance," he says. "It is also important to understand that to a large degree, focus must be on the data: where it is located, what regulations are applicable and how it is being protected. A coherent architecture is also important to achieve portability and interoperability between different cloud providers."

The key, says Irfan Saif, a principal with Deloitte Consulting LLP, is to gain an understanding of what the provider is doing behind the scenes. "Find out how they are managing their offering, what controls are in place, and how they can provide assurance given there is not

Questions to Ask Cloud Providers

It's crucial to have a comfortable working relationship with a cloud service provider for ongoing success. Kathy Owen, senior vice president and global CIO at Chattanooga, Tenn.-based Unum, a large insurance company, recommends asking some critical questions before entering into a contract or agreement:

- Who has access to the data?
- How many employees have root, database and infrastructure access?
- What policies are in place to prevent the cloud provider's employees from getting access to your company's data?
- Is the data encrypted at rest and in motion?
- Is the environment a multi-tenant one and if so, what controls data segmentation?
- Will data be stored on servers in other countries? If so, how does this impact compliance?
- What controls are in place to prevent data loss (i.e., a vendor insider downloading customer data on a USB drive)?
- What information is captured in audit/security event logs and is it available to the customer?

"When you are charged with the protecting organizational data, there needs to be several security measures in place including: strong authentication controls such as two-factor authentication and IP address restrictions to prevent a user from transmitting data from a non-company network; data encryption for data at rest, data transmission and backups; data segmentation, either physically or logically; and access control logs to show who accessed the data and when," says Owen. "Always make sure you are comfortable with what the vendor provides."

a prevailing standard," he says. When you work with a provider, you typically have a point person managing your organization's data, "who has access to things that in a traditional world you would have managed internally. In these instances, there needs to be not only the contractual pass-through, but also a way to somehow validate that the provider is following outlined practices and managing the appropriate risks on your behalf. This becomes increasingly important when managing compliance risk."

Visibility should also include access at a granular level, including the actions of privileged users, says Slavik Markovich, chief technology officer of Sentrigo, a Calif.-based database security software provider. "As a case in point, the recent Google disclosure that an engineer had viewed the private chat and Gmail of a user shows that this not only is possible, but likely occurs regularly," he says. "The more frightening point is that the privileged user is often able to cover their tracks, deleting or modifying log files to eliminate records of their access. Only with more sophisticated tools that ensure separation of duties can this be prevented."

PLANNING FOR RISKS

One way to head off pitfalls is to look at risk across the enterprise, with cloud being one channel. Saif says this enables a company to maximize cloud benefits while gaining broad visibility. It's important to determine whether to utilize public, private or hybrid cloud environments (see Cloud Definitions on page 9). The approach must fit the organization's requirements and in-house capabilities while meeting its needs for improved time to market, lower total cost of ownership and a timely return on investment.

Understanding the risks of each option is the key to success. With public clouds, servers are often shared between applications, introducing potential threats not present with dedicated hardware. "Administrators and developers with privileged access to one application may be more easily able to misuse access, affecting a broader range of systems," says Markovich. "Since you can't conduct background checks yourself on third-party personnel, you'll want assurances that the cloud provider meets certain criteria, such as SAS 70," an in-depth auditing standard.

In theory, private clouds seem to be the safer option because they offer the ability to retain control over physical assets. But many companies lack the resources to manage private clouds cost effectively, and there are some compatibility risks to consider. "The reality is that most organizations will be using services in multiple clouds, and will be managing hybrid cloud environments," says Reavis.

ESTABLISHING GROUND RULES

Before entering into a partnership with a cloud provider, get a clear understanding of service-level agreements and functionality. "The procurement and contract negotiation phase may be your best bet to getting the security guarantees you need," says Reavis.

Confirm whether the provider is maintaining its systems at the latest patch levels, adds Markovich. "It is often difficult to bring down production servers to implement recent patches to the operating systems, databases and other infrastructure software, yet these are very easy targets for hackers," he says. "Knowing that an application uses a certain piece of software, and that the vendor just issued a patch for a specific vulnerability, the hacker now knows exactly how to break in—at least until the patch is applied."

Another piece of advice: Understand how the provider handles physical copies of data. For example, if a drive goes bad in their storage farm and it is replaced, what happens to the old drive? How does the vendor ensure it is rendered unreadable? "The big players certainly have policies for this, but when you trust sensitive information with a smaller provider, a single lost drive could cause significant damages," says Markovich.

Many companies already have sensitive data outside their enterprise, via Software-as-a-Service (SaaS) applications such as salesforce.com or NetSuite. Typically, SaaS vendors have policies in place to prevent even their own privileged insiders from viewing your company's data, as well as controls to protect multi-tenancy environments. But you should investigate and ask questions.

"For example, can the administrator managing the backend database for your SaaS application make a copy of all the credit card numbers you've entered with orders?" Markovich asks. "Also, can the system administrator for that server you're sharing with an unknown number of other companies in your cloud infrastructure simply make a backup copy of the drive with the Social Security numbers of every employee in your company? Before putting this data on these systems, you should understand how the provider will protect these cases, as your own compliance team will likely want to know."

INTERNAL AFFAIRS

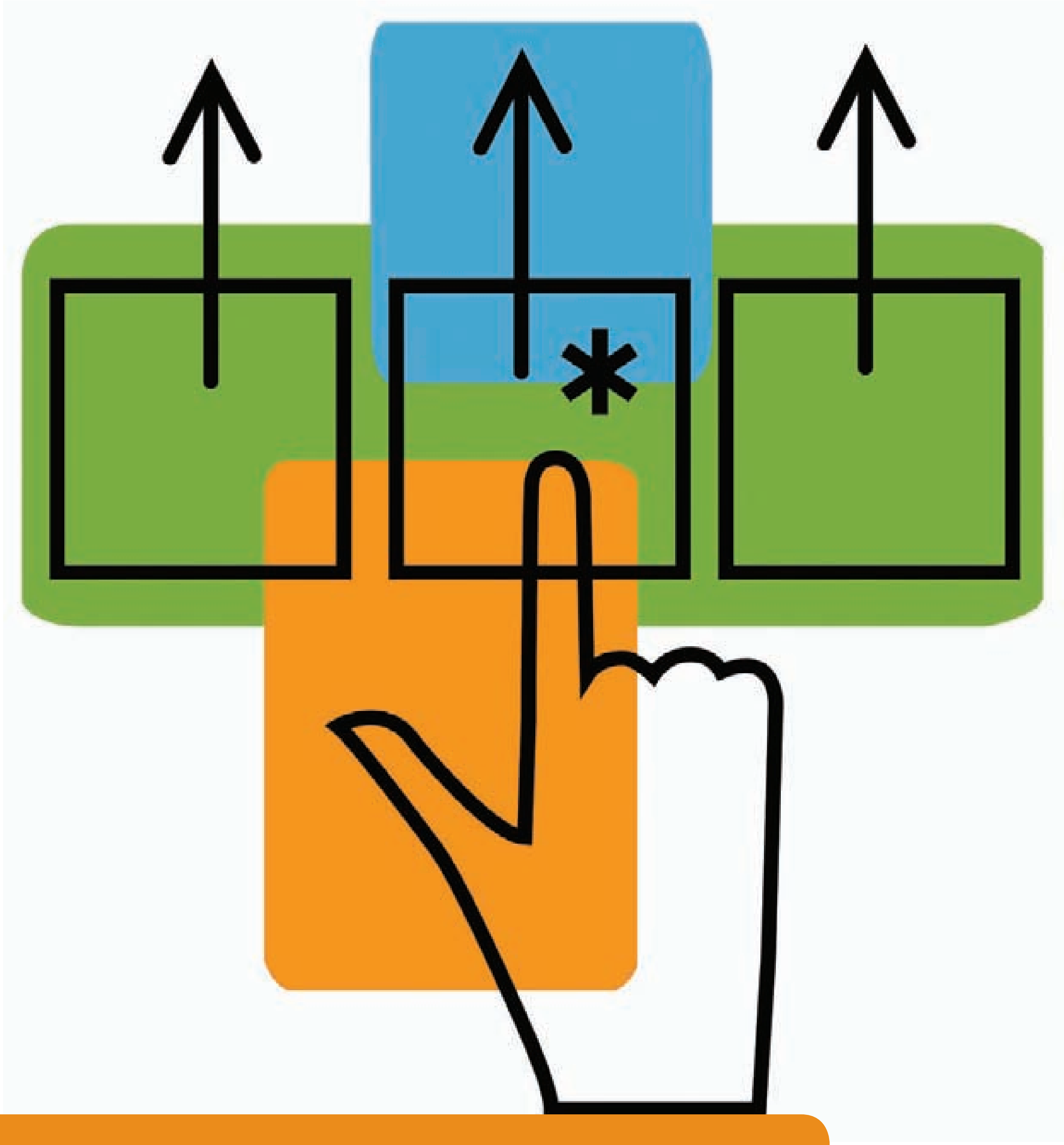
Don't overlook the need to tackle cloud compliance issues internally, too. Training and awareness are crucial elements. "Employees cannot just do things in a cloud environment without thought. A lot of security-related challenges are often inadvertent, which is why awareness in the cloud environment is so important," says Saif. To that end, heighten awareness among employees enterprise-wide about what information can be sent to cloud providers in light of organizational policy and regulatory requirements.

Meanwhile, IT needs to granularly monitor applications to ensure policies are enforced. "If it is possible to encrypt information before transmitting, by all means [IT] should do so," Reavis says. "In the long run, interesting developments such as format-preserving encryption have great promise to automate protection and prevent information outside of the enterprise from being compromised."

Without training and awareness, business units and departments will continue to obtain services without IT's involvement. "The enterprise compliance requirements need to be crystal-clear so more parts of the enterprise talk to IT directly rather than procuring cloud services on their own," Saif says. "Often, employees will go out and procure services on their own because it helps them achieve faster time to market and they feel like they do not need IT's permission. Yet this fractured approach creates real challenges and often results in a loss of cost benefit."

While there are potential pitfalls, cloud services represent a beneficial way for IT leaders help their companies gain new efficiencies. The key to success rests in understanding the compliance issues and talking openly with cloud service providers.

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



TAKING A LEAD ON CHANGE

INFORMATION SECURITY PROFESSIONALS SHOULD TAKE LEADERSHIP ROLES TO MANAGE CHANGE IN THEIR ORGANIZATIONS.

ILLUSTRATION BY JUDITH GOSSE

Economic and social factors are influencing the security industry.

Bill Snyder asks: **How will information security professionals manage these changes?**

Your senior vice president is on a flight to Asia reading the in-flight magazine when he notices an article on how useful the latest smartphone is in business. By the time the plane lands he has drafted an email authorizing the use of iPhones and Androids on the corporate network.

Never mind that there's no plan to roll them out nor, more importantly, a plan in place to secure them. "Business groups want things done immediately, but they may not understand the ramifications of bringing in new technologies," says Jerry Pittman, CISSP, global information security strategy officer for General Motors.

With the worst of the recession over, security management is coming to grips with a new environment of thin resources and pressure to make "business alignment" more than just a buzzword. What's more, there's a disconnect between traditional information security practices and the demands of an increasingly youthful workforce that feels entitled to use personal technology and social networking in the office.

And because of the heightened merger activity this year, security (along with the rest of IT) will be confronting an influx of new users, technologies and systems. Security managers are entering a period of rapid change that will test their leadership ability more than ever before. "We think the leadership aspect in managing change is as important as technology and process issues," says Ted DeZabala, national leader of Deloitte's Security and Privacy Services practice.

The first step in understanding how to lead in this new environment is to think about something you don't like to think about: failure. "Why do organizations fail? When there's a failure, people don't have an accurate view of the situation, or they don't know where they are going or don't have a workable plan that can be implemented," DeZabala says.

There are three overarching principles to keep in mind, adds DeZabala:

- **Carry out** a thorough situational analysis of where you are and what you want to transform. Too many organizations use opinions and anecdotes instead of fact-based analysis.
- **Be clear** about your goal and know what the desired state actually looks like. Have a clear definition of deliverables.
- **Understand** that doing the analysis also means understanding how to bring your team on the journey. When you have broad support, you won't have to manage every little detail yourself.

It's also important to realize that *not everyone will make it*—that is, people resist change. "Some are incapable of coming along because they don't have the right skills or just can't accept a new environment," says DeZabala. When that's the case, you've got to be tough. "Passive resistance is the death of an organization. When the person leading the transformation has provided the information and has set up accountable structures, you can no longer tolerate resistance," he says.

METRICS ARE FUNDAMENTAL

Making an objective analysis isn't easy when you're using the wrong metrics, says Brandon Dunlap, managing director of research for Brightfly, a security consultancy. "Security people spend much of their time trying to check the score, thinking how many vulnerabilities did we squash today and how many yesterday," he says.

In one sense, there's nothing wrong with this. You certainly need to know what and how many threats you're dealing with. But information security professionals must think of their job as business-focused. Squashing bugs is important, but it should never be separated from the top- and bottom-line success of the business. And your metrics should reflect that.

- Rather than just cataloging threats, counsels Dunlap, think about which threats actually could damage the core business of your enterprise. "If my accounting system has vulnerabilities that take a month to close, and vulnerabilities in

> **"Passive resistance is the death of an organization.** When the person leading the transformation has provided the information and has set up accountable structures, you can no longer tolerate resistance."
>
> – Ted DeZabala
> Deloitte's Security and Privacy Services

my print server are closed in a week, something is wrong," he says. Or as Adam Rice, vice president of managed security services for Tata Communications, puts it: "Don't just think risk; think about risk to revenue."

- In an environment where threats morph at lightning speed and business has little tolerance for malware-related downtime, your testing process has to be as quick and efficient as possible. "How long does a patch spend getting tested before deployment? If it's too long, you may be over-testing and wasting time," says Dunlap.
- Find out how long it takes to get a given vulnerability patched across the business. Do you really need to patch it everywhere? It could be that a patch of just 80 percent of the servers is enough to meet your company's risk management goals.

> "... **there are often good reasons to say no when security is at stake,** but too many information security professionals are unwilling to grasp the potential business value in a technology or process that seems risky."
>
> – Larry Miller
> senior IT manager for a large retailer

Are you collecting data on potential threats in a systematic way? One way to ensure that the job gets done is to create a cyber intelligence group within your company, says Rice. Tata is large enough to have a cyber intelligence division. If your company isn't that big, you can designate people to collect intelligence—and be sure their job descriptions (including bonus plans) reflect that responsibility.

In either case, says DeZabala, "you need to build that unit into the fabric of the organization. Once data is analyzed it must be spread to the right people with actions attached." If, for example, the intelligence unit becomes aware of a keylogger attack on a customer, it might alert the customer's account rep and have him or her pass on the corrective measures. It doesn't do much good to sound the alarm without telling people what they need to do.

LEARNING TO SAY YES

"You're probably tired of hearing this, but to line-of-business folks, security managers might as well be Dr. No. Sure, there are often good reasons to say no when security is at stake, but too many information security professionals are unwilling to grasp the potential business value in a technology or process that seems risky," says Larry Miller, a senior IT manager for a large retailer.

Prior to his current job, Miller worked as an IT manager for a large law firm where "our marketers wanted to use social networking apps like Facebook and Twitter, but IT was afraid of it," he says. Although Miller has been working in IT for more than two decades, he comes down on the side of the new technology: "IT shouldn't get in the way of business. It should build it."

One reason security and business professionals are often at loggerheads may be rooted in birthdays. There's a growing age gap between security and the rest of the workforce, says J.J. Thompson, a partner in Rook Consulting, a risk strategy firm based in San Jose, Calif. "The average age of the security pro is not decreasing as fast as the average business user. This tells me that we are not attracting as much young blood to the industry as I would have expected," he says.

Generational difference isn't the only issue. Take a look at the organizational chart for many large businesses—chances are the CSO doesn't report to the CEO or even the COO. That's not an accident. "Security doesn't have the standing; it hasn't demonstrated enough business value to the organization," says Thompson. If security wants a seat at the decision-makers' table "it has to understand what the direction of the executive team is and map directly into those objectives," he adds.

Organizational charts aside, communication between security and lines of business is key. But it has to be more than just talk. "There needs to be a structure in place to facilitate that," says Pittman. He suggests placing members of the security team inside business organizations to function as liaisons. It's also possible to turn that suggestion around and place business staffers within the security group. In either case, there's a chance to institutionalize communication and bridge difficult cultural and generational gaps.

Finally, now that many enterprises are starting to recover from the recession, you must be honest about what the downturn has done to your organization. "Expose the true state of your infrastructure—however bad it may be—and make sure that rectifying whatever high-risk problems you may have rises to the top of management's agenda for recovery spending. If you wait until the recovery is in full swing and the business has already committed capital to new projects, you'll be too late," wrote Matt Prigge, the systems architect for the SymQuest Group, in a blog post for *InfoWorld*.

You may not be able to keep your boss from getting impractical ideas while he jets around the world. But you can manage change.

San Francisco journalist Bill Snyder writes frequently about business and technology.

Start Your Adventure and Save!

Secure your place at RSA® Conference 2011, and stay one step ahead of the challenges that face the information security industry.

- **Expand your knowledge** with 200+ key industry-focused sessions, including network security, identity management, cloud computing, Web 2.0 security and more
- **Learn how new regulations** and constantly evolving compliance rules affect both the industry and your job
- **Demo the best technologies** and discover what's new and upcoming from over 350 exhibiting security companies—including (ISC)^2
- **Network with thousands of peers**, industry leaders and security luminaries
- **Receive an additional discount** off the registration fee as an (ISC)^2 member, plus an invitation to an exclusive reception and 25 CPE credits

Follow the Adventures of Alice & Bob at
www.rsaconference.com/aliceandbob2011

RSA®CONFERENCE2011

FEBRUARY 14-18 | MOSCONE CENTER | SAN FRANCISCO

20 YEARS

www.rsaconference.com/isc2

*** Register now and use the qualification code 1211ISCDL2A to receive the additional $200 discount on the Standard Registration rate for a total of $600 in savings for (ISC)^2 members.**

BUILDING Credibility with the BUSINESS

It's critical to understand what the business wants to hear before making security investments.

When Carlos Mena, senior director of global IT security at Sitel (a worldwide provider of outsourced customer contact center services), asks for money, he doesn't hear the word "no" very often. When he does hear it, he tries to figure out where he failed.

Several years ago, Mena was the new security manager at a multinational corporation. One of his first tasks was to interview business unit directors to understand the maturity of their security programs and assess their needs. A couple of minutes into one of his first meetings, a director interrupted and asked, "Why are we doing this? I don't have any security issues."

"If I left it at that, it would have been a disaster," says Mena. "So I did my homework, worked the data and researched incidents in that business unit over the past several years. It turns out that a few years earlier, an employee had broken into a computer and impacted the production line."

He created a security plan for the unit and met with the direc-

PHOTO BY SIMON POTTER/CULTURA/CORBIS

If you need to secure funding for a project, you'd better be prepared to address the issues that matter to the business and finance teams, discovers Manya Chylinski.

tor again. "I presented the plan, emphasizing the impact of this past incident on his business. In less than two minutes he was sitting up straight, listening and engaged."

Build Credibility

Most information security professionals have to work with business unit directors, finance teams, budget committees and chief financial officers to obtain funding approval for security projects. And no matter how obvious the need may seem, they're not interested in the technology. They're interested in what it does for the business—and how it affects the bottom line. Getting approval is about how well you communicate with the people who hold the purse strings.

"When you're talking to businesspeople, half the battle is understanding the audience," says Marilyn Weinstein, founder and CEO of Vivo Inc. Weinstein advises IT security personnel in the Silicon Valley area on this topic.

Procuring funding for a security initiative or department budget starts long before you write the business case or present to the budget committee. From data loss prevention and identity and access management to risk management and compliance initiatives, your job is to help others see the situation through your eyes.

"Security isn't fear mongering; it's driven by business," says Mena. "Every time you shout 'the sky is falling,' management starts to filter you and you lose credibility. Do the rounds. Get buy-in from key stakeholders. Think of finance as your partners. It's all influencing, partnering, and how evangelical you are."

There is homework to do before you create a budget or funding request. Every day, you have to build and maintain your credibility. Learn about the business and how IT security affects both revenues (for example, glitches that cause abandoned customer orders) and expenses (such as the security product that will fix those glitches). Understand the industry regulations and governance issues. Keep abreast of new developments in the IT security sphere.

Align Yourself

As you develop and nurture an understanding of the business, you should also build partnerships and alliances with key personnel throughout the company. This will help you see the business from different angles and get buy-in earlier in a project's lifecycle. You'll get a clear sense of how your company prioritizes security, and the types of projects that bring the highest value.

It's important to effectively manage the projects currently on your plate. Large or frequent overruns indicate you don't understand the true cost or scope of projects. "Be honest about what things really cost," says Ted DeZabala, national leader of Deloitte's Security and Privacy Services practice. "Not just external costs, but also incremental operational overhead resulting from the implementation.

"Also, emphasize business benefits and cost offsets, such as new sources of revenue or reduced administrative costs in areas outside security," he adds. "It's important to illustrate the P&L impact over time, especially if certain aspects of the investment can be capitalized. And finally, let's not forget about tax savings from R&D credits, transfer pricing, etc."

Deliver the Message

The starting point for a business case is creating the right message for the audience. "The best way to break through the clutter is to ask yourself: what's important to the listener," notes Weinstein. "Then, don't over-dramatize. Go with simple, easy-to-digest data."

Start with an analysis of the current situation. Support that with succinct, fact-based, business-driven data, highlighting any urgencies, deadlines or regulatory requirements. Then emphasize your understanding of the business and its vulnerabilities.

When it comes to requesting funding for large, multiyear projects, you have to think strategically. Decide whether it makes sense to go for one big initiative with a large price tag or smaller, less expensive projects that can give you quick wins.

Another effective way to get funding is to make a business case for a security component in a larger IT project, such as ERP implementations. "Those are usually driven by the CFO, with IT playing a supporting role," says DeZabala. "It's much easier to add a little more to the price tag of another project, such as implementing security elements to make it work appropriately."

As for the format for your presentation, you should tailor it to what your audience expects—and those expectations will differ by individual and by group. If you use a nontraditional format, even one you think is superior at communicating the information, it's likely that someone will question it and never get to the content.

When asking for funding, you are the evangelist. It's your job to help management understand how this initiative or budget item will protect the company, and illustrate clearly how a loss or security breach would damage it. "Understand the business and business drivers," says Mena. "Know your audience. Hone your marketing and sales skills. Do your homework. You're presenting to businesspeople interested in the bottom line."

You have to be prepared.

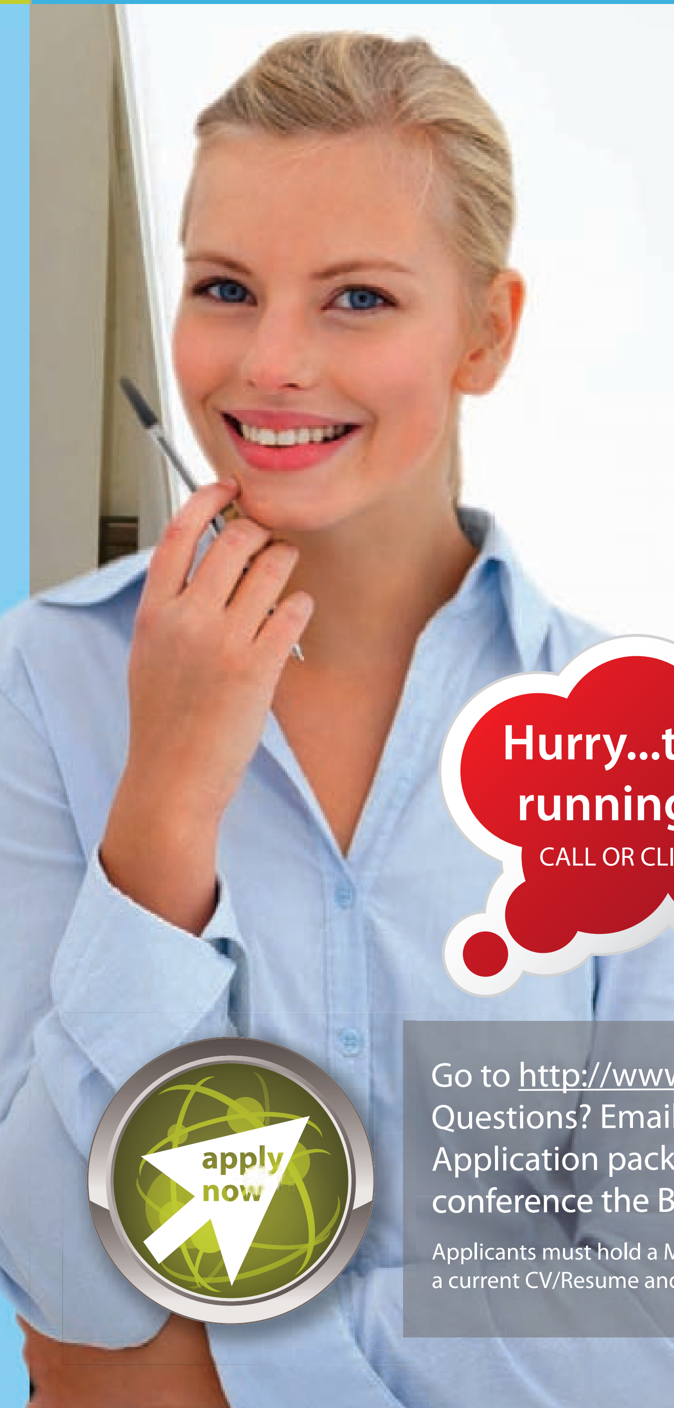
Manya Chylinski is a freelance writer based in Massachusetts.

CONTACT: +1 (703) 637.4424 | www.theBCIcertificate.org

Business Continuity
Institute

Alternative Route to Membership Program

What has your MBCP, CBCP or ABCP done for you lately?



MBCP, CBCP or ABCP will be considered for membership of the BCI

The Membership Council of the Institute has carefully examined other BCM credentials, mapping them against BCI certification, and felt it was appropriate to extend an invitation to join the BCI to those who hold respected credentials. The certification of MBCP, CBCP and ABCP have been identified as credentials whose foundations are broadly in line with the requirements or the AMBCI and/or MBCI certifications. Recognized as a validation of experience and knowledge, professionals that hold MBCP, CBCP or ABCP certifications and are in good standing are invited to apply for membership of the BCI without having to pass BCI's official certification exam.

Hurry...time is running out!

CALL OR CLICK HERE

Invite them to join the BCI - the most respected BCM Institute the world over.

apply now

Go to http://www.thebcicertificate.org/alternative_route.html to apply.
Questions? Email: membership@thebci.org
Application packets will also be available at the booth at any conference the BCI attends.

Applicants must hold a MBCP, CBCP, or ABCP certification in good standing and will be required to submit a current CV/Resume and references. One time application fee: $75 USD + annual membership fees.

The Merge Surge

EXPERTS DISCUSS HOW THE RECENT MERGERS AND ACQUISITIONS OF SECURITY TECHNOLOGY COMPANIES WILL AFFECT CUSTOMERS.

THERE HAS BEEN A SPATE of security company acquisitions this past year, including Intel's purchase of McAfee; HP's acquisitions of Fortify and ArcSight; IBM's BigFix buy; and Symantec's purchase of VeriSign. Rob Ayoub, global program director of network security at research analyst firm Frost & Sullivan, and Bob Bragdon, publisher of *CSO* magazine, offer insights into how these acquisitions affect information security professionals.

Q: How do these acquisitions affect customers?

Ayoub: Large enterprises are usually the most affected. They have typically invested the most and have the most to lose should the acquisition result in a drastic change to the product or service. For small and medium businesses, it can still be disruptive to have a technology they depend on acquired, changed or discontinued. Small businesses in particular may not be able to bear the cost of new investment.

Bragdon: Regardless of the size of the business, the company should be prepared to see changes in the way they interact with the vendors. Some of these mergers and acquisitions go better than others. The trick is how well the acquiring company integrates the acquired company into its product set. We usually don't see too much change in product or positioning for at least three calendar quarters.

Q: What should security professionals ask if one of their vendors is acquired?

Ayoub: Security professionals need to ask their vendor about the short-term changes, and should keep in close contact with the vendor as the transition occurs. They may not get much information initially, but it will show their concern about being supported. Next, they should talk internally and gauge how much their organization depends on the existing product. Finally, upper management should be apprised of the situation to understand change implications, discontinuation of a product or quality of service, and potential alternatives.

Bragdon: Speak with the acquirer and the acquired and ask why the deal was done. Surprisingly, you will often get different answers. Ask about timelines for the acquisition, plans for how the business will be integrated into the acquiring company, and what effect this will have on existing contracts and future product roadmaps. Make sure you are comfortable with what they are doing and, if you are not, then tell them. They want to hear this from you. No one drops millions of dollars on an acquisition and wants to then see the customer base walk away.

Q: How do these acquisition trends affect the global security technology market?

Ayoub: In some cases, acquisitions are good for the industry—allowing good products to become better, and improving the distribution and penetration of those products. On the other hand, there are plenty of examples of acquisitions that were ineffective and caused good products to suffer.

Bragdon: There will always be a steady supply of startups addressing emerging security concerns that can do so faster and better than large businesses. That being said, the natural model in capitalism is that those start-ups will either grow and go public, or they will be acquired. One of the unfortunate side effects of Sarbanes-Oxley and related legislation around the globe is that the cost of going public is significantly higher than it once was. The net result is that you'll see more businesses be acquired as their initial investors look for exit strategies. (ISC)²

PHOTO BY IVAN STEVANOVIC

Rigor – not Rigor Mortis

FOLLOWING A FRAMEWORK WHEN IMPLEMENTING SECURITY IS BENEFICIAL, BUT BEWARE OF DEATH BY PROCESS.

USING A SECURITY MANAGEMENT FRAMEWORK such as ISO 27001 can bring many benefits. However, it can also introduce bureaucracy that results in a frustratingly slow security service. This ultimately crushes innovation, constricts agility, and diverts attention away from the bigger picture: information security professionals are engaged in a struggle against ever-changing risks that threaten the organizations they serve.

Using an industry standard security management framework helps information security professionals reliably and cost-effectively gain a clear perspective on the data they must protect. An organized, structured security program also has mechanisms that enable information security professionals to report on the project's current status and plans for improvement and updates over time. The ability to coherently and reliably report this information to management is essential to gaining their ongoing support.

However, if poorly deployed, the security management framework could end up in rigor mortis, unable to protect company data. Overly bureaucratic and inappropriately detailed security processes (e.g., security risk assessments and change management) can slow down the security service. The deployment of security controls may be delayed, which could leave systems vulnerable for a prolonged period of time and increase the risk of compromise. It may also cause frustration in other areas of the business. For example, the project team may not be happy if their project is delayed three months while they wait for a security risk assessment to be completed.

Business is constantly changing, and new security threats are continually emerging. An overly structured security management framework is less likely to be able to respond to those changes. For example, in many organizations it's not unusual for it to take six months to agree to and implement a policy or technology change for malware protection. Having a more flexible structure would enable security professionals to quickly address emerging security threats, which crop up quickly.

Another problem is that process-oriented security management frameworks usually lead to formulaic, standardized security controls and practices. While this is not always a bad thing, it limits information security professionals' ability to think creatively about security solutions and practices. Meanwhile, attackers are not restricted by policy or detailed processes—they are free to be creative and daring.

It is essential that information security professionals keep their eyes on those who would seek to damage their organization so they can understand their methods and ensure that security defenses are appropriately deployed. Rigorously defined and delivered processes are crucial for a strong information security framework. But if that framework is over-engineered, rigor mortis can set in, rendering the security service ineffective. Allowing space for flexibility and creativity releases information security professionals to effectively respond to the changing nature of the threat landscape. (ISC)²

Alex Clayton, CISSP, is the security and continuity service manager at 3i. He is based in Birmingham, England, and can be reached at alex.clayton@3i.com.

PHOTO TOP BY GEORGE DIEBOLD

CISSP®
ISSAP
CISSP®