VOLUME 6, 2012

ISACA® Journal

Cybersecurity and Risk Analysis

Featured articles:

The Changing Face of Cybersecurity

Using Scenario Analysis for Managing Technology Risk

Preparing for HTML5 Capabilities and Threats

And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG

Get recognized as an expert in your profession.

Résumés/CVs may *list* your experience and knowledge, but an ISACA® designation after your name *proves* it.

CISA® Certified Information Systems Auditor®
An ISACA® Certification

CISM® Certified Information Security Manager®
An ISACA® Certification

CGEIT® Certified in the Governance of Enterprise IT®
An ISACA® Certification

CRISC™ Certified in Risk and Information Systems Control™
An ISACA® Certification

Registration for the 8 June exam opens soon!

Early registration deadline: 13 February 2013
Final registration deadline: 3 April 2013

ISACA members save US $175 off exam registration!

Visit our web site for more information and updates at w*ww.isaca.org/certification-vol6.*

ISACA®
Trust in, and value from, information systems

KEEP YOUR **CAREER** ON TRACK

Regis University offers a graduate certificate as well as a master's degree in Information Assurance. With both programs, you have the option to take classes *online or on campus.* Regis University is also designated as a Center of Academic Excellence in Information Assurance Education by the National Security Agency.

INFORMATION ASSURANCE PROGRAMS

GRADUATE CERTIFICATE

- Can be completed in less than a year
- Four classes (12 credit hours)

MASTER'S DEGREE

- Two year program
- Specialize in cyber security or policy management

The curriculum is modeled on the guidelines and recommendations provided by:

- The Committee on National Security Systems (CNSS) 4000 training standards
- The $(ISC)^2$ Ten Domains of Knowledge
- ISACA

Classes can be taken on campus or completely online.

Regis University is an accredited, 130-year-old Jesuit institution in Denver, CO. Regis has been recognized as a national leader in education for adults and is committed to programs that are accessible and affordable. *U.S. News & World Report* has ranked Regis University as a Top University in the West for 17 consecutive years.

REGIS UNIVERSITY
School of Computer & Information Sciences

LEARN MORE

www.regisdegrees.com/ISACA | 855.508.8454

Volume 6, 2012

ISACA® Journal

Columns

Features

Plus

The *ISACA® Journal* seeks to enhance the proficiency and competitive advantage of its international readership by providing managerial and technical guidance from experienced global authors. The *Journal's* noncommercial, peer-reviewed articles focus on topics critical to professionals involved in IT audit, governance, security and assurance.

Read more from these *Journal* authors…

Journal authors are now blogging at *www.isaca.org/journal/blog*. Visit the *ISACA Journal* Author Blog to gain more insight from colleagues and to participate in the growing ISACA community.

Journal Online

Want more of the practical, peer-reviewed articles you have come to expect from the *Journal*? Additional online-only articles will be available on the first business day of each month in which no *Journal* is released, i.e., February, April, June, August, October and December. These articles will be available exclusively to ISACA® members during their first year of release. Use your unique member login credentials to access them at *www.isaca.org/journalonline*.

Online Features
The following articles will be available to ISACA members online on 3 December 2012.

A Strategic Framework for IT Disaster Recovery Assessments
Klaus Julisch, Ph.D., and Damian Walch

Book Review: Security Metrics—A Beginner's Guide
Reviewed by Upesh Parekh, CISA

Is the Business Network Connected to SCADA? Need for Auditing SCADA Networks
Ashwin K. Chaudary, CISA, CISM, CGEIT, CRISC, CISSP, PMP

Discuss topics in the ISACA Knowledge Center: *www.isaca.org/knowledgecenter*

Follow ISACA on Twitter: *http://twitter.com/isacanews;* Hash tag: #ISACAJournal

Join ISACA LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*

Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

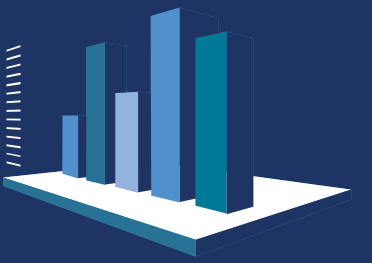
ISACA®
Trust in, and value from, information systems
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone +1.847.253.1545
Fax +1.847.253.1443
www.isaca.org

Worldwide Threat Assessment

analysis, definitions, & guidance

Featured Intelligence

Regional Threat Assessment



local deep dive of security threats

Intelligence provided from Microsoft products and services.

Microsoft Malware Protection Center
Digital Crimes Unit
Security Science
Microsoft Security Response Center

Microsoft Forefront
Windows Live Hotmail
Windows Internet Explorer 9
bing

Security Engineering Center
Secure Development
Defense-in-Depth

Security Intelligence Report

The *Microsoft® Security Intelligence Report (SIR)* is an analysis of the threat landscape with focus on malware, software vulnerabilities, vulnerability exploits, and related trends. Download the latest report at **www.microsoft.com/SIR**.

Managing Risk

Organizations

Protect your organization's network from security threats.

Software

Protect your applications and minimize malware threats.

People

Protect workers against privacy and security threats.

For information about how to protect yourself and your family, visit www.microsoft.com/security

Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. Ross has been writing one of the *Journal*'s most popular columns since 1998. He can be reached at *stross@riskmastersinc.com.*

The Cost of Cyberattacks

At the end of a previous article, I passed along a question asked by a correspondent with regard to the inhibitors to effective security: "Are there other explanations (to poor security) that we are not exploring?"[1] In response, I received a message from Daniel Tan in Kuala Lumpur, Malaysia. Tan made the point that "the key issue lies in the difficult task of quantifying the true cost of an information breach." As difficult as it may be, there have to be sources of information. The most widely quoted figures come from the Ponemon Institute. Its most recent survey on the cost of data breaches that I am aware of was released in 2011 with data gathered in 2010. The report states that:

> *Actual costs varied widely by country, but last year's relative rankings remained unchanged. The US had the most expensive average cost of US $7.2 million. Germany came in second with US $4.7 million. The United Kingdom and France had nearly identical average costs at US $3.1 million apiece. Australia had the cheapest average cost of US $2 million.*[2]

Now, US $7.2 million is a lot of money and US $2 million is still a lot. But in the great scheme of things, any organization that had enough capital tied up in data to lose that much money could probably withstand the financial impact of a loss of that magnitude. However, I submit that considering the cost of an information breach on individual organizations misses the most frightening point: What would be the cost of an attack that targeted an entire economy?

Let me say right here that I have no specific answer. But I do not think that the issue is an idle or hypothetical one. Without delving into the question of who wrote and released the Stuxnet worm, it is clear that it was intended to cause damage to Iran's nuclear capabilities and that it was effective in doing so.[3] Worse yet, an element of Stuxnet accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet.[4]

WHAT WOULD A CYBERATTACK LOOK LIKE?

So, from a purely financial standpoint, what would a widespread cyberattack look like should it be broadly targeted on the economy of an entire nation?

In trying to anticipate the moves of economic cyberwarriors, I would expect them to start by cutting the sinews that hold together commerce. In a digital sense, that would mean taking down the Internet. The decentralized nature of the Internet makes this particularly difficult to achieve on a wide scale, although local outages could be quite devastating. However, the features of the Internet that make it useful are more vulnerable. I am referring specifically to a so-called Domain Name System (DNS)[5] bomb, which evidently is not just a theoretical threat. The US Federal Bureau of Investigation (FBI) recently announced action against a class of malicious software (malware) called DNSChanger, which changes a computer's DNS server settings to direct World Wide Web searches to rogue servers operated by an attacker. The FBI stated that it had, in fact, uncovered a network of rogue DNS servers and has taken steps to disable it.[6]

Were such a DNS bomb or other malware to become widespread, e-commerce would come to a halt. Even assuming that it could be cleared away in a day, it is quite likely that many more organizations would lose much more than the US $7.2 million reported by the Ponemon Institute. Just to give a hint of the potential economic impact, if only 1,000 organizations lost only(!) the Ponemon figure, the losses could be more than US $7 billion in just one day.

It is even more likely, to my mind, that cyberwarriors would attack the central nervous system of an economy, those institutions that enable the flow of money and goods that keep society running. These would include central banks, clearinghouses, centralized freight tracking systems and air traffic control systems. If banks could not transfer funds and transportation systems could not move merchandise, the cost would be incalculable.

To give some idea of the scale of the potential cost, just one institution, the New York Federal

Reserve Bank, in just one of its fund transfer activities, the Commercial Automated Clearinghouse, has a daily volume of 41.2 million items totaling US $70.9 billion.[7] It would be crippling if none of that money could move.

DEALING WITH THE REALITY

Even though cyberweapons have apparently been used, there is still time to protect a nation's critical infrastructure of systems and data. The first step is to accept the reality of the threat: Cyberweapons are real; cyberattacks are real; cyberwarfare is a distinct possibility. With that understood, information security in the commercial sector is a societal priority in all nations. And in fact, organizations have had countermeasures at hand for quite some time, so there is nothing really startling in my suggestions for protection:

- The primary locus of cyberattacks is an operating system. So as security patches are released they should be disseminated and applied as quickly as possible.
- Intrusion detection and prevention systems (IDPS) identify possible incidents, log information about them, attempt to stop them and report on them to security administrators.[8] If there is any one safeguard that is intended to protect against cyberattacks, this is it. Even accepting the cost of implementing IDPS on all platforms, I see these tools as essential for those institutions that are central to a nation's commercial infrastructure.
- Firewalls are hardly new security devices, but they are only as good as the rule sets that determine what will be allowed to pass through a protected perimeter. Organizations, especially if they are probable targets, should review and tighten their rules. Then, they should enforce the rules, not lowering the firewall to the point that it really does not offer protection against a concerted attack.
- Recognize the potential to transport cyberweapons via USB drives. Evidently, the initial version of Stuxnet was spread just that way.[9] These drives should be kept away from critical systems.

There is one factor that may inhibit the use of cyberweapons. In the First World War, the Central Powers deployed mustard gas on the Western Front. It was deadly, but its effectiveness was limited by the fact that the gas could blow back on the attacker's own troops. In the same way, a cyberweapon once unleashed is very difficult to control. Just as Stuxnet replicated itself all around the world, so any entity that might use a cyberweapon might well find it turned on itself.

This is scant comfort, but this article was not intended to provide much comfort. To return to Mr. Tan's email, he also remarked that "cyberattacks are truly a serious topic that needs to be handled with the utmost priority. Like all other risk that has to be managed, every organization should integrate the risk of cyberattacks into its mainstream risk management program so that the issue will be handled with the appropriate gravity and sensible consideration. A more sober and rational approach devoid of hype will actually improve the information security posture of most organizations and should eventually lead to more robust defenses."

ENDNOTES

[1] Dormer, Stan cited in Ross, Steven J.; "This Should Not Be Happening," *ISACA Journal*, USA, vol. 3, 2012,

[2] Ponemon Institute, "2010 Annual Study: Global Cost of a Data Breach," 2011, Symantec Corporation, p. 2

[3] *The Independent*, "Iran's Nuclear Agency Trying to Stop Computer Worm," UK, 25 September 2010, *http://www.independent.co.uk/news/world/middle-east/irans-nuclear-agency-trying-to-stop-computer-worm-2089447.html*

[4] Sanger, David E.; "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, 1 June 2012

[5] US Federal Bureau of Investigation defines DNS as "an Internet service that converts user-friendly domain names into the numerical Internet Protocol (IP) addresses that computers use to talk to each other."

[6] Federal Bureau of Investigation, "DNSChanger Malware," USA, 2011, *http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf*

[7] US Board of Governors of the Federal Reserve System, "Commercial Automated Clearinghouse Transactions Processed by the Federal Reserve—Annual Data," *http://www.federalreserve.gov/paymentsystems/fedach_yearlycomm.htm*

[8] Scarfone, Karen; Peter Mell; *Guide to Intrusion Detection and Prevention Systems (IDPS)*, Special Publication 800-94, National Institute of Standards and Technology, USA, 2007, p. ES-1

[9] *Op cit*, Sanger

Leveraging the Cloud for Added Value

Steven C. Markey is the principal of nControl, a consulting firm based in Philadelphia, Pennsylvania, USA. He is also an adjunct professor and the current president of the Delaware Valley (Greater Philadelphia) chapter of the Cloud Security Alliance (CSA). Markey holds multiple certifications and degrees, and has more than 11 years of experience in the technology sector. He frequently presents on information security, information privacy, cloud computing, project management, e-discovery and information governance.

Cloud computing has been around for several years now; however, this paradigm is just starting to hit critical mass. As organizations look to leverage the cloud, it behooves IS professionals to understand how these solutions may be deployed. This article provides an understanding of how organizations large and small are leveraging the cloud for cost savings, a faster time to market, and/or to realize additional value with their technology.

CASE STUDY 1: PUBLIC CLOUD

nControl is a small consulting firm based out of Philadelphia, Pennsylvania, USA. Being a small business, the firm uses the public cloud extensively, mostly with the Software as a Service (SaaS) delivery model in which an organization uses a prebuilt application for processing. Examples of SaaS applications used include customer relationship management (CRM), web-based surveys, email marketing campaigns, fax services, project management and income tax filing.

nControl has realized the following benefits from using SaaS solutions:

- A degree of cost savings (US $2,000 a year) on desktop-based software
- An ability to remain focused on its core competency
- Improved time to market for the organization, dropping to within hours for establishing new accounts, services and/or business partnerships

The firm uses other cloud delivery models as well, specifically Platform as a Service (PaaS). PaaS requires that an application be built and configured on top of existing hardware and virtual operating system (OS) resources by the cloud consumer. nControl uses this platform for relational database services and web site hosting. PaaS requires more involvement from the cloud consumer; however, this model affords the company more flexibility and agility than the traditional software model for delivery of computational resources.

nControl has been using the cloud for more than four years and is happy with the benefits. That said, there are also challenges with using the cloud, e.g., the costs associated with using PaaS-based databases (or what is called Database as a Service [DBaaS]). Deploying an Oracle 11g instance through a cloud service provider (CSP) can cost US $200-plus per month. Furthermore, if the company takes a backup and/or snapshot of the data on that database, it cannot be ported over easily to another provider. The portability issue extends to the SaaS space when employees try to sync data between Microsoft Outlook and the SaaS-based CRM.

To mitigate the risk associated with going to the cloud, nControl relied heavily on the thought leadership of the Cloud Security Alliance (CSA). CSA, in conjunction with partners such as ISACA®, has created matrices, best practices and software standards to use when evaluating a CSP, which nControl used. Furthermore, the firm relied upon the CSP having relevant certifications and assertions from, for example, the American Institute of Certified Public Accountants (AICPA) (SAS 70), the American National Standards Institute (ANSI)/British Standards Institution (BSI) (ISO 27001), and the US Department of Commerce (Safe Harbor).

CASE STUDY 2: COMMUNITY CLOUD

When thinking of a community cloud, which is a pool of shared resources found within a private cloud deployment model, a good example is the Illini Cloud. This collaboration among the State of Illinois school districts is well executed.

Jim Peterson, the technology director for the Bloomington (Illinois) School District, noted that:

- One's smallest client may be its largest consumer
- A particular service (e.g., videoconferencing) may be a surprise hit

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

- The delivery of a blended hardware/software solution set may be appropriate in order to receive the maximum return on investment (ROI)
- A service that may have been cost-prohibitive before may be cost-effective in a cloud environment
- Collaboration (with stakeholders) is key to enhanced participation

Jason Radford, who is a system administrator for the Bloomington School District, suggested that:

- Community cloud consumers should not underestimate the economies of scale/cost efficiencies that can be reached by deploying a community cloud
- An organization should focus on its core competency/technical skill set, thus enabling the use of these different skill sets throughout the conglomerate
- An organization can leverage a community cloud for necessities, such as disaster recovery (DR)
- Community clouds leverage a grassroots approach for stakeholder buy-in

Peterson and Radford are planning the following as their next steps: leveraging vertical/regional data automation, which is analogous to master data management (MDM), for data snapshots of the community as a whole. They are also using hypervisor-neutral technologies, such as Cloud.com, for enhanced portability/interoperability. Both cloud implementers are working on expanding the community cloud to other interested stakeholders/parties, namely other states and school districts. The Illini Cloud team is also working on packaging cloud software/service solutions as a stack for the consumer. Finally, the team is working with consumers to reduce their reliance on office automation solutions (e.g., MS Office) and/or manual business processes for information processing.

As the team looks to enhance the Illini Cloud, it will continue to leverage security and privacy controls to mitigate risk. By leveraging manual safeguards and native VMware and Cisco-based automated access controls, the team members can rest assured that they are compliant with the various regulations required of public education institutions (e.g., the US Children's Online Privacy Protection Act of 1998 [COPPA]). To further lock down the environment, the team is also looking to establish federated identities.

CASE STUDY 3: HYBRID CLOUD

As the cloud grows in scale, additional organizations will use it to deliver other value-added services. This is especially true for larger organizations because they have the economies of scale to set up various deployment models. A great example is Pfizer's high-performance computing (HPC) environment.

Pfizer, one of the largest pharmaceutical conglomerates in the world, uses a hybrid cloud for additional computational power during worldwide research and development (WRD) efforts, such as US Federal Drug Administration (FDA) trials and human genome research. The company leverages an external private cloud Infrastructure as a Service (IaaS) delivery model offering—Amazon Web Services' (AWS) Elastic Compute Cloud (EC2) in addition to the Virtual Private Cloud (VPC)—for additional resources when needed. Being a large organization that is heavily regulated, the entity's data are stored within its internal data centers. However, through the use of encryption for data in transit, the company leverages EC2 computational resources when necessary, via a secure connection.

The benefit of using an external private cloud, such as AWS EC2, for additional computing power is the elasticity of the cloud. In essence, Pfizer pays for only what it uses when it uses it. However, there is risk involved. So, to mitigate the risk and comply with FDA and national and/or statutory jurisdictional data privacy regulations, the organization uses encryption, virtual firewalls/networks, network and system monitoring, and identity and access management (IAM) mechanisms.

By having to implement the various controls mentioned previously to ensure the security and privacy of such regulated data, the organization observes a different level of cost savings than other industries. However, as FDA trials ebb and flow during the course of business in the pharmaceutical industry year by year, the flexibility and the agility to provision and/or deprovision resources are of paramount importance. Furthermore, as new technologies such as homomorphic encryption, which allows for computations to be executed on native ciphertext (as opposed to a need to decrypt the ciphertext for processing), are introduced, the ability of heavily regulated industries to do faster computational processing in the cloud will increase.

CONCLUSION

IS professionals must be ready to articulate the pros and cons of this new environment, and where and how it can provide added value for the business. The examples provided here present thought leadership on what can go to the cloud and how to get there. Furthermore, these case studies show that an organization of any scale can go to the cloud.

Risk and Responsibility

Vasant Raval, DBA, CISA, is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). Raval is the coauthor of two books on information systems (IS) and security. His areas of teaching and research interests include information security and corporate governance. He can be reached at *vraval@creighton.edu.*

Physical access controls are probably occupying our minds these days due to many recent tragedies around the world. For example, in Oak Creek, Wisconsin, USA, an intruder raided a Sikh temple and took seven lives. And earlier, in Aurora, Colorado, USA, a gunman killed 12 people at a movie theater. In both cases, the attacker managed to get inside the facility with a gun. Most public places in India seem to have learned a hard lesson following the 2008 terrorist attacks in Mumbai where 195 people lost their lives and 295 were wounded. However, the question of what is an acceptable level of risk is more complex; everyone thinks, "It just cannot happen to me." A determination of an acceptable level of risk is normally the responsibility of some individual or group designated, formally or otherwise, to manage the risk.

If we agree that in our profession, a primary concern is risk assessment and risk management,[1] it is imperative that we comprehend the fundamental nature of risk. ISACA's glossary describes risk as "the combination of the probability of an event and its consequence; an event is something that happens at a specific place and/or time."[2] Simply, we understand the concept of risk as a consequence, the combined effect of probability of something occurring—an unwanted event—and its likely impact. A quantification of risk in this manner allows us to proceed to mitigate any unacceptable levels of risk.

At first glance, making the choice seems like a question of a few calculations: Determine the probability of an unwanted event, assess its consequences and combine the two to estimate the impact. A comparison of this result with the cost of instituting and operating appropriate controls guides the decision regarding what to do to protect from an unwanted event. A quantification of risk in this manner technically allows us to proceed to mitigate any unacceptable levels of risk.

But there is more to this than meets the eye. What many of these disparate approaches (e.g., environmental impact assessment; multi-criterion evaluation; probabilistic, comparative, and environmental risk assessment; cost-benefit and cost effectiveness analysis) hold in common is the tendency to treat the concept of risk as an objectively determinate quantity, with the task of appraisal being simply to identify the "best" of a series of options. To this extent, they share the objective of converting the socio-political problems of risk into precisely defined and relatively tractable analytical puzzles.[3] The point is that significant uncertainties in the consequences cannot be adequately handled by standard cost-benefit analyses.[4]

In this thinking, Andrew Stirling[5] is not alone. S. Rayner and R. Cantor reject the essential character of the quantitative definition of risk. An agreement on which consequences are unwanted, followed by an assessment of the factors of probability and magnitude, are not enough to meet the necessary and sufficient conditions of risk choices. Other factors that might be relevant are not mere byproducts, but rather could be inherent parts of the risk itself.[6]

Rayner asserts that the notion of risk can be better grasped if we are to think of risk as an open concept comprised of two components: the scientific and the societal. The scientific component is illustrated by the traditional means of risk analysis. The societal component is fairly new; it concerns trust put in the institutions regulating the technology, acceptability of the principle used to apportion liabilities and acceptability of the procedure by which collective consent is obtained. However, we should note that the elements in this chain of concepts may not be equally important across all situations of risk.[7]

The talk of risk devoid of responsibility is incoherent. In reality, the two are inseparable and not mutually exclusive. In a thought-provoking treatise on risk and responsibility, Anthony Giddens sets the ground for considering the notion of responsibility as closely linked to risk. He asserts that new technologies penetrate more

and more to the core of our lives, and more and more of what we feel and experience comes under the scientific spotlight. The situation leads to increasing insecurity in the world.[8] He believes that all of us are now involved with systems, which even we ourselves do not understand. A risk society is a society in which we increasingly live on a technology frontier that absolutely no one completely understands and that generates diversity of possible futures.[9]

In a risk society, the interaction of social factors with technology factors produces possible futures. Take the issue of privacy in this electronic world. Do you get the feeling that others know more about you than you yourself do? Are you concerned that your every click on the Internet generates an instant lead for some opportunistic entity? Does anyone come to know that you have donated a certain sum of money to your favorite charity? How are you contributing to this problem with your own choices? How do you protect your privacy (or can you)? Is the abuse of privacy hurting some while benefiting others? Is an opt-out solution a good idea for those whose personal information is extracted? Who is winning and who is losing in this battle?

Take another example: the question of copyrights and intellectual property.

Documents we access, electronic copies we forward to our world of connections, photos we share, songs we download, journals we search—in all of this, are we self-regulating to preserve the human decency and obey the rules of society? Since it does not cost us anything more to add email addresses, are we too generous in distributing information? Are we doing a good deed by flooding the receivers' mailboxes? Do we make good decisions because of our sharing? Does it not feel like a chaotic world where if we are able to do something, such as forwarding copies of a copyrighted article, we do it? Does ease of use translate into ease of abuse?

As a final example of sociotechnological factors of risk society, consider the new realities of driverless cars. Is it possible for us to fathom the diversity of possible futures likely to be created by numerous embedded pieces of logic in a vehicle? How will this translate into risk? We live in the world of "manufactured" uncertainty, which occupies a critical space in our lives today. Celine Kermisch[10] suggests that risk can be calculable or unknown; unknown risk can be sourced in uncertainty or ignorance; risk sourced in uncertainty can be external (e.g., tsunami) or manufactured (e.g., privacy, robotics).

Inherent in the notion of ethics is the idea of responsibility—responsibility as a moral agent of our family, church, employer or society at large. As a moral agent, we make decisions that impact others and, probably, these impacts are beyond calculations. In a traditional setting, we may find that we are working with a closed system in which we make the risk choices, we are accountable for them, and we and our organizations exclusively face the consequences. This is no more. In many cases, our role as a moral agent could reach well past the employer's door, into the lives of many people and even the global community. The definition of responsibility may emerge from our role (e.g., privacy officer), cause (disaster recovery planner), capacity (having the credentials to perform the role of a moral agent, e.g., IT auditor) and liability (e.g., duty to comply with regulations, policies and practices, as in the Payment Card Industry Data Security Standard [PCI DSS]). In addition, J. Ladd introduces a moral role, a form of responsibility that refers to "moral deficiency and not just to fault, for example, the absence of care or concern for the welfare of others."[11] Moral agency and moral responsibility are more vivid in situations in which risk choices made by the agent impact other stakeholders.

In the era of manufactured uncertainty, we will see the churning of technology, innovation and risk in various forms. Consequently, there will be political debates about right vs. wrong; the impact on society at large; and stakeholder interests, voice and protection. Not every organization will have to wrestle with questions that span beyond their boundaries, but most will. Risk and responsibility, and the corresponding ethical issues, will rise to the fore. Using Vincent di Norcia's term, we can say that we do not, and cannot, have a "utilitarian calculus,"[12] but we do need guidance that is more specific than the broad ethical theories. And if anything, we will be less secure, not more.

AUTHOR'S NOTE

Opinions expressed in this column are the author's own, and not those of Creighton University.

ENDNOTES

[1] ISACA's entire glossary contains about 950 terms. Of these, there are 33 terms that include the word "risk" as a part of the term. The frequency of usage of the term "risk" in describing the terms in the glossary is 93 times, where some of the terms include reference to risk as many as five times. This is just one indicator of the importance of the notion of risk to the profession.

[2] ISACA, Glossary, *http://www.isaca.org/Pages/Glossary.aspx*

[3] Stirling, Andrew; "Risk at a Turning Point?," *Journal of Risk Research*, 1(2), 1998, p. 98

[4] Aven, Terje; *On the Ethical Justification for the Use of Risk Acceptance Criteria*, Risk Analysis, 27(2), 2007, p. 309

[5] *Op cit*, Stirling

[6] Rayner S.; R. Cantor; "How Fair Is Safe Enough?," *Risk Analysis*, 7(1), 1987, p. 3–9

[7] Rayner S.; "Cultural Theory and Risk Analysis," S. Krimsky and D. Golding Editors, *Social Theories of Risk*, Westport: Praeger, 1992, p. 83–115

[8] Giddens, Anthony; "Risk and Responsibility," *The Modern Law Review*, 62(1), 1999, p. 1–10

[9] Ulrich Beck is to be credited for developing the notion of risk society.

[10] Kermisch, Celine; "Risk and Responsibility: A Complex and Evolving Relationship," *Science Engineering Ethics*, 2012, 18, p. 91–102

[11] Ladd, J.; "Bhopal: An Essay on Moral Responsibility and Civic Virtue," *Journal of Social Philosophy*, 22(1), 1991, p. 73–91

[12] Di Norcia, Vincent; "Ethics, Technology Development, and Innovation," *Business Ethics Quarterly*, 4(3), 1994, p. 237

Graduate into a community that's already winning the war on cyber warfare.

ONLINE MASTER OF SCIENCE IN INFORMATION SECURITY

MANAGEMENT TRACK | TECHNICAL TRACK

Do more than just advance your career with your MSIS from Lewis University. Put it to work right away defending and protecting human justice at the corporate, national and global cyber level.

The U.S. fights off millions of cyber attacks each year. Lewis alumnus and MSIS instructor Matt Kwiatkowski is a leader in that effort. His team at Argonne National Laboratory designed a shared network early warning system, an achievement that won the 2009 U.S. D.O.E. Cyber Security Innovation and Technology Award and has countered untold cyber threats.

Matt Kwiatkowski, '06

LEWIS UNIVERSITY
A Catholic and Lasallian University

You advance. The world gets better.

ONLINE.LEWISU.EDU/ISACA
CALL NOW (866) 967-7046

What Every IT Auditor Should Know About Proper Segregation of Incompatible IT Activities

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA, is an associate professor of information systems (IS) at Columbus State University (Columbus, Georgia, USA). Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs & Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998–1999 Innovative User of Technology Award. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications.

One element of IT audit is to audit the IT function. While probably more common in external audit, it certainly could be a part of internal audit, especially in a risk assessment activity or in designing an IT function. While there are many important aspects of the IT function that need to be addressed in an audit or risk assessment, one is undoubtedly proper segregation of duties (SoD), especially as it relates to risk. Similar to traditional SoD in accounting functions, SoD in IT plays a major role in reducing certain risk, and does so in a similar fashion as well. This article addresses some of the key roles and functions that need to be segregated.

IT DUTIES VS. USER DEPARTMENTS

The most basic segregation is a general one: segregation of the duties of the IT function from user departments. Generally speaking, that means the user department does not perform its own IT duties. While a department will sometimes provide its own IT support (e.g., help desk), it should not do its own security, programming and other critical IT duties. To mix critical IT duties with user departments is to increase risk associated with errors, fraud and sabotage.

User departments should be expected to provide input into systems and application development (i.e., information requirements) and provide a quality assurance function during the testing phase. In fact, a common principle of application development (AppDev) is to ask the users of the new application to test it before it goes into operation and actually sign a user acceptance agreement to indicate it is performing according to the information requirements. However, the majority of the IT function should be segregated from user departments.

DATABASE ADMINISTRATOR VS. REST OF IT FUNCTION

The database administrator (DBA) is a critical position that requires a high level of SoD. The DBA knows everything, or almost everything, about the data, database structure and database management system. Thus, this superuser has what security experts refer to as "keys to the kingdom"—the inherent ability to access anything, change anything and delete anything in the relevant database. This situation leads to an extremely high level of assessed risk in the IT function.

Because of the level of risk, the principle is to segregate DBAs from everything except what they must have to perform their duties (e.g., designing databases, managing the database as a technology, monitoring database usage and performance). The IT auditor should be able to review an organization chart and see this SoD depicted; that is, the DBA would be in a symbol that looks like an island—no other function reporting to the DBA and no responsibilities or interaction with programming, security or computer operations (see **figure 1**).

A similar situation exists for system administrators and operating system administrators.

APPDEV VS. DBA AND IT OPERATIONS

The development and maintenance of applications should be segregated from the operations of those applications and systems and the DBA. That is, those responsible for duties such as data entry, support, managing the IT infrastructure and other computer operations should be segregated from those developing, writing and maintaining the programs. The same is true for the DBA.

It is also true that the person who puts an application into operation should be different from the programmers in IT who are responsible for the coding and testing.

This SoD should be reflected in a thorough organization chart (see **figure 1**).

NEW APPDEV VS. APP MAINTENANCE

For organizations that write code or customize applications, there is risk associated with the programming and it needs to be mitigated. One way to mitigate the composite risk of programming is to segregate the initial AppDev from the maintenance of that application.

In a large programming shop, it is not unusual for the IT director to put a team together to develop and maintain a segment of the population of applications. For instance, one team might be charged with complete responsibility for financial applications. This situation should be efficient, but represents risk associated with proper documentation, errors, fraud and sabotage.

This scenario also generally segregates the system analyst from the programmers as a mitigating control. However, this control is weaker than segregating initial AppDev from maintenance.

The above scenario presents some risk that the applications will not be properly documented since the group is doing everything for all of the applications in that segment. This is especially true if a single person is responsible for a particular application. Improper documentation can lead to serious risk. For example, if key employees leave, the IT function may struggle and waste unnecessary time figuring out the code, the flow of the code and how to make a needed change. Documentation would make replacement of a programmer process more efficient.

The lack of proper SoD provides more opportunity for someone to inject malicious code without being detected—because the person writing the initial code and inserting malicious code is also the person reviewing and updating that code. Therefore, a lack of SoD increases the risk of fraud. If the departmentalization of programmers allows for a group of programmers, and some shifting of responsibilities, reviews and coding is maintained, this risk can be mitigated somewhat.

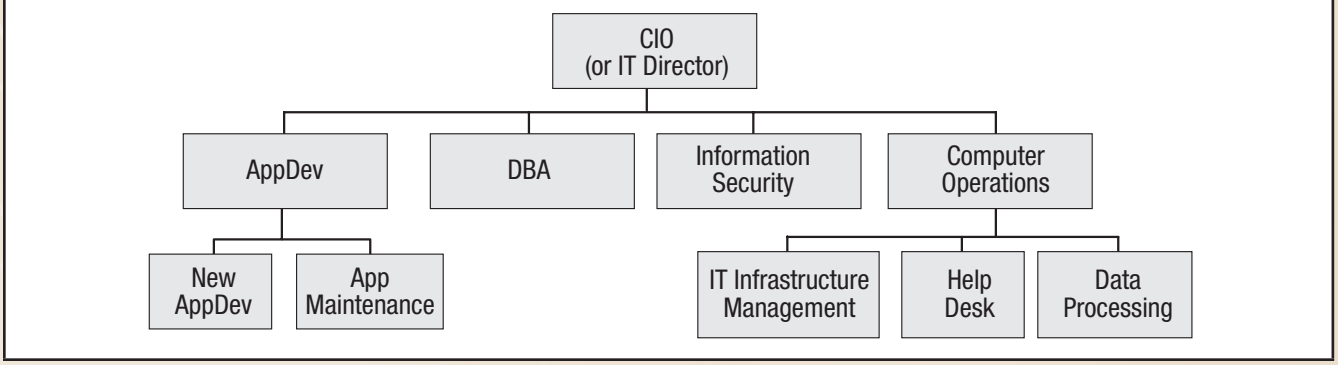
A similar situation exists regarding the risk of coding errors. If the person who wrote the code is also the person who maintains the code, there is some probability that an error will occur and not be caught by the programming function. This risk can be somewhat mitigated with rigorous testing and quality control over those programs.

A proper organization chart should demonstrate the entity's policy regarding the initial development and maintenance of applications, and whether systems analysts are segregated from programmers (see **figure 1**).

INFORMATION SECURITY VS. REST OF IT FUNCTION

Much like the DBA, the person(s) responsible for information security is in a critical position and has "keys to the kingdom" and, thus, should be segregated from the rest of the IT function. This person handles most of the settings,

Figure 1—Sample Organization Chart Demonstrating Effectual Segregation of IT Duties



configuration, management and monitoring (i.e., compliance with security policies and procedures) for security. Login credentials may also be assigned by this person, or they may be handled by human resources or an automated system. Therefore, this person has sufficient knowledge to do significant harm should he/she become so inclined. This risk is especially high for sabotage efforts.

AUDITING THE IT FUNCTION AND SOD

The audit program should include:

- A review of the information security policy and procedure
- A review of the IT policies and procedures document
- A review of the IT function organization chart (and possibly job descriptions)
- An inquiry (or interview) of key IT personnel about duties (CIO is a must)
- A review of a sample of application development documentation and maintenance records to identify SoD (if in scope)
- Observation of personnel for SoD
- Verification of whether maintenance programmers are also original design application programmers
- A review of security access to ensure that original application design programmers do not have access to code for maintenance

CONCLUSION

Figure 1 summarizes some of the basic segregations that should be addressed in an audit, setup or risk assessment of the IT function. The sample organization chart illustrates, for example, the DBA as an island, showing proper segregation from all the other IT duties. The same is true for the information security duty. The AppDev activity is segregated into new apps and maintaining apps. IT auditors need to assess the implementation of effective SoD when applicable to audits, risk assessments and other functions the IT auditor may perform. The reason for SoD is to reduce the risk of fraud, (undiscovered) errors, sabotage, programming inefficiencies and other similar IT risk.

Brian Schaeffer, CISA, CISSP

Brian Schaeffer, CISA, CISSP, is senior vice president and chief information officer (CIO) at Liberty Bell Bank. Schaeffer has 17 years of experience in IT and information security within financial services, health care, publishing and the public sector. Schaeffer has served as CIO for Liberty Bell Bank since 2002, building the bank from its inception to a US $170 million asset-size community bank supporting a four-branch operation in southern New Jersey, USA. He is currently the president of the Philadelphia Chapter of InfraGard, an information-sharing and analysis effort between the US government and an association of businesses, academic institutions, and state and local law enforcement agencies.

Q **You are an active member of both ISACA and Infragard Member Alliance (IMA) *(www.infragardmembers.org)*. As an ISACA member, what particular value do you find in IMA? How do you see the two organizations correlating, and how does IMA provide value to you as an ISACA member?**

A As an ISACA member, I think InfraGard provides me an opportunity to broaden my professional horizons. Besides having access to law enforcement professionals, the knowledge I gain from attending InfraGard meetings has helped me to round out what I have learned through ISACA. Certain events, especially those that are cyberrelated, transcend both groups. Being able to hear two perspectives really helps to round out the important aspects of a given issue. Beyond that, what I find helpful in being a member of both organizations is having access to smart people with diverse knowledge. In my experience, it is generally who you know, not what you know, that gets you out of a tough situation.

Q **After having served as a systems administrator and chief technology officer (CTO) for many years, you expanded into security. Did you find this to be a natural progression and do you find your administrator background of value?**

A Information security is woven into a large part of systems administration. Each operations system or application has its own set of permissions and controls that need to be configured. You also have to be knowledgeable about how networks work and how business functions. All of this knowledge served as a foundation for building and evaluating information security in the enterprise. So, the transition was natural and extremely useful.

Q **As an entrepreneur and founding officer of a bank, what unique challenges have you encountered in your role as chief technology/information/security officer?**

A Well, in the beginning, you are doing everything. One moment you are drawing out the network on a white board, the next you are unboxing and configuring servers and routers. It is both extremely exciting and tremendously stressful. You have to be able to stomach the ups and downs of entrepreneurial life. You also find yourself working on things outside your realm of expertise. There were many regulatory things I had to do as well as help the chief financial officer (CFO) with some of the public accounting reporting. One thing is sure, there is never a dull moment.

Q **How do you believe the certifications you have attained have advanced or enhanced your career? What certifications do you look for when hiring new members of your team?**

A I believe my certifications have enhanced my career. Their biggest value was in dealing with the bank regulators. Regulators are always trying to ensure that the person leading the project is appropriately qualified. My certifications, in conjunction with my work experience, have helped me to build confidence with bank regulators. When looking for candidates I like to see certain certifications, such as Certified Information Systems Auditor® (CISA®) and Certified Information Systems Security Professional (CISSP). With certifications that require continuing education credits, it is easy to verify whether someone is staying current in the profession. This also shows some initiative, a trait all employers like to see in a candidate.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

Q **What has been your biggest workplace or career challenge and how did you face it?**

A I guess one of the biggest challenges was starting Liberty Bell Bank. In the beginning, none of us knew how or what to do. There is no book that gives you step-by-step instructions on how to build a bank. We had to do a tremendous amount of leg work to get things rolling. In addition to our particular specialties (mine being IT), we had to build all of the regulatory and compliance programs from scratch. We spent hundreds of hours pulling everything together. We engaged some professional help and asked lots of questions. It was an extremely challenging and stressful time, but ultimately very rewarding.

Enjoying this article?

- Learn more about and discuss career management.
  www.isaca.org/topic-career-management

Demonstrating Due Diligence in the Management of Information Security

Ed Gelbstein, Ph.D., has worked in IT for more than 40 years and is the former director of the United Nations (UN) International Computing Centre, a service organization providing IT services around the globe to most of the organizations in the UN System. Since leaving the UN, Gelbstein has been an advisor on IT matters to the UN Board of Auditors and the French National Audit Office (Cour des Comptes) and is also a faculty member of Webster University, Geneva, Switzerland. He is a regular speaker at international conferences covering audit, risk, governance and information security and is the author of several publications. Gelbstein lives in France and may be contacted at *ed.gelbstein@gmail.com.*

A 1992 Datamation magazine article, titled "How Good Is Your Data Center? Maybe You Should Find Out Before Your Boss Does,"[1] had a big impact on this author. He has followed the title's advice ever since and encourages others to adopt it.

COBIT® 5 for Information Security provides an excellent, up-to-date and practical tool kit for practitioners, managers and auditors, which has helped the author continue to heed the advice of that 1992 article.

This article discusses how *COBIT 5 for Information Security* can be applied to maximum effect and to complement other tools to assess the extent to which due diligence has been exercised to provide appropriate information security.

While the components of information security, i.e., requirements definition, strategy and policies, technology, processes, and people (including system and data custodians), are common to all organizations, like snowflakes, no two implementations are identical.

The parameters that make a difference include organizational requirements, culture, the level of resources available and employee engagement. Then, there are other differences such as the individual capability maturity levels associated with processes. The consequence of this is that what may be "good enough" for one organization, may be totally inadequate for another.

COBIT® 5 includes a discussion of pain points and trigger events, any of which may initiate a need to determine whether appropriate due diligence has been exercised. This article suggests five complementary activities to get this done:

1. Determine metrics (i.e., what gets measured, by whom, how it is analyzed and reported).
2. Perform self-assessments of gap analysis (e.g., against COBIT 5 practices), vulnerabilities, controls and risk.
3. Determine the need for certification, whether process (e.g., 27001), professional (e.g., CISM®) or end user (e.g., tests leading to an attestation of the successful completion of a training program).
4. Complete audits of the same domains as self-assessments. Audits are independently conducted, evidence-based and supported by standards and guidelines.[2]
5. Complete penetration tests (i.e., ethical hacking).

Each of these is briefly examined and discussed later in this article.

> "While the components of information security…are common to all organizations, like snowflakes, no two implementations are identical."

PAIN POINTS AND TRIGGER EVENTS

COBIT 5 includes an excellent description of both pain points and trigger events in section 2.3 (and they appear again in section 2.5 and in some of the appendices). Being aware of how information security performance is perceived by senior management and other parts of the business is of fundamental importance to assure alignment.

The scope of information security has grown enormously in the last 50 years and its focus continues to shift as technology and computer literacy become increasingly powerful and sophisticated. In the early days, there were few users of computer systems, which consisted of mainframes linked to dumb terminals. Some work was done in real time, the bulk in batch processing. *Confidentiality* was the prime concern, and access controls were a key activity.

As mainframe architectures evolved, real-time computing became widespread and *availability* became a further important requirement. Whatever networking existed was proprietary and hacking was, by and large, a hobby that began to grow when personal computers first became available in the 1970s. Acoustic couplers and a low-speed dial-up link were enough. And, of course, hacking was clearly targeted to specific computers.

In 1983, the US Federal Bureau of Investigation (FBI) arrested six teenagers known as the "414s" (it was the area code in which they resided) for hacking into several high-profile computer systems. The movie *War Games*[3] was released in the same year. In this movie, a young man finds a back door into a military computer and comes close to launching World War III.

Jumping to the 2010s, security practitioners face multiple challenges—from bring your own device (BYOD), which creates architectural complexities and management issues, to weapons-grade malicious software (such as Stuxnet and Duqu)—as well as issues of investigations and digital forensics, regulatory and legal compliance, building awareness among users, engaging systems and data owners, and so much more.

One of the early lessons practitioners learn is that their activities are invisible until something goes wrong, at which time the reaction is swift and often hard. Engaging in dialog with executives, senior managers and other parts of the business—including procurement and legal counsel—to understand their perceptions and requirements is highly recommended. It must be recognized that these groups have their own accountabilities and pressures to deal with, that their time is valuable (and not to be wasted), and that information security may not appear on their lists of priorities. Therefore, good preparation and soft skills have become prerequisites for such dialog to be meaningful.

METRICS

In a lecture given in 1893 to the UK Institute of Civil Engineers, William Thompson (Lord Kelvin) said, "If you can measure that of which you speak and can express it by a number, you know something of your subject; but if you cannot measure it, your knowledge is meager and unsatisfactory." This has since been changed into, "You cannot manage what you do not measure." The original is, as usual, more accurate.

However, it is not easy to find information security metrics that are meaningful in business terms. (*COBIT 5 for Information Security*, the NIST SP 800 series and ISO 27000 publications suggest lists of possible metrics.) Out of the hundreds of possible metrics, the most valuable ones are those that meet the following four criteria:

1. They are accessible and credible, i.e., they are not laborious to obtain and the source can be trusted.
2. They involve a transparent calculation, i.e., one that can be explained, understood and shared.
3. They have a common interpretation, i.e., the recipient understands what the metric means.
4. They are actionable, i.e., changes in the metric point to the source of a problem and to actions needed to remedy it.

In addition, metrics and how they are reported are likely to be most valuable when they have clear links to business impact analysis (BIA), enterprise risk management (ERM), IT and security strategies.

There is no universal set of metrics that will fit the needs of all organizations. Information security events are neither random nor independent; they are targeted. Therefore, statistical analyses using a Gaussian (normal) distribution are of no use,[4] as are most lagging indicators, such as key performance indicators (KPIs). However, key risk indicators (KRIs) are leading indicators and point to actions to be taken.

SELF-ASSESSMENTS

The security practitioner is well placed to perform a series of self-assessments as suggested by Robert Burns when he wrote (loosely translated into current English): "Oh, what if some Power gave us the gift to see ourselves as others see us! It would from many a blunder free us…."[5]

Five areas where self-assessment is likely to have a good return on the time and effort invested include:

- **Gap analysis of security practices and related metrics**—Using, for example, *COBIT 5 for Information Security* (however, it should be noted that this publication contains 192 such practices)
- **Vulnerability analysis**—Integrating, for example, items known to the practitioners and their teams, reports from vendors and other advisory services, high-impact open items in the risk register, and relevant audit recommendations not yet implemented.
- **Key controls**—Not waiting for the auditors to identify areas for improvement. These should represent what is most critical to the organization and are likely to include, among others, privileged access, change and configuration management, third-party service providers, core business applications, and identity and access management (a full list would be quite long).
- **Risk**—Ensuring that a risk register is maintained and used to identify high-impact items (regardless of their likelihood) and their appropriate mitigating actions, and also monitoring to ensure that these items are properly reflected in a corporate risk register and supported by (ideally tested) contingency plans

- **Intelligence**—Building a good awareness of security incidents around the world to avoid being surprised, as this is never a good thing

As useful and valuable as self-assessments can be, they have four major limitations:

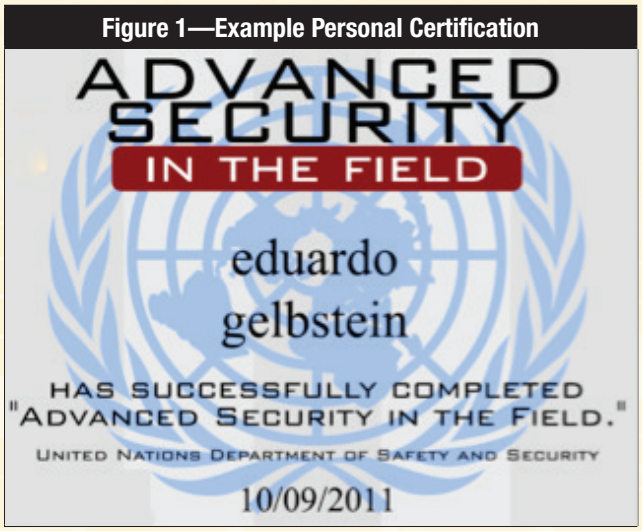
1. They require considerable time and effort.
2. They require good knowledge of how to conduct and document them.
3. They must involve other players in the organization, notably system and data custodians.
4. They must be carried out objectively. Optimism would diminish the value of the exercise.

CERTIFICATIONS

Certifications are documents issued by a body with the authority to grant recognition to an organization, a set of processes or services, and/or an individual, that assert that certain established criteria have been met. There are three types of certification:

- **Process certifications**—There are a number of certifications with good practices that are well known to security practitioners, such as compliance with ISO 27001, *Information Security Management System (ISMS)*.[6] Such certifications are voluntary; each organization must decide the merits of pursuing them, for example, to demonstrate to its stakeholders that information security is formally addressed at the strategic level. There are, of course, disadvantages to pursuing these certifications, such as the cost of preparing for a certification inspection and the risk of failing to acquire it (or to renew it at a future mandated revalidation).
- **Professional certifications**—Individual practitioners of information security can obtain professional certification from bodies such as ISACA. To obtain these certifications, individuals often must meet eligibility requirements (education and/or experience), pass an examination and pay a fee. Additional requirements that must be met may include retesting and participating in a minimum number of continuing professional education (CPE) activities. Professional certifications are voluntary, and the individual usually invests personal time for preparation and incurs the cost of training, related material and the examination. It is conceivable that growing numbers of organizations will require such professional certification as a condition of employment. As such certifications provide independent evidence of an individual's qualifications, experience and knowledge, those who possess them can be seen as being more attractive to potential employers than those who do not, thus introducing the risk of increased turnover among information security professionals.
- **Personal certifications**—A third category of certification is the issuance of the equivalent to a drivers license for users who access critical systems or data (or even for all users). This is practiced by many organizations. The United Nations, for example, made it mandatory in 2003 for all staff traveling on mission to hold a basic certificate of "Security in the Field" and, for those traveling to higher-risk destinations, an advanced certificate (see **figure 1** for the author's own such certificate). These certificates are valid at the UN for three years, after which time the online course and its associated test must be retaken.

Figure 1—Example Personal Certification



Thus, all three types of certification become a matter of corporate policy and imply monitoring for compliance.

Certification for individuals, who need to access systems and data, raises design issues such as how long the test should take and how much knowledge is required to pass. If it is too easy, the exercise becomes pointless and if too difficult, one must consider what to do about those who are unable to pass it. Such certifications also require data to be held on expiration dates and the tracking of requalification. Certifications must not be seen as the equivalent of a guarantee.

AUDITS

Audits are performed to ascertain one or more of the following: the validity of information (financial and other such as performance reports), an independent assessment of

internal controls, and an assessment of the completeness and capability maturity level of operational processes.

The outcome of an audit is an opinion of the items being audited (e.g., an organization, a set of processes, systems reflecting work done on a sampling or test basis). Therefore, an audit report can only provide reasonable assurance that its findings, observations and recommendations are free from material error.

There are many guidelines and good practices for IT and security audits, such as those published by ISACA.[7]

The challenges here fall in two categories:

1. Defining the scope of an IT security audit so that it is appropriate to the organization, does not require an inordinate amount of time to complete, does not unduly disrupt the work of the IT security organization and its practitioners, and provides information that was previously unknown. An audit report that merely reports facts and issues already known to the organization is a waste of time and resources.
2. Engaging auditors with appropriate qualifications and experience to ensure that the parties being audited can have confidence in the audit

PENETRATION TESTS

Also known as ethical hacking, penetration tests differ from an external hacking attack only in that they have the consent of senior management, which, in turn, requires a good measure of trust and suitable contractual nondisclosure agreements.

It is prudent to remember that "anything built by man can be broken by man"[8] and to fully expect the ethical hacking to confirm this.

Penetration tests can take many forms:

- They may give the testers a measure of prior knowledge of the target (none equals black box, detailed equals white box, some equals gray box).
- They may be announced to security team members prior to the engagement or be conducted without their knowledge.
- They may be conducted either by testers with links to vendors or by independent testers.
- They may be performed over a limited time, mainly to contain costs.

CONCLUSIONS

"If there is no problem, you are not needed. If there is a problem, you are incompetent."[9] This statement is made from time to time in security conferences, and it is clear that no professional would wish to be labeled "incompetent" or blamed.

COBIT 5 for Information Security[10] can be used to help practitioners identify the trigger events and pain points that are relevant to their organizations at the time of review. This can also be supported by *Principles for Information Security Practitioners*[11] issued jointly in December 2010 by ISACA, (ISC)^2 and the Information Security Forum.

The ability to demonstrate that due diligence has been exercised needs to be considered and an appropriate plan of action developed accordingly.

The five approaches described in this article are compatible with *COBIT 5 for Information Security*, and regarded as worthwhile initiatives subject to Nassim Taleb's statement in *The Black Swan* that "No evidence of vulnerabilities is quite different from evidence of no vulnerabilities."[12]

ENDNOTES

1 "How Good Is Your Data Center? Maybe You Should Find Out Before Your Boss Does," *Datamation*, vol. 38, no.18, 1 September 1992

2 ISACA, *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*, October 2010, *www.isaca.org/standards*

3 *War Games*, *www.imdb.com/title/tt0086567/*

4 Taleb, Nassim; *The Black Swan*, 2007 (also by the same author, *Fooled by Randomness*)

5 Burns, Robert; *To a Louse*

6 International Organization for Standardization (ISO), *Information Security Management System*, ISO 27001, 2005

7 ISACA, *Guidance for Best Practice in Information Security and IT Audit*, 2009

8 Source unknown

9 Source unknown

10 ISACA, *COBIT 5 for Information Security*, 2012, *www.isaca.org/cobit*

11 ISACA, *Principles for Information Security Practitioners*, December 2010, *www.isaca.org/Knowledge-Center/Standards/Pages/Security-Principles.aspx*

12 *Op cit*, Taleb

Lack of Privacy Awareness in Social Networks

S. Srinivasan is professor of information systems (IS) and chairman of technology studies at the Texas A&M International University (TAMIU), Laredo, Texas, USA. Prior to joining TAMIU, Srinivasan was at the University of Louisville (Kentucky, USA). He started the information assurance (IA) program at the University of Louisville in 2003. This program was designated a national center of academic excellence in internal audit (IA) education by the National Security Agency and the Department of Homeland Security (NSA/DHS). Srinivasan's research interests are in information security. He can be contacted at *srini@tamiu.edu*.

Social networks have opened up a new avenue of communication for millions of people around the world. The major attraction of this technology is the ease with which people can share their personal information with their friends. In analyzing this new technology, one needs to first understand the clear meaning of social networks. The following definition will be used in the analysis of this concept: Social networks are facilitated by web technology that allows several users to publish content freely on any subject for use by friends and others. Such sites allow users to create personal profiles visible to the people they allow.

This phenomenon started with the tool known as Six Degrees, launched in 1997 by Andrew Weinrich in New York, New York, USA. This was the first social network. In 2000, Richard Ericsson launched a social network in Sweden called the Lunar Storm for use by teenagers. This social network became extremely popular.[1]

The next significant event in social network evolution occurred when Friendster was launched in San Francisco, California, USA, by Jonathan Abrams in February 2003. Friendster grew too rapidly and was unable to maintain a high quality of service.[2] Future social networks MySpace and Facebook learned from the failures of Friendster. In May 2003, Reid Hoffman launched LinkedIn from San Francisco, California, USA, with a focus on connecting all business people. Today, with over 160 million users, LinkedIn is one of the four major social media networks.[3] Popularity of social networks seemed evident and so Orkut Buyukkokten of Stanford University (California, USA), created Club Nexus for use by Stanford University students in 2001. Google helped him launch this network as Orkut in January 2004, a watershed year in the rapid growth of social networks. Orkut was the dominant social network in Brazil until 2011[4] and widely popular in India as well. The next major entrant to the social network scene was MySpace by Tom Anderson and Chris DeWolfe, from Los Angeles, California, USA, in August 2003. MySpace grew rapidly and became the network of choice among high school and college students.[5] Today, MySpace has switched its focus to music-related activities.[6]

In concluding the history of social networks evolution, it is important to mention the two major players in the field: Facebook and Twitter. Facebook was launched by Mark Zuckerberg and his friends from Harvard University (Cambridge, Massachusetts, USA) in 2004. Facebook adopted a staggered-launch approach to meet the demand. Today, Facebook has grown to be the number-one social network around the world with a subscriber base of 845 million.[7] Jack Dorsey and his friends launched Twitter in 2006 from San Francisco, California, USA, as a way to share one's thoughts with 140 characters at most in the message. Today, Twitter has more than 600 million customers worldwide.[8] Many people follow the tweets of others, not necessarily their friends.

In all the tools identified so far, the major goal has been ease of use and sharing of information. With this came the concern of excessive information sharing, often without the knowledge of the user. Compounding this problem have been the periodic changes in privacy policies that resulted in users losing control of their personal information posted online. Facebook, with several hundred million users worldwide, has also contributed to the concerns about privacy, according to a 2011 report from the Federal Trade Commission.[9]

USER PERCEPTIONS

Social media users believe that convenience comes first. Users do not have any reservations about providing personal information as part of their profile.[10] When the user gives personally identifiable information (PII), such as address and date of birth, the intent is for the benefit of friends. Users believe that their friends already know the PII and they are sharing something that only provides clarity to their circle of friends.

Issues arise when access to the information is extended beyond the circle of friends by

transferring of privileges.[11] This is where the initial privacy compromises take place.

In many cases, the customer is unaware of the extent to which the PII has spread. One reason for this confusion is the way social networks enable the settings for the account. If sharing privileges were made available by default as opt in, as opposed to opt out, it would greatly facilitate user control for PII. Another reason is the fact that social networks are still emerging.[12] Until they reach a mature state, privacy concerns will continue to pose problems. For example, consumers still trust their friends more than any other source when it comes to researching a product, service or a topic.

When looking at the rapid growth of social networks, it is worth noting that the three most popular social networks were launched less than a decade ago. Their millions of users point to the public's desire to keep connected to their friends and coworkers. Therefore, some of the privacy issues can be attributed to the growing pains of the rapidly changing technological landscape.

Another viewpoint to consider in this regard is the perceptions of the majority of users who are on social networks. Even though social networks have pervaded every demographic, they are still widely used by people in the 17–24 age group. People in this age group tend to trust systems more and do not have concerns about their personal information getting misused.[13] Also, they might unwittingly provide their information and do not see reasons to be cautious in social networks. According to a 2007 research survey, nearly 90 percent of teenagers post a video and expect feedback from their friends.[14] This attitude lends itself to keeping some privacy settings open to a larger group of people. These kinds of benefits of social networks, especially Facebook, are further reinforced by the study of M. D. Roblyer. The main benefits to note from Roblyer's study are summarized in **figure 1**.[15]

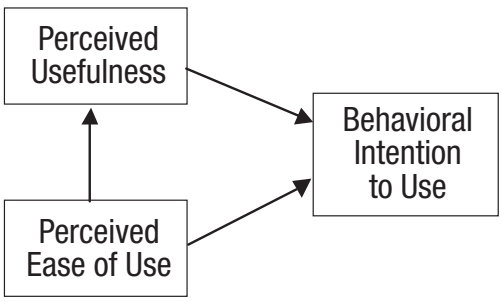
Figure 1—Summary of Student Responses on Reasons for Using Facebook

Criteria for use	Respondents
Keep in touch with friends	92.5 percent
Let others know what is happening in my life	48 percent
Connect with people I have lost touch with	72 percent

An innate problem that many Facebook users seem to overlook is the possibility that personal information could be released to unintended people. Many users perceive that when they add a friend, their friend will be judicious in passing on the privilege to view their information to others. However, many users are not that discriminating when it comes to setting the privileges. The Technology Acceptance Model (TAM)[16, 17] was used in analyzing this aspect of user perceptions (see **figure 2**). Two of the three main components of the TAM are "perceived ease of use" and "perceived usefulness." Facebook users clearly experience the ease of use aspect in connecting with their friends. They value such interactions with their friends and find Facebook useful in facilitating those interactions, thus validating the second aspect of TAM concerning perceived usefulness. The overwhelming numbers of Facebook users demonstrate that their use of Facebook clearly validates the third and final piece of TAM, namely the "behavioral intention to use."

Moreover, the analysis shows that users perceive ease of use as an overwhelming factor in overlooking the trust aspects when it comes to befriending new persons on a social network. Furthermore, Catherine Dwyer also studied the trust aspects in social networks and found that users overwhelmingly feel comfortable sharing personal information on the network for the benefit of their friends.[18] This observation is validated by a 2011 Pew Internet and American Life Project research survey, which showed that 91 percent of all social networking teens use the sites to stay in touch with friends, while 82 percent use the sites to stay in touch with friends they do not see in person often.[19]

Figure 2—Technology Acceptance Model



Source: Davis, Fred

PRIVACY AND SECURITY

The concept of privacy in general dictates that no one should be able to observe things about a person without that person's knowledge. In social networks, privacy is greatly ignored unwittingly. Many people perceive that rejecting a request to be your friend based on one of your other friends' recommendations might be considered rude.[20] It is important to recognize that friendships are dynamic. A typical scenario in Facebook could be that a friend posts "Five Things About Me" and encourages the recipient to do the same. In response to this suggestion from a friend, the posting by the recipient states, "I attended Valley High," and, "My cat's name is Myra." It is likely that the user has chosen these two answers as his/her challenge response for an online bank account. This simple scenario points to the vulnerability of exposing personal information unwittingly.[21]

One type of serious privacy violation that occurs in social networks involves photos. A conscientious user might have placed appropriate controls on his/her settings concerning the ability to view photos posted on his/her wall. When a friend posts a photo on his/her wall without putting it in context and invites all mutual friends to view the photos, it could jeopardize the carefully crafted privacy settings of the first user. This kind of privacy violation is all too common in social networks. A similar experience was also discussed by Dwyer about a teacher feeling awkward after her students befriended her and posted some pictures.[22] Another source of privacy violations on Facebook involves third-party applications. Users constantly subscribe to new and popular applications. Such applications find acceptance because they are referred by friends. Consider the following scenario in which the user has violated his/her own carefully crafted privacy settings: User downloads a phone app which finds the answer to the question, "Which 1970s movie reflects you?" Before this app is launched, the user is informed that in order to find the answer to the question the app needs access to the user's profile and that of his/her friends. A whole host of privacy settings have been violated by the simple use of this one app. In the world of social networks, such apps are prevalent. Aaron Beach, Mike Gartrell and Richard Han have studied the role of applications in violating user privacy,[23] thereby reinforcing the statement that applications have a way of bypassing some of the security controls.

The ease of use in social networks significantly contributes to many privacy violations. For example, two users participating in the update-and-reply feature of a Twitter conversation are unwittingly sharing their conversations with their friends unless they took specific steps to block the feeds.[24] Twitter feeds are brief but contribute to some major privacy violations. A large corporation that allows the use of Twitter by employees could face a serious threat. An employee might tweet to one of his close confidants that a new system developed by the organization has a serious bug. Unfortunately, Twitter feeds are followed by many, and so a confidential organizational problem is now exposed. This example shows that privacy violations need not be at the individual level.

According to a 2011 research survey, social networks provide "a concentrated posse of easily contactable friends."[25] Given the large number of friends to communicate with on social networks, many use the networks in a variety of ways. The research survey results appear in **figure 3**.

These statistics show how information gets posted and communicated among friends through social networks without much filtering. Potential users must be aware that what is posted on social networks will find its way to a very large audience quickly, so any information that could expose one's privacy should be guarded.

Figure 3—Uses of Social Networks for Communication With Friends

Type of Use	Respondents
Post messages to a friend's page or wall.	84 percent
Send private messages to a friend through the social network system.	82 percent
Post comments to a friend's blog.	76 percent
Send a group message to all friends.	61 percent
Give e-props or kudos to friends.	33 percent

Source: Pew Internet and American Life Project research survey

The benefits of social networks extend not only to individuals, but also businesses. In a survey of 72 business managers conducted at Texas A&M International University regarding the perception of the use of social networks in business, the respondents were skeptical of new technologies. However, they recognized that the introduction of both the Internet and email had significant benefits to business. With this experience, the analysis of the data shows that managers perceived that the use of social networks in business builds:

- Employee morale
- Satisfaction
- Commitment
- Enhanced performance

The survey showed that some managers perceived that allowing the use of social networks at work is essential because their competition allows it. This line of reasoning should be tempered by the fact that every business should assess its business goals in light of what technology has to offer.

Social networks realize the importance of security and provide some tools to protect the information. However, the overwhelming goal is ease of use and rapid dissemination of information. It is clear from various statistics on the use of social networks that younger people use it extensively. The prior comment concerning the goals of social networks comes as a result of this observation as well as the fact that older adults also use social networks for ease of use and rapid communication capabilities.[26] These aspects pose an inherent security problem in social networks.

A typical Facebook user's preferred device of choice is the cell phone. Even though setting a user ID and password are options from a cell phone, virtually all users ignore this aspect for the sake of convenience. Given this fact, if the cell phone is misplaced or lost, then anyone obtaining the device will have access to the Facebook account of the user. Someone with a criminal intent could post a damaging or misleading message.

A new security threat is emerging in social networks because of location tracking. Facebook has a feature called "check-in," which lets friends know one's GPS location. Since one's circle of friends sometimes gets very large simply by transference of friends, one must monitor one's privacy settings closely.

The login notification on Facebook is similar to Skype. Friends are notified when a user logs into their Facebook account. Facebook and other social networks let members link up to their account in other popular sites such as YouTube. Even though this feature allows for the setting up of user ID and password, many users simply ignore this security feature. Thus, a user logged into one social network potentially exposes all their other accounts as well.

On Facebook, the update feature is a major security vulnerability. An innocuous message such as, "I am looking forward to my vacation in Europe next month," gets forwarded to a large circle of friends. Since some of the friends are basically acquaintances, the user has essentially broadcast a message that they are not going to be home, thereby creating an opportunity for someone to rob them.

These simple instances illustrate the security threats widely prevalent in social networks.

BEST PRACTICES

This article highlights some of the widely practiced usage patterns in social networks that may lead to privacy and security vulnerabilities of one's confidential information and personal safety. In this section, some best practices are provided for users to protect their privacy.

First, users should not feel obligated to accept invitations from friends because they show a referral from another friend. This preventive action alone could significantly enhance privacy and security because the people whom a user accepts as friends should indeed be people known to the user.

Second, in social networks URL shortening or obfuscation[27] is widespread. Since trust among friends is widespread, people with criminal intent befriend people to post obfuscated web links to questionable sites. To protect against such an intrusion into their circle of friends, users should choose to copy and paste the web link rather than navigate from it directly. If a web link appears questionable, there are web sites such as *www.longurl.org* or *www.longurlplease.com* that can verify the authenticity of web links.

Finally, attachments are another source of potential threat in social networks, and users should remain vigilant. The vulnerable aspect of attachments is that even if they appear to emanate from known friends, they could be potential attacks originated by hijacking users' address books.

CONCLUSION

Social networks have revolutionized communication among an extended circle of friends. This technology has many benefits to offer society. Millions of people around the world are benefiting from the use of social networks. An analysis of this new technology shows that it has many positive aspects, but at the same time it has significant problems with respect to privacy of information and security. Social networks themselves are evolving and, as such, some of the settings that could offer the necessary security and privacy are still emerging. The ease of use aspect of the major social networks, such as Facebook, Twitter and LinkedIn, undermines their privacy and security features. The discussion established in this article also sheds light on some of the steps users can take to protect both privacy and security.

ENDNOTES

[1] Kirkpatrick, David; *The Facebook Effect*, Simon and Schuster, USA, 2010

[2] Boyd, Danah M.; Nicole B. Ellison; "Social Network Sites: Definition, History, and Scholarship," *Journal of Computer-Mediated Communication*, vol. 13, p. 210–230, 2008

[3] LinkedIn Press Center, *http://press.linkedin.com/about*

[4] ComScore,"Facebook Blasts Into Top Position in Brazilian Social Networking Market," January, 2012, *www.comscore.com/Press_Events/Press_Releases/2012/1/Facebook_Blasts_into_Top_Position_in_Brazilian_Social_Networking_Market*

[5] *Op cit*, Kirkpatrick

[6] Houghton, Bruce; "MySpace Reboots Today With a Focus on Music, Facebook Integration," Hypebot, December 2011, *http://hypebot.com/hypebot/2011/12/myspace-reboots-today-with-focus-on-music-facebook-integration.html*

[7] Crunch Base, *www.crunchbase.com/company/facebook*

[8] Twopcharts, "The Last 100 Million Twitter Accounts," *http://twopcharts.com/twitter500million.php*

[9] The Federal Trade Commission, "Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises," 2011, *www.ftc.gov/opa/2011/11/privacysettlement.shtm*

[10] Jeff Fox, May 2012, *http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm*

[11] Dwyer, Catherine; Starr Roxanne Hiltz; Katia Passerini; *Trust and Privacy Concern With Social Networking Sites: A Comparison of Facebook and MySpace*, Proceedings of 13th Americas Conference on Information Systems (AMCIS), USA, August, 2007

[12] Nielsen, "New Online Activities, Services and Devices Bringing Australians More Choices and New Ways of Doing Old Things...," Nielsen Australian Online Consumer Report 2011-12, March 2012

[13] Beck, Timo; *User Perception of Targeted Ads in Online Social Networks*, University of St. Andrews, School of Management, Scotland, UK, 2010

[14] Lenhart, Amanda; Mary Madden; Alexandra Rankin Macgill; Aaron Smith; "Teens and Social Media," Pew Internet and American Life Project, USA, December 2007, *www.pewinternet.org/Reports/2007/Teens-and-Social-Media.aspx?r=1*

[15] Roblyer, M. D.; Michelle McDaniel; Marsena Webb; James Herman; James Vince Witty; "Findings on Facebook in Higher Education: A Comparison of College Faculty and Student Uses and Perceptions of Social Networking Sites," *Internet and Higher Education*, vol. 13, Elsevier, USA, 2010, p. 134–140

[16] Davis, Fred; *A Technology Acceptance Model for Empirically Testing New End-user Information Systems: Theory and Results*, Thesis (Ph.D.), Massachusetts Institute of Technology (MIT), Sloan School of Management, 1986

[17] Lee Y.; K. A. Kozar; K. R. T. Larsen; "The Technology Acceptance Model: Past, Present, and Future," *Communications of the Association for Information Systems*," vol. 12, iss. 1, 2003, p. 752–780

[18] *Op cit*, Dwyer

[19] Pew Internet and American Life Project research survey, "Why Americans Use Social Media," November 2011, *http://pewresearch.org/pubs/2131/social-media-facebook-twitter-myspace-linkedin*

[20] Tokunga, Robert S.; "Friend Me or You'll Strain Us: Understanding Negative Events that Occur Over Social Networking Sites," *Cyberpsychology, Behavior and Social Networking*, vol. 14, issue 7–8, p. 425–432

[21] Dinerman, Brad; "Social Networking and Security Risks," white paper, GFI software, 2011, *www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf*

[22] *Op cit*, Dwyer

[23] Beach, Aaron; Mike Gartrell; Richard Han; "Solutions to Security and Privacy Issues in Mobile Social Networking," International Conference on Computational Science and Engineering, vol. 4, p. 1036–1042

[24] Chen, Guanling; F. Rahman; "Analyzing Privacy Designs of Mobile Social Networking Applications," Procceedings of International Symposium on Trust, Security and Privacy for Pervasive Applications, Shanghai, China, 2008

[25] *Op cit*, Pew Internet

[26] Media Badger, 2011, *www.mediabadger.com/2011/10/senior-citizens-and-social-media/*

[27] Obfuscation means that the full web site information is shortened, so that it may not be apparent what the web site is by just looking at the text displayed.

Preventive Technical Controls for Application Security

Rohit Sethi, CISSP, CSSLP, is vice president of product development at SD Elements. Sethi is a specialist in building security controls into the software development life cycle (SDLC), and a SANS course developer and instructor on Secure J2EE development.

Ehsan Foroughi, CISM, CISSP, is director of research at SD Elements. Foroughi is an application security expert with eight-plus years of management and technical experience in security research and an extensive development and reverse engineering background. He is the founder and chief technology officer (CTO) of TELTUB.

COBIT®,[1] the Payment Card Industry Data Security Standard (PCI DSS) and several other software security maturity models[2, 3, 4] address the security requirements necessary to produce secure applications. In the authors' experience, software development groups rarely address technical application security requirements at the breadth or level of detail found in The Open Web Application Security Project (OWASP)[5] or similar developer guides to security.

Organizational application security efforts tend to focus on automated detective and/or corrective solutions, such as static analysis, binary analysis, run-time testing and web application firewalls.[6] IT control audits that primarily assess detective application security controls tend to bias enterprises' application security efforts toward building software features and subsequently fixing security defects rather than preventing the defects from occurring in the first place.

> "Secure application life cycle management (SALM) systems can help auditors assess organizations for preventive technical security requirements of either procured or in-house developed applications."

An emerging class of in-house and commercial off-the-shelf (COTS) software called secure application life cycle management (SALM) systems can help auditors assess organizations for preventive technical security requirements of either procured or in-house developed applications.

CHALLENGES WITH DETECTIVE CONTROLS

Detective controls face challenges. Static and/or dynamic analysis systems cannot report on the *absence* of a technical security control mechanism, such as session management, altogether.[7] In practice, this sort of logic flaw is caught by manual source-code review or manual penetration testing. These techniques suffer from scalability and high cost. Few organizations can afford to perform the level of manual testing required for their entire application portfolio. The problem is further exacerbated by domain-specific flaws or bugs such as insufficient authorization, which require not only human expertise, but also an understanding of the software domain to uncover.[8] In one famous example, security researchers without sufficient permission were able to access privacy-protected photographs on Facebook.[9] While the security community and security tool developers already have a strong understanding of insufficient authorization, there is simply no practical method of detecting such a vulnerability using a completely automated mechanism.

DETECTION IS INEFFICIENT

Detective techniques for flaws are inefficient when compared to preventive techniques as a result of extremely high remediation costs in the software development life cycle (SDLC). Researchers have long studied the sheer cost-effectiveness of planning for and preventing defects upfront rather than finding and fixing them later.[10]

DEVELOPER EDUCATION

Another preventive technique—developer education—seeks to empower developers with the knowledge to write secure code. Research shows a noticeable positive correlation between education and the quality of application security.[11] Continuous training is crucial. With a single training class as a point-in-time activity, the value of the education diminishes over time unless the developers are continuously in touch with material and are updated on new and emerging techniques. Moreover, given the pressures of building software under strict deadlines, software developers could forget about specific security defects due to cognitive burden.[12] Thus, developer education is important but not sufficient for preventing application security defects.

UNDERSTANDING SALM

SALM systems seek to close the gaps in the current detection-focused software security space. SALM systems are the security extension of SALM products—tools designed to help manage the process of building software.[13] SALM systems define specific application security defects and their corresponding preventive controls, as relevant to a given application, by rules relating to the application's underlying properties, such as class of application (e.g., web vs. client/server), technology stack (e.g., Java EE, C/C++, Android SDK) and regulatory drivers (e.g., PCI DSS). For example, a SALM system might define a rule that a Structured Query Language (SQL) injection[14] weakness applies to all applications that interact with databases using SQL. SALM systems are produced in-house by some of the most mature application security organizations in security-sensitive industries, such as software development, financial services and e-commerce. Commercial solutions also exist.

> "SALM systems seek to close the gaps in the current detection-focused software security space."

SALM content providers continuously update the database of common software security flaws and corresponding compensating controls tied to rules. Developers or security analysts can, thus, model an application by profiling its technology stack, compliance requirements and other properties. Based on the application's profile, SALM tools generate a series of checklists of preventive controls and corresponding guidelines to follow in various phases of the SDLC.

Each checklist item specifies an underlying security weakness, a succinct discussion of the control and a contextually tailored guideline based on the technology stack specified in the application priorities. With this structure, users can achieve three pillars of application life-cycle management: contextual training, project and progress tracking, and auditability.

CONTEXTUAL TRAINING

By providing contextually relevant tasks, SALM systems reinforce one of the most effective application security controls—developer awareness training—while reducing the cognitive burden of remembering all relevant security issues.

The training is contextually relevant, thereby increasing its effectiveness.[15] The SALM system may also provide examples of known good source code in the developer's programming language. Moreover, by providing instructional videos on how to test for defects, SALM systems provide contextual training on how an attacker may exploit an underlying weakness.

PROGRESS TRACKING AND AUDITABILITY

SALM solutions provide auditability into application security posture. Currently, many organizations assess application security posture by manual risk assessments[16] or by testing for security through dynamic and static analysis. Consistent risk assessments can often be difficult to deploy for information security. One practitioner suggests: "Security is more like art, and a security risk really cannot be calculated."[17] Approaches such as penetration testing also have limitations such as cost.[18] SALM solutions detail lists of controls for known software security weaknesses and track completion status. As a result, security auditors can quickly ascertain if an in-house, outsourced or COTS application has appropriately handled security controls by profiling the application in a SALM solution and tracking which security controls are completed.

Knowing security controls upfront allows development teams to build cost estimates and prioritize security issues alongside other priorities at project or iteration inception. Application owners can decide to accept risks at the planning stage. Upfront discussion and risk acceptance have the benefit of side-stepping disagreements later in a development cycle and avoiding a culture of development vs. security.[19]

CONCLUSIONS

SALM solutions offer the unprecedented ability to achieve auditable and scalable prevention-based application security. Although detection-based controls such as static and dynamic analysis are still critical components of an overall secure SDLC, early evidence shows a clear business case for adopting a SALM solution.

The fact that enterprises in disparate industries have independently developed SALM systems in-house points to a pervasive need. Combining this with the ability to provide visibility into application security risk posture across an enterprise, SALM solutions are indispensable for reducing the risk of common weaknesses of software developed or purchased. IT controls auditors should consider the existence of SALM systems when auditing the effectiveness of an enterprise's application security posture.

ENDNOTES

1 IT Governance Institute, COBIT 4.1, AI2.4 Application Security and Availability, 2007, *www.isaca.org/Knowledge-Center/cobit/Documents/CobiT_4.1.pdf*

2 BSIMM3, "Intelligence: Standards and Requirements (SR)," *www.bsimm.com/online/intelligence/sr/*

3 Chandra, Pravir; "Software Assurance Maturity Model: A Guide to Security Requirements," *www.opensamm.org/downloads/SAMM-1.0.pdf*

4 Microsoft, Microsoft Security Development Lifecycle (SDL) Process: Requirements, *www.microsoft.com/security/sdl/discover/requirements.aspx*

5 The Open Web Application Security Project (OWASP), *A Guide to Building Secure Web Applications and Web Services, 2.0 Black Hat Edition*, 27 July 2005, *http://sourceforge.net/projects/owasp/files/Guide/2.0.1/OWASPGuide2.0.1.pdf/download*

6 The 451 Group, "The Application Security Spectrum: From Concept to Cloud," *www.the451group.com/reports/executive_summary.php?id=1832*

7 OWASP-ASVS, "V3 - Session Management Verification Requirements," February 2012, *http://code.google.com/p/owasp-asvs/wiki/Verification_V3*

8 Sethi, Rohit; Yuk Fai Chan; "Domain-Driven Security," OpenSAMM, January 2011, *www.opensamm.org/2011/01/domain-driven-security/*

9 Grubb, Ben; "Security Experts Go to War: Wife Targeted," *Sydney Morning Herald*, 17 May 2011, *www.smh.com.au/technology/security/security-experts-go-to-war-wife-targeted-20110517-1eqsm.html*

10 LKP Consulting Group, "The Real Cost of Software Defects," *www.lkpgroup.com/Cost%20of%20Software%20Defects.pdf*

11 Veracode, *State of Software Security Report*, vol. 4, p. 6

12 Jing, Xie; Bill Chu; Heather Lipford; "Idea: Interactive Support for Secure Software Development," In Proceedings of Engineering Secure Software and Systems 3rd International Symposium (ESSoS), Madrid, Spain, February 2011

13 IBM, "Application Lifecycle Management: Effective ALM Helps Capital District Physicians' Health Plan Immediately Increase Efficiency," 2008, *www-142.ibm.com/software/products/us/en/category/SW860*

14 The Open Web Application Security Project (OWASP), "SQL Injection," 2012, *www.owasp.org/index.php/SQL_Injection*

15 Jing, Xie J.; B. Chu; Lipford H. Richter; "Why Do Programmers Make Security Errors?," Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC), 18–22 September 2011, Pittsburgh, Pennsylvania, USA

16 Stoneburner Gary; Alice Goguen; Alexis Feringa; SP 800-30 *Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology (NIST), July 2012, p. 8, *http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf*

17 Faessler, Mike; "Improving Security Risk Management," Web Wire, June 2011, *www.webwire.com/ViewPressRel.asp?aId=138969*

18 Wai, Chan Tuck; "Conducting a Penetration Test on an Organization," SANS Institute, 2002, *www.sans.org/reading_room/whitepapers/auditing/conducting-penetration-test-organization_67*

19 Wilander, John; "Security People vs. Developers," February 2011, *http://appsandsecurity.blogspot.com/2011/02/security-people-vs-developers.html*

The Changing Face of Cybersecurity

Stewart Hayes has been involved in risk management and security practices for more than 25 years, providing specialist consultancy services in the Americas, Asia Pacific, Europe and the Middle East. Hayes can be reached at *stewart.hayes@jakeman.com.au*.

Malcolm Shore has an extensive IT background with more than 20 years of experience in security and risk management. He can be reached at *malcolm.shore@stratsec.com.au*.

Miles Jakeman, Ph.D., is a business management specialist. As the Citadel Group Limited's managing director, Jakeman has advised senior business leaders and government officials on a number of occasions, including representing countries in ministerial forums.

In today's environment, it is commonplace for business transactions—everything from home shopping to multibillion-dollar deals—to take place over the Internet. But, while the Internet has developed rapidly as a channel for business, security on the Internet has lagged. The Internet has a well-earned reputation as a hostile environment, and the growth of organised cybercrime is evidence that there is not enough being done to manage the risk. In 2004, Butler Lampson noted:

> *After thirty years of work on computer security, why are almost all the systems in service today extremely vulnerable to attack? The main reason is that security is expensive to set up and a nuisance to run, so people judge from experience how little of it they can get away with. Since there's been little damage, people decide that they don't need much security. In addition, setting it up is so complicated that it's hardly ever done right. While we await a catastrophe, simpler setup is the most important step toward better security.*
>
> *In a distributed system with no central management like the Internet, security requires a clear story about who is trusted for each step in establishing it, and why. The basic tool for telling this story is the 'speaks for' relation between principals that describes how authority is delegated, that is, who trusts whom. The idea is simple, and it explains what's going on in any system I know. The many different ways of encoding this relation often make it hard to see the underlying order.*[1]

Over the last 20 years, there has been immense growth in the number of computing and network services, enabling transactions to be undertaken by the smallest businesses across a global marketplace. At the same time, there has been a growing community of individuals who have sought to exploit the vulnerabilities of network devices, computer systems and applications.

IT systems have proved over the last 20 years to be less than perfect, requiring compensating controls to address problems when they arise. Vendors continually release tactical patches and upgrades to fix problems, but hackers with knowledge, skills and capability have developed and released exploits and easy-to-use tools to enable even the least technical users to become adversaries.

At the user level, the approach to securing government and business systems has seen little change, with a continuing model of perimeter protection through firewalls and soft internal networks; limited, if any, segregation of applications; and the continuing use of ineffective security mechanisms such as password authentication. Even the more advanced security mechanisms such as encryption and two-factor authentication have not lived up to their promises, their fragility exposed through incidents such as the RSA breach[2] and the failure of MD5.[3] Vendors have delivered sophisticated monitoring capabilities to alert operators should unauthorised changes or accesses be attempted, but few user organisations have the ability to configure the equipment adequately enough to deliver effective security. Organisations such as the International Organization for Standardization (ISO) and the PCI Security Standards Council have created and driven the adoption of security standards, but the levels of penetration, effectiveness of implementation and even their suitability to protect against sustained attack are all questionable.

For those organisations with multinational locations, local legislation often causes variances to the security model, potentially opening holes in security and creating attack vectors in the more secure parts of the network. Data are transferred and modified across multiple systems, which may result in discrepancies and possible errors. Outsourcing of services or data storage facilities

is often done with little due diligence on provider security capability and hiring policies. Trying to manage records consistently in a dispersed environment (which may or may not be within the organisation's control) can be a nightmare for the security manager.

The ability to evolve a digital society and to gain the many promised benefits depends in large part on a widespread confidence in the fabric of cyberspace. The denial-of-service attacks against Paypal and Amazon.com (2010), CNN (2008), Twitter (2009), the Australian Parliament (2010) and US oil firms (2011) may or may not have been successful in damaging the target, and indeed may have been used for publicity by Internet security companies, but they have increased public concern over security in cyberspace. The more serious intrusion attacks against Sony Corp. (in which credit card details of thousands of gamers were released) and RSA (in which highly sensitive information relating to its secure two-factor authentication device was compromised) demonstrate that the Internet is increasingly a very dangerous place to operate.

> "Serious intrusion attacks…demonstrate that the Internet is increasingly a very dangerous place to operate."

Cybersecurity as a national strategy and plan needs to deliver not only better security in government and business services, but a fundamental shift in the safety of the electronic environment in which they operate.[4] Over the last 20 years, the IT community has failed to deliver a data utility that has the level of trust common in other utilities. What can the IT community do to turn around the current obstacles to developing an effective digital society?

WHAT HAS CHANGED?

So what has changed on the Internet? The answer, of course, is everything—business activities, information technology, the communications environment and the threat landscape. Today, vendors and attackers have become embroiled in a cyber arms race, and users are the losers. There are regular reports of government and business systems being infiltrated and data breaches in government departments. Consumers' computers, wireless modems and, increasingly, cell phones are being subverted, and even the basic fabric of cyberspace is under attack, with nations demonstrating their ability to take control of the Internet.[5]

In the last five years, there have been a number of fundamental shifts in technology and its use that require equally fundamental shifts in attitudes towards security. Information technology has evolved from purely a means of systems automation into an essential characteristic of society: cyberspace. The kind of quality, reliability and availability that has traditionally been associated only with power and water utilities is now essential for the technology used to deliver government and business services running in cyberspace.

Technology is changing rapidly, and another fundamental shift is occurring with the emergence of cloud computing. Cloud computing enables individuals and organisations to access application services and data from anywhere via a web interface; it is essentially an application service provider model of delivery with attitude. The economies possible through use of cloud, rather than internal IT solutions, will inevitably see the majority of businesses and, increasingly, governments running in the cloud within the next five years. This substantially changes the ways in which organisations can affect and manage both their IT function and security in their systems.

Today's security standards were developed in a world in which computers were subject to fraud and other criminal activities by individuals inside and, in some cases, outside the organisation. However, this has changed in the last five years with the rapid increase in organised cybercrime through the emergence of robot networks (botnets), which enable criminal activity to be conducted on an unprecedented global scale and can also be used as force multipliers to deliver massive denial-of-service attacks on targeted businesses—at a level at which nations are increasingly at risk of being cut off from the global Internet.

Unfortunately, the capability of national police forces to stop global cybercrime is developing much more slowly than the technical abilities of cybercriminals. Cybercrime is now arguably a bigger issue than illegal drugs. The adoption of the Council of Europe Convention on Cybercrime is setting the scene for a global response to cybercrime, and there are signs that police forces globally are working together. However, much more needs to be done to develop the concept of a global jurisdiction before an adequately agile response to cybercrime can be developed.

In what is increasingly recognised as a Hobbesian[6] world, government systems are under relentless attacks from other nations seeking to gain national intelligence and industrial information. While China has been publicly accused of such

activity,[7] many nations are known to possess such a capability. Further, offensive use of the Internet by nation states is not limited to the intelligence sector. The paradigm, based on the movie *War Games*, of adolescents breaking into defence systems and playing war games has given way to credible evidence in cases, such as the one in Estonia,[8] of state-sponsored attacks by professional armies of cyberwarriors within or sponsored by the military. Indeed, the US has created its own Cyber Corps[9] and now considers a cyberattack as a standard component of a campaign.

WHERE TO GO FROM HERE?

Many of the shortcomings in technology and technology management discussed previously were recognised many years ago, but nationally, commercially and personally sensitive systems continue to be installed and operated with these shortcomings. Indeed, with improvements in technology and capability, organised attackers are much more easily able to cause disruption and fraud. There are a number of specific steps that can be taken to improve the situation and redress somewhat the woeful state of affairs in which the information security industry finds itself.

Given the number of vulnerabilities that exist in new applications (as demonstrated by the numerous security patches that are issued by major software vendors), the plethora of tools available to cause mayhem across organisations connected to the Internet, and the growing knowledge and capability of the user community, government and industry are avoiding major incidents through luck rather than good judgement. Can government and industry continue absorbing these threats to their business model, knowing that, with the deployment of the Australian National Broadband Network, for example, and Internet Protocol version 6 (IPv6), the frequency and severity of issues will only increase? Higher bandwidth and increased computing power may extend the ferocity of any concerted attack, and every IP-enabled device could become a potential threat—not just home computers, but also household appliances, cars and mobile phones. In cyberspace, one's refrigerator could be a hostile agent. Following the Irish Republican Army (IRA)'s bombing of the Brighton Grand Hotel in 1984, the IRA released a statement that said '...we only have to be lucky once; you will have to be lucky always'. So it is with cyberspace.

Understanding the Threat Source

Clearly, understanding the source of any threat and the likelihood of the threat being a danger to an organisation's business interests is a critical first step in building a cybersecurity strategy. Steven Bucci describes the threat actors as shown in **figure 1**.[10]

Figure 1—Threat Actors

Threat Sources	Description
Bot network operators	Bot network operators are hackers; however, instead of breaking into systems directly, they take over multiple systems to co-ordinate attacks and distribute phishing schemes, spam and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organised crime groups are using spam, phishing and spyware/malware to commit identity theft and online fraud.
State-sponsored actors	Foreign governments and intelligence services use cybertools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programmes and capabilities.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites.
Insiders	The disgruntled organisation insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals or small groups who execute phishing schemes in an attempt to steal identities or information for monetary gain
Spammers	Individuals or organisations that distribute unsolicited email with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware or attack organisations (e.g., denial-of–service attacks)
Spyware/malware authors	Individuals or organisations that produce and distribute spyware and malware, sometimes for free and sometimes to sell to the highest bidder
Terrorists	Terrorists seek to destroy, incapacitate or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the global economy, and damage public morale and confidence.

Steven Bucci shows that while cyberthreats are changing from individual hackers through organised crime and terrorist-based attacks to national- or state-sponsored cyberattacks, the level of danger is correspondingly increasing.[11] Thus, while individuals may cause mayhem, it has been largely unsustainable and fairly contained. Now an attack may result in widespread destruction and an ongoing undermining of state sovereignty.

This follows the accepted crime model: Is the value of the target sufficient to warrant an access attempt, what is the likelihood of getting caught, and how difficult or expensive is the undertaking? The profiles of each of these aspects determines the demographic of a likely attacker. Similarly, changing the parameters of each of these aspects affects the likelihood of being targeted—bearing in mind that a state-sponsored cyberattack is likely to have extensive resources.

Avoiding Vulnerabilities

The problems in cyberspace do not come from threats alone, but from the combination of threats and vulnerabilities. The vulnerabilities are neither more nor less than byproducts of a low or non-existent level of quality in personnel and products used to provide cybersecurity.

It is no longer acceptable for professionals, tradespeople, products and services that are critical to the success of cyberspace to operate *caveat emptor*. Professions such as law, medicine and psychology are controlled through rigorous professional standards, while other professions such as accountancy have established institutes that award chartered qualifications. In some countries, a recognised qualification is mandatory for an individual to register as a tradesperson, such as an electrician or a builder. The establishment of cybersecurity as a profession and a trade is well overdue.

Countries are increasingly recognising the requirement for cyberspace to be built upon a reliable infrastructure. In the UK, to ensure telecommunications service providers deliver an IP infrastructure at the same level of quality as it has its analog networks, an incentive model of public-private partnership for the delivery of infrastructure services to government departments based on the next generation security standard[12] has been established. Many countries, including Australia, have released Internet service provider (ISP) codes of practice,[13] which incorporate requirements for ISPs to take some responsibility for the content on their connections.

Building trustworthy software (i.e., software without exploitable weaknesses) continues to be a challenge. While there are theories, models and techniques for developing secure architectures and coding secure software, this has been ineffective in driving the IT industry. In part, the academic community has been blind to the need for software security to be a core element of any computer security curriculum, and, in part, vendors have been too ready to build new systems on insecure foundations, patching holes rather than rebuilding fundamentally secure systems. There is no easy solution to this problem, although linking research funding to programmes that meet basic cyberspace requirements would be a good start. Also, continuing the use of selective purchasing by governments will drive more responsible academic and vendor behaviours.

While avoiding vulnerabilities is the 'holy grail', the reality is that vendors continue to create vulnerabilities. Adopting a security strategy that focuses on situational awareness is now an important foundation for understanding threats. Organisations must stay informed about attack trends and specific-to-them security exposures, and be able to react to these. In addition, testing systems against known security exposures provides a defence-in-depth approach to managing such vulnerabilities. A simple penetration test of an organisation's external systems

will reveal configuration issues or unapplied patches. Hardening systems is another technique used to limit exposure from vendor-delivered vulnerabilities, by closing unused connections and checking for password vulnerabilities, dormant accounts and other weaknesses that may be exploited by any number of readily available attack tools.

For business, however, cyberspace is just a means by which business can be conducted, not an end in itself. Businesses are evolving rapidly to ensure that they remain competitive and are able to meet customer demand, increasingly through strategic alliances. One of the most effective quality controls that can be put in place is to conduct ongoing, high-quality due-diligence reviews on organisations with which information is shared, to which services are outsourced or with which information is sourced. As described by Peter Keen in 2002:

> *Business process outsourcing (BPO) is the investment strategy for sourcing best practice process capabilities end to end along business value chains: the customer relationship chain, supply chain, organizational productivity chain, and product and service innovation chain. It is intensively collaborative because it rests on meshing the BPO client's skills, technology base and processes with the BPO provider's distinctive offerings. It is additive —strengthening capabilities along the value chain.*[14]

More often than not, the technology used by partner organisations exists in other countries with complex legal arrangements and data ownership laws—and possibly an implicit or explicit legal act, such as the US Patriot Act.

While the new threats to cyberspace come from outside, this does not mean that insider attacks have ceased. Insufficient attention is often given to carrying out background checks on staff and contractors as they are hired and during their employment, validating the quality of security contractors installing equipment, continually testing implemented controls and reviewing the organisational risk profile. Simple actions such as these are a start, but much more needs to be done to ensure that users can rely on their cyberservices to the same extent as they rely on power and water. National cybersecurity strategies will affect some of the improvements needed to deliver an adequate level of quality in cyberspace, but this will need to be supported by strong industry and consumer support through discretionary purchases and employment.

Understanding the Business

While work continues on developing and fielding the foundations of a secure cyberspace environment, digital societies are emerging that are less than perfect. For these societies to survive, and possibly even thrive, there must be a clear and absolute understanding of the risk and development of management approaches that mitigate it. At an individual business level, traditional security solutions are often applied with little understanding of the business needs and business information provenance and flow. Without this, it is difficult to properly assess the risk, and without a good risk profile, it is hard to build effective solutions that obviate the need for complex and unwieldy security controls.

"Without a good risk profile, it is hard to build effective solutions that obviate the need for complex and unwieldy security controls."

Aligning the business needs, information flows and security architecture requires the cybersecurity professional to understand:

- The business, the strategic objectives, the market, the stakeholders and what information is used and shared
- The business information flows, relationships and dependencies
- The value of the business information in financial, strategic and operational terms
- The impact of failure in information management—corruption, loss or disclosure—and failure in the service provided
- What it takes to recover to a manageable position in the event of failure, and (to understand) where that is not possible
- The relationships inside and outside of the business, and how failures in one area can impact other areas

With this understanding, the cybersecurity professional can start to develop the risk profile for the business and derive options for establishing a security model both from a budgetary and architecture perspective.

Architecting the Solution

By understanding the business and the operational environment, it is possible to develop a security model that is

effective and sustainable. Generic security models have been developed over the years based on physical security controls to protect information and systems that are housed in a single or defined location as well as an electronic perimeter to protect systems that are complete in themselves; however, these models no longer apply. With the advent of virtual companies that exist predominantly on the Internet, with staff members working in a variety of locations, and with information on mobile devices and in the cloud (and where is that?), traditional models can protect only a fraction of the business information. Most of the security expenditure today is focused on some form of compliance and not on protecting the critical business information.

> "Technology needs to be architected to reduce the propensity for attacks in cyberspace."

Technology needs to be architected to reduce the propensity for attacks in cyberspace. This will require a fundamental rethink of the way services are provided to the network. 'The old walled-garden approach to computer security with its firewalls and intranets seems out of step'.[15]

The Open Group's Jericho Forum[16] advocates an approach more aligned with cyberspace and one that addresses the de-perimeterisation of organisational systems. The Jericho model is based on establishing trusted paths between partner organisations, improving authentication of users (human and machine) and information, and improving access controls at a more fundamental level of information. This enables business to collaborate with more confidence.

By also creating an architecture that is resilient and self-healing, the effects of an attack on a single target can be minimised. This approach was first advocated in 1989 as the Digital Distributed System Security Architecture (DDSSA):

> *The architecture covers user and system authentication, mandatory and discretionary security, secure initialisation and loading, and delegation in a general-purpose computing environment of heterogeneous systems where there are no central authorities, no global trust, and no central controls. The architecture prescribes a framework for all applications and operating systems currently available or to be developed. Because the distributed system is an open OSI environment, where functional interoperability only requires compliance with selected protocols needed by a given application, the architecture must be designed to securely support systems that do not implement or use any of the security services, while providing extensive additional security capabilities for those systems that choose to implement the architecture.*[17]

The initial thinking around DDSSA was followed by the development of the concepts of survivable networks,[18] which can continue, albeit in a reduced manner, to deliver critical services when under attack. Robust and reliable systems based on these concepts have yet to emerge in the product space and be widely deployed, although the emergence of a resilient network standard[19] should go some way towards addressing these issues.

In cyberspace, the focus must be on the protection of information. Information exists either in stored form or in transit across cyberspace, and in either form, it can be stolen with no discernible change. Once stolen, it can be altered or re-sourced and used for repeat frauds. Access controls may reduce this risk in a private setting, but not when information is placed in the public domain. Digital rights management (DRM) technology has been developed to meet this challenge by enabling controls to be applied to information items that prevent changing, copying, printing, forwarding or executing (applications). Organisations such as the Electronic Frontier Foundation (EFF) see this as an infringement of the individual's rights to access and share information freely, so DRM has not had widespread adoption.

In cyberspace, planning for business continuity continues to be important. As systems become more reliable, businesses become more dependent on them and the impact of failure increases dramatically. In the 2011 Christchurch (New Zealand) earthquake, an estimated 25 percent of buildings were or had to be destroyed, requiring wholesale relocation, and many businesses were unable to recover material from the buildings before they were demolished.[20] While the use of cloud services would reduce exposure to such localised events, the cloud itself is not a panacea for all ills, as demonstrated by Amazon.com's cloud failure in 2011.[21] In fact, the use of cloud services brings with it major issues relating to data ownership and the ability to recover data from clouds in the event of service termination. A successful business continuity

plan not only ensures that business activity is able to continue and business data and systems are recovered, it also includes damage control over customer relationships.

SUMMARY

Although the scale of activity involving highly sensitive transactions over the Internet has increased dramatically over the last 20 years, there has been very little in terms of step change in the security industry. Vulnerabilities that were identified and exploited in the early 1990s remain and continue to be exploited to greater effect in the 2010s. There has been slow uptake of the security architectures that could address these vulnerabilities, while the improvement in technology and communications has made it easier to carry out attacks.

There is no single solution or panacea to the issues of cybersecurity, nor should there be. Each organisation should assess what its needs are, how it intends to conduct its business activities and what the risks are to that process. There are a plethora of highly capable solutions that can then be implemented and, more important, maintained.

Consumers in cyberspace, be they government, industry or society, continue to be more mobile, more demanding and less tolerant of failure. While there is an increased awareness of threats, often the increased adoption of security comes only after data breaches and system failures.

Security is not an adjunct or add-on to cyberspace; it is a fundamental aspect that must be considered alongside all other core functions to ensure that the business can meet its strategic objectives. Academics need to include cybersecurity as a core component of computer and information science to deliver a workforce properly prepared for its role in the digital society. The organisation's leaders need to ensure that security architectures are developed to reflect the needs of the business, that the people it employs are certified professionals and tradespeople, and that the technology products and services that it uses are fit for purpose. For its part, government can usefully set the necessary standards and lead by example.

New governance models need to be developed that provide a consistent and effective basis for trust in a business process co-sourcing environment, and should ensure the existence of testing, monitoring and business continuity.

Security technology continues to be complex and unwieldy, and not well aligned with consumer needs. Having to remember multiple IDs and complex passwords is a major inconvenience and a cause of many security issues. Posting personal information to public sites continues to be a contributing factor to identity theft. Firewalls protect what information is left behind inside the corporate electronic perimeter, but do little to protect the vast amount of business-sensitive information outside. Intrusion detection systems detect yesterday's problems, but not tomorrow's problems. Security models, architectures and technologies need to reflect these concerns.

Multiple activities within the business do not mean that there should be multiple security architectures to support them. Having a single, consistent and persistent approach that is proven and flexible is much easier to maintain.

> "There is no single solution or panacea to the issues of cybersecurity, nor should there be."

However, this does require a good understanding of the business objectives, the operational market and the risks the business faces. Hence, the security model must recognise that protection of services and information in itself is not enough; the company must be able to recover from failure and continue to operate at a level expected by its operating partners and customers. And, it must be able to demonstrate that capability on a continuous basis.

ENDNOTES

[1] Lampson, Butler W.; 'Computer Security in the Real World', *IEEE Computer*, 6 June 2004, *http://research.microsoft.com/en-us/um/people/blampson/69-SecurityRealIEEE/69-SecurityRealIEEEpub.pdf*

[2] Williams, Alex; 'RSA Breach: An Attack That Used a Social Media Boobytrap?', ReadWrite Enterprise, 18 March 2011, *www.readwriteweb.com/enterprise/2011/03/rsa-breach-an-attack-that-used*

[3] Wang, Xiaoyun; Hongbo Yu; 'How to Break MD5 and Other Hash Functions', *www.cs.cmu.edu/~bhiksha/11-795.privacy/reports/How.to.break.MD5.and.Other.Hash.Functions.pdf*

[4] Banks, Lisa; 'Attorney General Outlines Cyber Security Strategy', *CIO*, 20 July 2011, *www.cio.com.au/article/394302/attorney-general_outlines_cyber_security_strategy/*

[5] PBS, 'China's Internet "Hijacking" Creates Worries for Security Experts', 26 November 2010, *www.pbs.org/newshour/bb/science/july-dec10/chinainternet_11-26.html*

[6] Williams, Michael C.; 'Hobbes and International Relations: A Reconsideration', JSTOR, 1996, *www.jstor.org/pss/2704077*

[7] Norton-Taylor, Richard; 'Titan Rain—How Chinese Hackers Targeted Whitehall', *The Guardian*, 4 September 2007, *www.guardian.co.uk/technology/2007/sep/04/news.internet*

[8] As reported in various publications, including: Tiirmaa-Klaar, Heli; 'Cyber Security Threats and Responses at Global, Nation-state, Industry and Individual Levels', *SciencesPo*. Shackleford, Scott; 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem', University of Cambridge. Greenberg, Andy; 'When Cyber Terrorism Becomes State Censorship', Forbes.com.

[9] US Department of Defense, Cyber Strategy, *www.defense.gov/home/features/2011/0411_cyberstrategy/*

[10] Bucci, Steven; 'The Confluence of Cyber Crime and Terrorism', The Heritage Foundation, 12 June 2009, *www.heritage.org/Research/Lecture/The-Confluence-of-Cyber-Crime-and-Terrorism*

[11] *Ibid*.

[12] 'CESG IL2/IL3 Accreditation (224 & 334)', 21 October 2010, *http://interweave-consulting.blogspot.com/2010/10/cesg-il2il3-accreditation-224-334.html*

[13] News4Us, 'Australian ISP Code of Practice Now in Effect', 2 December 2010, *www.news4us.com/australian-isp-code-of-practice-on-cyber-security-icode-now-in-effect/223611/*

[14] Keen, Peter; 'Business Process Outsourcing: Imperative, Historically Inevitable, Ready to Go', 2004, *http://ebcs-consulting.com/wp-content/uploads/2010/10/BPO.pdf*

[15] Lohr, Steve; 'The Internet Firewall: R.I.P.?', *The New York Times* Bits, 11 September 2007, *http://bits.blogs.nytimes.com/2007/09/11/the-internet-firewall-rip/*

[16] The Jericho Forum Vision, *www.opengroup.org/jericho/*

[17] Gasser, Morrie; Andy Goldstein; Charlie Kaufman; Butler Lampson; 'The Digital Distributed System Security Architecture', 1989, *http://research.microsoft.com/en-us/um/people/blampson/41-DigitalDSSA/41-DigitalDSSAAsPub.pdf*

[18] Shore, Malcolm; Xianglin Deng; 'Architecting Survivable Networks Using SABSA', 23 September 2010, *http://wenku.baidu.com/view/9bc51f1efc4ffe473368abb5.html*

[19] *www.cesg.gov.uk/products_services/iacs/cas/faqs-comms.shtml*

[20] Stevenson, Joanne; Hlekiwe Kachali; Zachary Whitman; Erica Seville; John Vargo; Thomas Wilson; 'Preliminary Observations of the Impacts of the 22 February Earthquake on Organisations and the Economy', 18 April 2011, *www.resorgs.org.nz/pubs/EconImpacts_22Feb_ChristchurchEarthquake.pdf*

[21] Gilbertson, Scott; 'Lessons From a Cloud Failure: It's Not Amazon, It's You', *Wired*, 25 April 2011, *www.wired.com/epicenter/2011/04/lessons-amazon-cloud-failure/*

SME Cybersecurity and the Three Little Pigs

David R. Han is a technology consultant specializing in information assurance, and works as the computer network defense (CND) architect for policy, plans, and governance, risk and compliance management. He supports the US federal government, ensuring that agency cyberincident handling and response processes align with federal mandates, industry standards and management best practices. Han has more than 27 years of process engineering, quality engineering, compliance management, metrics development and requirements analysis experience.

Small and medium-sized enterprises (SMEs) are very susceptible to cyberattacks, but many of them ignore the threat, hoping it will pass them by, or perhaps they do not recognize its severity. Cybersecurity is getting a lot of attention due to the actions of hacktivists, cybergangs and nation states. Hacktivists are trying to make a statement, cybergangs are seeking easy money, and nation states are using hackers to conduct espionage.

Cybersecurity attacks have increased in frequency and affect virtually all industries. Law enforcement is relegated to playing catch-up because it is hampered by the lack of laws and the fact that cyberattacks often originate in other countries. Ultimately, the cyberattacker is aided by the ignorance of users, naiveté of companies and the difficulty of capture/enforcement. SMEs must take action now to secure their networks from hackers or continue to accept the risk of assured intrusion and cyberpilfering of their most precious assets.

THE PROBLEM

The Internet is as lawless and free as the Wild West,[1] and everyone faces the same dangers and potential pitfalls. Cyberattacks are a common occurrence. "The average time to resolve a cyberattack is 18 days, with an average cost to participating organizations of US $415,748 over this 18 day period."[2] This means that the average dwell time is often greater than 18 days. The dwell time is a measure of the time an intruder is on the network before being discovered and extricated. With that in mind, how much damage can an intruder do in 18 days beyond the explicit cost of US $415,748?

To mitigate some of these dangers and pitfalls, all businesses, regardless of size, must implement a minimum set of safeguards (firewall, intrusion detection/prevention system [IDS/IPS] and antivirus). Each business can scale its security measures to meet its needs, and it can choose to implement more stringent security measures.

SMEs are generally unsecure due to the lack of properly trained security personnel and a correlating lack of security measures.[3] "A typical medium-sized business with 50 to 1,000 users has an average of 1.8 IT professionals on staff, according to McAfee research. In addition, only eight percent of companies within this market segment typically have a security specialist on staff."[4] If only 8 percent of medium-sized businesses have a security specialist on staff, who is doing the security work within the other 92 percent of medium-sized businesses?

Figure 1 shows the annualized cost of cybercrime for fiscal years 2010 and 2011. The reported maximum value of cybercrime in 2011 is US $36.4 million. Dividing that total by the average cost of an intrusion (US $400,000) reveals that an estimated 91 attacks were concluded in fiscal year 2011. In the "First Annual Cost of Cyber Crime Study" conducted by the Ponemon Institute in 2010, the 45 organizations in the study "experienced 50 successful attacks per week and more than one successful attack per company per week."[5] SMEs cannot continue to ignore cybersecurity.

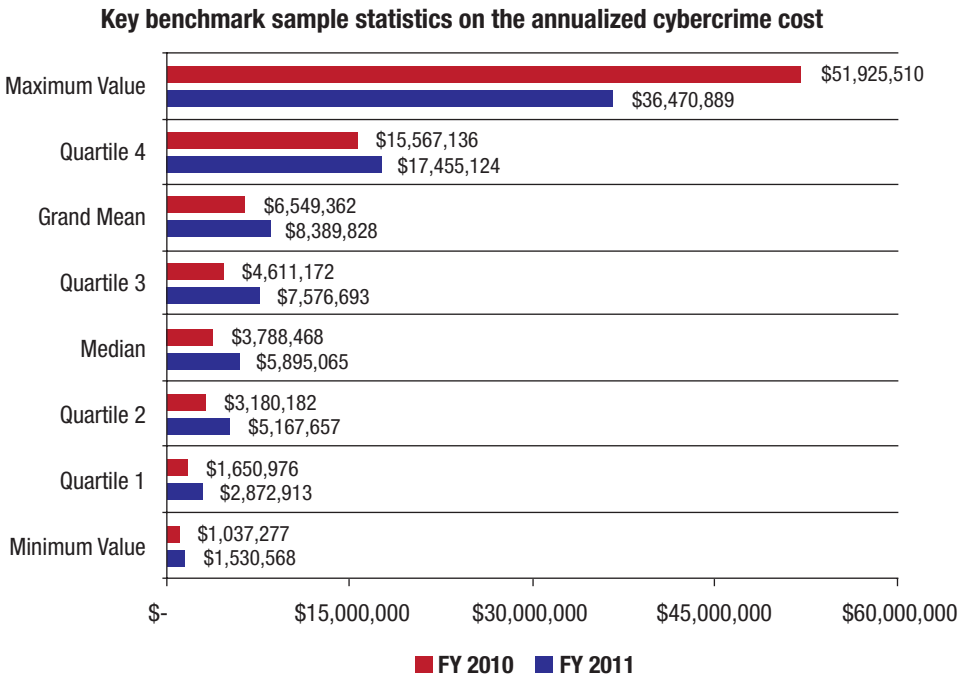
THE THREE LITTLE PIGS—CYBERSECURITY ANALOGY

Most people are familiar with the story of the three little pigs. The three little pigs provide a good analogy of how SMEs can approach cybersecurity. In this version of the story, the hacktivists, cybercriminals and nation states portray the Big Bad Wolf. The three little pigs are SMEs that go off on their own to try and protect themselves from the Big Bad Wolf.

First Little Pig

The first little pig was the youngest brother and did not really understand the threat posed by the Big Bad Wolf. The first little pig thought the company was entirely too small to be of interest to the Big Bad Wolf. He decided to rely on security through obscurity and not really implement any security. His company just did not have enough resources to pay for a cybersecurity engineer, much less an

Figure 1—2010 and 2011 Annualized Cost of Cybercrime



Source: Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies," August 2011. Reprinted with permission.

IT specialist. Besides, all the organization did was make washers that they sold to a defense contractor. Who cared about a company making specialty washers for the defense industry?

The first little pig failed to properly understand the threat that the Big Bad Wolf posed. In this day and age, with the advanced tactics used by the Big Bad Wolf, small companies that supply parts to bigger companies represent the soft vulnerable underbelly. The bigger company's defenses were stronger than the Big Bad Wolf's capabilities, but by hacking into the smaller company and exploiting the trust relationship, the wolf was able to get into the bigger company's networks.

The first little pig thought he could not afford cybersecurity, but the truth was that he could not afford not to implement cybersecurity measures. Bigger companies are starting to understand the threat posed to them by smaller, unsecured businesses. Bigger companies cannot extend the boundaries of their networks to compensate for smaller companies that do not have or cannot afford security countermeasures.

The first little pig was hacked and, due to the intrusion, was forced to file for bankruptcy. He then went running to his sibling's arms.

Second Little Pig

The second little pig understood a little more about cybersecurity than her little brother. Her company made circuit boards used by other companies in their computers. She knew she had to comply with federal mandates and government regulations. But, security was more of a hassle than anything, so she did just the bare minimum to comply. With the recession, did the government not realize that every dollar spent on compliance directly impacted her bottom line? With any more requirements, she would be forced to start laying off some people or cutting back hours. The security architecture included an IDS, firewall and antivirus, but nothing had been patched in 18 months and the antivirus DAT file was 10 months old.

While the second little pig had security measures in place, by doing the minimum required to comply with the mandates and requirements, her company was really not

much better off than the first little pig. The bare minimum, while satisfying requirements, does not offer much in terms of security. Additionally, not patching and allowing the antivirus signatures and definitions to be forgotten vitiated the security measures she had in place. Zero-day attacks are not as prevalent as the number of successful intrusions perpetrated through vulnerabilities that remain unpatched long after the patch was released. Stuxnet was one of the biggest cyberattacks and Stuxnet's attack vectors included zero-day attacks and unpatched vulnerabilities.[6]

Cybercriminals sending a flood of emails containing malicious links create most botnets or attachments,[7] which infect users' workstations and beacon back to the command and control (C&C) server for additional malware or instructions. The botnet herders (those who control the botnets) use unpatched vulnerabilities to gain control of the victim machines.[8] "The most common detection and mitigation techniques include flow data monitoring, anomaly detection, Domain Name Server log analysis and honeypots."[9] Companies that implemented a security incident event management (SIEM) system "experienced a substantially lower cost of recovery, detection and containment than non-SIEM companies. In addition, SIEM companies were more likely to recognize the existence of advance persistent threats (APTs) than non-SIEM companies."[10]

The second little pig received a spear-phishing email from a friend who was stranded in Albania and had no cash. She clicked the link and entered her banking information to send her friend US $100. She did not think anything about the fact that she had not spoken to her friend since high school. Her corporate bank account was hacked and her company's accounts emptied.

Now, the first and second little pigs had to run to their older brother.

Third Little Pig

The third little pig was the oldest. He had seen and experienced more. His company made missile systems and had recently started selling them to Taiwan. He took a proactive stance toward cybersecurity. His company complied with all of the government mandates and actively participated in associations that worked with the government to shape the requirements. Cybersecurity was baked into every system, and it was a force multiplier. Including security in the early requirements development phase ensured that things were done securely and saved the company money because there was no expensive redesign to bolt on security at the end. His company's security architecture was robust, with an IDS/IPS, firewalls, demilitarized zone and a modest honeypot. The enterprise's antivirus was continuously updated at different times throughout the day. The IDS/IPS did not just focus on signature-based defensive measures, but also looked at the heuristics to detect anomalous behavior and network activity that behaves like malware. The third little pig was able to protect his brother and sister and stave off the Big Bad Wolf…for today.

THREATS TO SMES

If companies employ good IT hygiene, such as patching vulnerabilities, malicious code such as agent.btz[11] and even its more sophisticated cousin, Stuxnet, would not be as effective.

> "If companies employ good IT hygiene… malicious code…would not be as effective."

"Most of what we see today is exploitation—that's theft, stealing secrets, either commercial or military," US Department of Defense (DoD) Secretary William J. Lynn told Ray Suarez on *PBS Newshour*. "[But] we know the tools exist to destroy things, to destroy physical property, to destroy networks, to destroy data, maybe even take human lives."[12]

The largest threats to SMEs are a result of the following:

- Adversaries continue to refine their tools and techniques.
- Spear-phishing emails remain the most prevalent attack vehicle.
- Firewalls, intrusion detection systems and antivirus programs are passive, signature-based systems that can detect only *known* exploits and compare MD5 hashes for known malicious code.
- Liberal Internet usage policies force companies to spend more time dealing with network attacks and intrusions.
- Social networking sites pose even more dangers to an SME. There are few legitimate business uses that justify the risk posed by permitting access to social networking sites.
- APTs are any sort of long-term attacks that are advanced only in their persistence. Mandiant.com says that "APT is a sophisticated and organized cyberattack to access and steal information from compromised computers."[13]

- Supply chains are vulnerable to attack and corruption. For example, recent events have seen companies distribute free thumb drives with their products only to find that the thumb drives were infected with malware.

WHAT CAN SMES DO TO DEFEND THEIR NETWORKS?

SMEs can implement protective measures to proactively defend their networks. Any measures an SME implements must be composed of people, processes and technology. As previously discussed with the second little pig, there is a minimum level of security measures involving technology that should be implemented. Technology serves well for automating work and processes. However, even with the most cutting-edge SIEM system implemented and fine-tuned to rule out all false positives and catch all false negatives, someone still has to be there to investigate the alerts and interpret the reports. Technology alone is not the solution, but should be part of the solution. The following is a list of what an SME can do to protect its networks:

> "Technology alone is not the solution, but should be part of the solution."

- Manage network and applications vulnerabilities by establishing a vulnerability management program and patch those vulnerabilities.
- In addition to IDS/IPS, antivirus and firewalls, deploy an SIEM solution to monitor network traffic (especially outbound traffic).
- Implement a network forensics capability to identify, contain, isolate and eradicate the intruders.
- Implement protective measures to defend the networks and address the people, processes and technologies.
- Implement governance, risk and compliance management:
  - Governance—Consider adopting standards or frameworks such as ISACA's COBIT for governance and management of enterprise IT (GEIT).
  - Compliance—Be aware of and adhere to federal regulations as well as regional/local laws.
  - Risk—Look at and implement other federal regulations and requirements, such as NIST Special Publication (SP) 800-37 *Risk Management Framework* and NIST SP 800-53 *Recommended Security Controls for Federal Information Systems and Organizations.*

Enjoying this article?

- Read the *Cybercrime Audit/Assurance Program.*
  www.isaca.org/cybercrime-AP
- Discuss and collaborate on cybersecurity in the Knowledge Center.
  www.isaca.org/topic-cybersecurity
- Attend North America ISRM/IT GRC, where track 1 is Thwarting Cyberthreats.
  www.isaca.org/governancerisk

- Establish and implement a program of mensuration. Metrics and frameworks provide a good indication of an organization's overall security posture. Both metrics and frameworks examine indicators to measure the effectiveness of security measures. Metrics, when used properly, assist leaders and managers in making effective decisions about the allocation of finite resources.
- Invest in people and training for cybersecurity professionals. People are the third leg of any security solution. US DoD 8570.01-M *Information Assurance Workforce Improvement Program* mandates that all employees (government, military and contractor) filling information assurance roles must be certified to demonstrate a base knowledge required to fulfill those roles. There are a number of organizations, such as ISACA, (ISC)², SANS, CompTIA and EC Council, that provide information assurance training and certifications. Certifications can be expensive, and finding good qualified people with the desired certifications can be a pricey challenge. In some cases, it may be easier for organizations to grow their own qualified individuals, through training. This training can also help employee retention by making employees feel valued and part of the team. Enterprises need to provide regular training (not just once a year) on cybersecurity for their employees, customers and users. Anyone who can access the enterprise's network or computers should be included in cybersecurity training. SMEs should also ensure that any company they do business with requires and conducts similar training for its employees. A threat to one company is a threat to all.

- Ensure that effective policies are in place. Policies establish guidelines for appropriate use of company assets, proper employee conduct, Internet usage and email.

MSN Money recently published an article listing "9 Ways to Avoid Cybercrime." These tips are good tips and apply to SMEs and consumers alike:[14]

- Do not click on links in suspicious emails, even those that appear to be from friends.
- Know how to recognize phishing.
- Recognize that a smartphone is really a pocket-sized computer and is prone to the same types of attacks directed at a laptop and desktop.
- Keep personal information to yourself.
- Know the pitfalls of public Wi-Fi.
- Beware of public computers.
- Use credit cards, rather than debit cards, when making purchases online.
- Purchase only from reputable web sites (and look for "https" in the web address). Check accounts and credit reports regularly.

CONCLUSION

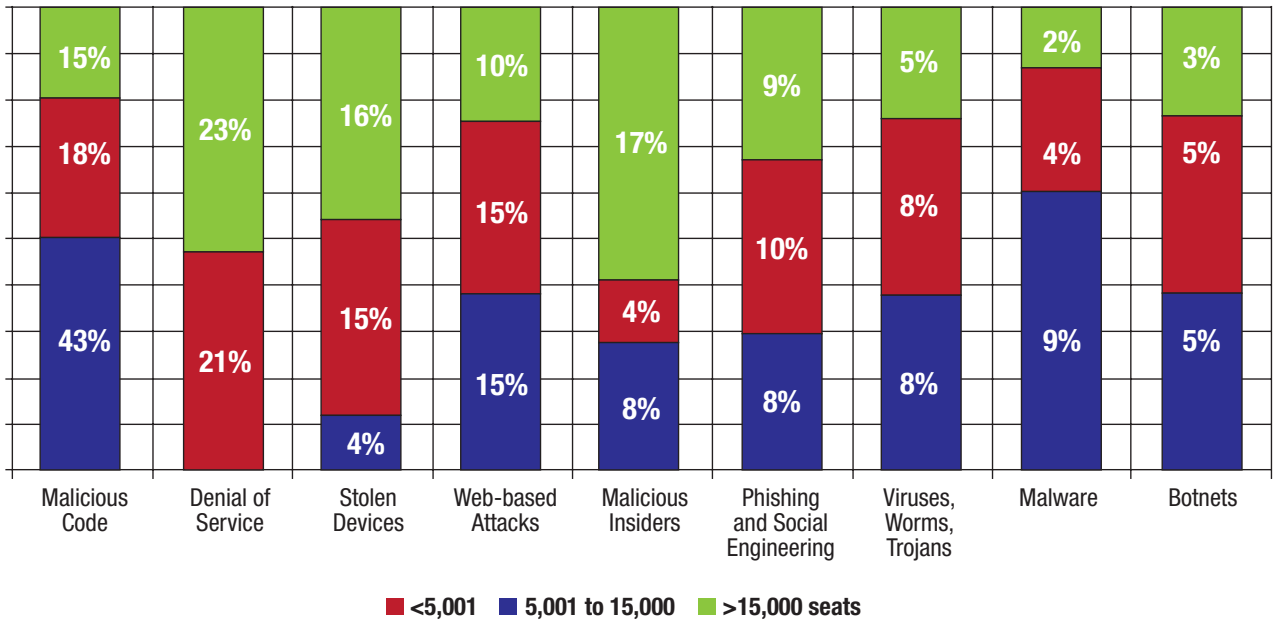
Figure 2 provides a comparison of small, medium-sized and large organizations and "reveals that the cost mix for specific cyberattacks varies by organizational size. Specifically, small organizations (less than 5,001 seats) experience a higher proportion of cybercrime costs relating to malicious code and malware. In contrast, large organizations (greater than 15,000 seats) experience a higher proportion of costs relating to malicious insiders, stolen or hijacked devices, and denial of service."[15] SMEs are faced with considerable resource constraints, but there are different ways to secure their networks and information.

> "The cost of inaction far outweighs the upfront cost of cybersecurity."

SMEs are beginning to address cybersecurity and put safeguards and defensive countermeasures in place. For some businesses, their delayed action and hesitant response is too little too late. The cost of cybersecurity can provide a bit of "sticker shock" for SME executives and decision makers. But the cost

Figure 2—The Cost Mix of Attacks by Organizational Size

Size measured according to the number of enterprise seats within the participating organizations.



Source: Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies," August 2011, *www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf*

of inaction far outweighs the upfront cost of cybersecurity. The threats are real, and if an SME has not been hacked, chances are high that it will be soon. If an SME continues to think that it is too small to be important, it must be reminded to consider whether the information it has might cause damage to a customer or to a business partner. What is the potential impact of that information being stolen, being hijacked or being posted on the Internet for everyone to see? Will the damage be something the SME can recover from, or will the damage cause it to file for bankruptcy? The longer SMEs take to implement the appropriate security countermeasures, the more risk to which they are exposed. The only real option SMEs have left is to treat risk by mitigating the threat and achieving an acceptable amount of residual risk.

ENDNOTES

[1] This term refers to the western US during the gold rush of the second half of the 19th century.

[2] Ponemon Institute, "Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies," August 2011, *www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf*

[3] Prince, Daniel; "Event Reveals New Insights Into Businesses' Cyber Security Concerns," School of Computing and Communications, Lancaster Unversity, 29 September 2011, *www.scc.lancs.ac.uk/info/news/001214/*

[4] Moscaritolo, Angela; "SME Security: Sizable Differences," IT Security News and Security Product Reviews, *SC Magazine*, 1 May 2009, *www.scmagazineus.com/sme-security-sizable-differences/article/136042/*

[5] Ponemon Institute, "First Annual Cost of Cyber Crime Study," ArcSight, July 2010, *www.riskandinsurancechalkboard.com, www.riskandinsurancechalkboard.com/uploads/file/Ponemon%20Study(1).pdf*

[6] Naraine, Ryan; Emil Protalinski; Dancho Danchev; "Stuxnet Attackers Used 4 Windows Zero-day Exploits," ZDNet, 14 September 2010, *www.zdnet.com/blog/security/stuxnet-attackers-used-4-windows-zero-day-exploits/7347*

[7] McDowell, Mindi; "US-CERT Cyber Security Tip ST06-001—Understanding Hidden Threats: Rootkits and Botnets," US Computer Emergency Readiness Team (US-CERT), 24 August 2011, w*ww.us-cert.gov/cas/tips/ST06-001.html*

[8] *Ibid*.

[9] Cisco Systems Inc., "Botnets: The New Threat Landscape White Paper," 23 October 2011, *www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns441/networking_solutions_whitepaper0900aecd8072a537.html*

[10] *Op cit*, Ponemon Institute, August 2011

[11] The agent.btz malware was not specifically written to target the US Department of Defense (DoD), but three years after the initial breach occurred in 2008, the US DoD is still combatting the effects of agent.btz and its newer variants. Stewart, Phil; Jim Wolf; "Agent.btz Worm Won't Die After 2008 Attack on Military," Breaking News and Opinion, *The Huffington Post*, 17 June 2011, *www.huffingtonpost.com/2011/06/17/agentbtz-worm-attack-military_n_878880.html*

[12] Parrish, Karen; "Cyber Threat Grows More Destructive, Lynn Says," US Department of Defense, 15 July 2011, *www.defense.gov/news/newsarticle.aspx?id=64690*

[13] Mandiant, "MANDIANT: Intelligent Information Security: Advanced Persistent Threat," 25 October 2011, *www.mandiant.com/services/advanced_persistent_threat*

[14] Datko, Karen; "9 Ways to Avoid Cybercrime," *MSN Money*, 14 September 2011, *http://money.msn.com/saving-money-tips/post.aspx?post=12ad8244-9ffe-434f-8795-a3668b5e1a35*

[15] *Op cit*, Ponemon Institute, August 2011

[16] Net-security.org, "40% of SMBs Suffered Breach Due to Unsafe Web Surfing," Help Net Security, 12 October 2011, *www.net-security.org/secworld.php?id=11773*

Using Scenario Analysis for Managing Technology Risk

Mukul Pareek, CISA, ACA, AICWA, PRM, is a risk professional based in New York, USA. He has more than 20 years of audit and risk experience in industry and financial services. He is copublisher of the Index of Cyber Security, *www.CyberSecurityIndex.org.* He can be reached at *mp@pareek.org.*

In the world of market and credit risk, scenario analysis is used as a part of stress testing. Stress testing is mandated by national regulators and central banks, and takes the form of asking financial institutions to consider the effect of adverse scenarios on their capital and solvency. Scenarios include historical events, such as market crashes and debt defaults, and hypothetical scenarios, such as larger-than-expected moves in interest rates, housing prices or foreign exchange rates.

In the world of operational risk, scenario analysis is used in combination with the loss distribution approach to estimate operational risk capital under the Basel framework.[1]

For technology risk managers, scenario analysis can be a useful tool to identify, understand and articulate the technology risks faced by their organizations. Taken a step further, it can also be used as a tool to quantify and express a technology-value-at-risk number by expressing future losses in the form of a loss distribution.

In essence, scenario analysis consists of identifying future "what-can-go-wrong" situations that can cause a loss to an enterprise. This is something most technology risk managers already do as part of their daily task of explaining controls to business managers (e.g., when explaining risks or audit issues or when requesting new investments in security). What scenario analysis allows us to do is to consciously understand what adverse events can occur, explain how controls prevent (or, in some cases, are unlikely to prevent) unfavorable outcomes and explain how bad circumstances can get within a reasonable range of probability.

SCENARIO ANALYSIS AND THE TECHNOLOGY RISK MANAGER

There are a number of reasons why technology risk managers and analysts need to consider scenario analysis as part of their risk management tool kit:

- **Risk and control comprehensibility**—Scenarios put controls in the context of real-life situations that profit-and-loss (P&L) managers can comprehend. Scenario analysis helps create conversations that are in plain business language, as opposed to discussions about arcane control frameworks. Scenarios transform the discussion from, for example, talking about the control benefits of an identity management system to a discussion about business data that could be stolen by a competitor.
- **Completeness of scope**—If scenarios are comprehensive and cover the risk universe against which the technology risk function provides protection, they become a useful tool for a coherent explanation of the value of the technology risk function to the enterprise. They also help set boundaries for what the function does and protects against, and set expectations for senior management.
- **Response preparedness**—Scenarios can help enterprises plan for how to react in the event that the scenario transpires.
- **Identification of risk drivers**—When constructed methodically, scenarios can help isolate the drivers of risk, allowing for focused action.
- **Control effectiveness**—The identification of scenarios necessarily involves a consideration of the controls in place to prevent them from occurring, which allows a qualitative assessment of the effectiveness of controls themselves. Scenarios help us understand how controls interact with and reinforce each other.

At its essence, scenario analysis is not all that different from risk analysis, with the notable difference being that multiple individual risks are required to combine together to create a comprehensive and plausible scenario. A scenario follows in the tradition of storytelling, whereas enumerating risk at a granular level is more of an exercise for the risk- and control-literate risk manager.

HISTORICAL VS. HYPOTHETICAL SCENARIOS

Broadly, there are two ways to identify scenarios: first, through an analysis of historical events, and second, through the construction of hypothetical yet plausible adverse events that may reasonably occur. Taken together, scenarios should be comprehensive and updated from time to time.

> "Scenarios should be comprehensive and updated from time to time."

Scenarios based on historical events may include real events that happened to the organization or its peers (e.g., a large compromise of its billing systems revealing sensitive personal information). Generating hypothetical scenarios requires judgment, skill and a good understanding of the business. Hypothetical scenarios are important because they allow for the completion of the gaps left by historical events.

Scenarios based on historical experience need no explanation as to their plausibility. Hypothetical scenarios can be made plausible by seeking input from business managers who should play an active role in identifying them.

DISTINGUISHING BETWEEN EXPECTED AND UNEXPECTED LOSSES

Expected losses are losses that are considered part of the cost of doing business, and arise year after year. They are characterized by a high frequency of occurrence and a low impact. An example would be average annual credit card fraud events experienced by a bank. Up to a point, these are just ordinary losses that are absorbed as part of the cost of doing business. The product is priced to include the occurrence of expected losses. These are governed by the law of large numbers. Unexpected losses include events such as a large-scale data breach.

Scenario analysis should not cover expected losses. Scenarios should be directed toward high-severity, exceptional and infrequent events. The nature of the technology risk universe means it rarely has to deal with expected losses; nonetheless, this is an important point to make so that technology risk managers do not become too engrossed with the details of ongoing transactional events.

WHAT SHOULD A SCENARIO INCLUDE?

At the very minimum, a scenario should include:

- **The situations**—An explanation of the sequence of events that leads to an adverse outcome. These may be industry- and organization-specific, but must include things such as:
  - BCP events
  - External attacks by hackers, competitors or nation states
  - Malicious insiders stealing information
  - Accidental release of confidential information
  - Vendors and third parties mishandling data
- **The outcomes**—Clearly identified outcomes that are unfavorable to the organization and are a result of the event. An event may have multiple outcomes. For example, the same scenario may result in the loss of revenue, legal costs and regulatory fines. Each outcome should be explicitly laid out, describing its impact.
- **Controls in place**—Controls work as separate lines of defense—at times in a sequential way, and at other times interacting with each other—and help prevent the occurrence of the adverse event. Often, the correct operation of just one control may provide adequate protection or mitigation. If the controls operate independently of each other, as they often do, the combined probability of all of them failing simultaneously tends to be significantly lower than the probability of failure of any one of them. An attacker, for example, who is trying to get into a network may first have the intrusion detection/prevention system (IDS/IPS) to deal with, which may have a failure rate of 10 percent. But even after the attacker gets in and tries to install a rogue program, there may be protection provided by the antimalware protection, operating at a failure rate of 10 percent, for example. The probability of both controls failing together will be only 1 percent, showing how multiple controls acting together may create a 10-fold improvement in the security, even though on their own each

may be a pretty coarse control. A third control, e.g., restricting users from administrative privileges, may further reduce the effectiveness of the attack to extremely unlikely.

- **Frequency of occurrence**—The frequency, or likelihood, of the scenario actually being realized should be a part of the scenario analysis, and is best estimated during a discussion with the business managers. What the technology risk manager is truly interested in is a probability, but the question is better framed in terms of how likely the scenario is over a long enough period (e.g., 10 years). This question is best answered by business managers, in partnership with the technology risk manager. If the answer is that the scenario might materialize once over 10 years, the probability of its occurrence each year is 10 percent.
- **Severity of the outcomes**—Much in the same way as frequency, the severity of each of the adverse outcomes should be estimated separately. Now what does severity mean? Is it the worst-case loss, or the most likely or median loss? In some cases, the absolute worst case may not be knowable, or may mean something as catastrophic as the end-of-game for the organization. Such scenarios should be modeled separately from scenarios that are expected to occur over a long-term period.

  In some cases, estimating the worst case may be a meaningless exercise, as the technology risk team may not have the mandate to manage for the truly catastrophic. While this may sound surprising, it is generally not expected that technology risk management provides for events such as nuclear attacks or meteor strikes.

  The technology risk analyst must strive to get at least two data points for severity—one at the 50th percentile and another at a higher percentile, such as the 90th. The question for the 50th percentile is easily posed as: What is the median expected loss level if the scenario in question were to materialize, i.e., the loss right in the middle? For the 90th percentile, it may be better to pose the question: Of all losses possible, what would be the loss if the enterprise were in the top 10 percent of the category of such losses? Precision is not desired nor should it be pursued, as it is neither achievable nor meaningful.

ADJUSTING FOR BIAS

People have a generally optimistic bias toward their perception of their own competence and good fortune. This bias is likely to be reflected in any scenario-analysis session that a technology risk manager organizes—in the form of lower expected frequency of occurrence or severity.

One possible way to correct for this may be for the risk analyst moderating the scenario analysis not to focus on the enterprise, but to talk about similar organizations or competitors (i.e., how likely is such a scenario at the top four or five competitors, and if they were to suffer a loss, how much is it likely to be?). Any internal loss data or anecdotes of actual occurrences may help further align perceptions to reality.

COMPLETENESS OF SCENARIOS—MAPPING THE ENTIRE RISK UNIVERSE

Scenarios should cover the range of known technology risks that the business is likely to face. Documented controls should address one or more of these scenarios, and if the technology risk managers find controls that do not address a scenario, then either the universe of scenarios is incomplete or the control is redundant. Under each of the broad categories, such as process and workflow errors, information leakage events, business continuity events and external attacks (these may differ across organizations), there would be a number of scenarios.

Compiling a list of acceptable risk scenarios including all the attributes described previously is not a trivial task and requires sponsorship, cooperation from P&L managers and an understanding of the business by the technology risk manager. Scenario building may be carried out in a conference room setting with the technology risk manager or analyst leading the agenda.

In many cases, the scenario-analysis exercise is a valuable end itself. In some cases, the risk manager may choose to perform additional quantitative analysis by calculating a technology-value-at-risk number, as detailed in the next section.

COMPUTING TECHNOLOGY VALUE AT RISK

Once scenarios have been identified, together with their expected frequency and severity, as explained in the previous section, these estimates can be converted to estimates of losses at different confidence intervals, similar to value at risk. We will call it the technology value at risk to distinguish it from the more common measure of financial risk.

The steps to determine a technology-value-at-risk number are:

1. **Assume a distribution for the frequency and severity estimates.** Generally, the Poisson distribution for frequency and the lognormal distribution for severity are reasonable

choices. Using a distributional approach recognizes that both frequency and severity are not single-point estimates, but can cover a wide range of possible values. This makes the calculation process more acceptable in a management discussion, as the technology risk analyst is not claiming certainty in any calculations.

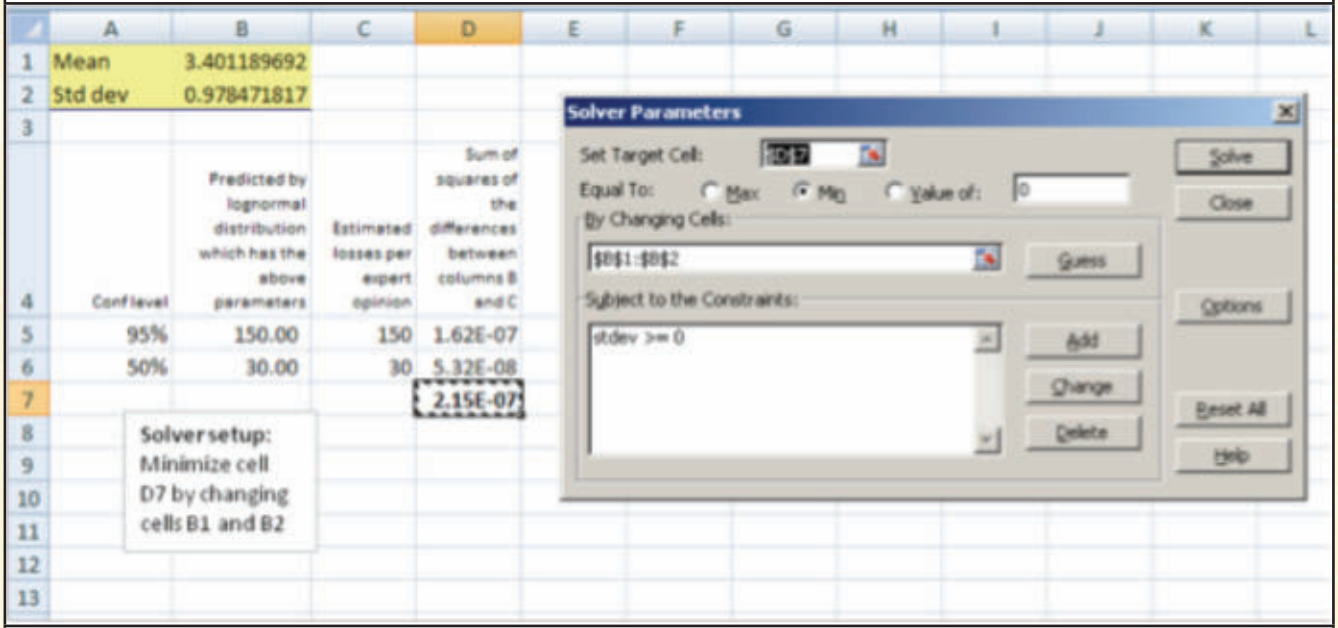
The remainder of this article will proceed with these distributional choices (i.e., Poisson and lognormal), though the overall process would be quite similar even if other distributions were selected.

For the frequency distribution modeled by the Poisson distribution, there is only a single parameter, the mean, that is required to build the distribution. The mean was estimated as part of the scenario analysis exercise.
For the severity distribution modeled by a lognormal distribution, two parameters are needed to describe the complete distribution: the mean and the standard deviation. Estimating these will require the availability of two (or more) data points for the losses that were estimated as part of the scenario analysis exercise—the most likely loss and the loss at the 90th (or another) percentile. Using the method of least squares, the two-point estimates can be used to estimate the best fitting mean and standard deviation for the severity distribution. This can be done in Excel, using Solver[2] (see **figure 1**), or using a mathematical package such as R[3] (see **figure 2**).

2. **Build the loss distribution.** The loss distribution is a product of the frequency and severity distributions, much in the same way as loss equals frequency multiplied by severity. While there is no way to formulaically multiply the Poisson (for the frequency) and the lognormal (for the severity) distribution, one can use a Monte Carlo simulation[4] to obtain the loss distribution. This requires picking a random number from each of the frequency and severity distributions and multiplying them to get a single data point representing a loss. This process is then repeated thousands of times to get enough data points to produce a loss distribution.

Figure 1—Practical Modeling Using Excel

Step 1: Determine distributional parameters for the lognormal distribution using ordinary least squares.
In Excel, the mean and standard deviation for the lognormal distribution can be obtained using the Solver add-in. An illustrative example appears here.



Step 2: Use Monte Carlo simulations after distribution parameters have been estimated.
Random numbers from both the Poisson and lognormal distributions to simulate frequency and severity may be generated in Excel using the Analysis Toolpak, a standard Excel add-in. The data points for the loss distribution are obtained by multiplying severity with frequency. The technology value at risk can then be calculated at the desired confidence level, e.g., at the 99th percentile the loss will be =PERCENTILE(data_range_loss_column,0.99).

3. **Calculate the technology-value-at-risk number for the scenario.** Once the loss distribution has been obtained as a large set of data points, the technology value at risk for the particular scenario can be determined by calculating the quantiles in which one is interested. For example, if one wishes to calculate the loss at the 99th percentile, one would look at the loss level below which 99 percent of all losses lie.
4. **Aggregate the technology value at risk.** As an additional step, an aggregate technology-value-at-risk number that includes all the scenarios may also be calculated by doing a Monte Carlo simulation for all the scenarios simultaneously. This is assuming that the loss events are independent and not correlated.

These steps can be performed in Excel, or in a mathematical package such as R. While Excel is a great environment for prototyping and solving less-complex problems, R is more suitable to heavy-duty work. The decision of which to use would depend upon how widely and repeatedly the technology risk manager needs to use the risk model, and available skill sets.

To summarize, the technology-value-at-risk calculation includes the following steps, as visualized in **figure 3**:

1. Identify scenarios.
2. For each scenario:
   - Determine frequency as a single-point estimate. Use this estimate as the mean for a Poisson distribution that models the likelihood of the scenario occurring.
   - Determine severity as a point estimate at two quantiles or more. Using these data points, calculate the mean and standard deviation of the closest lognormal distribution. This lognormal distribution now defines our severity distribution.
   - Simulate the loss distribution, picking one point each simultaneously from both the frequency and severity distributions
3. For each scenario, calculate the appropriate percentile (usually the 95th or 99th) as the technology value at risk.

Figure 2—Practical Modeling Using R

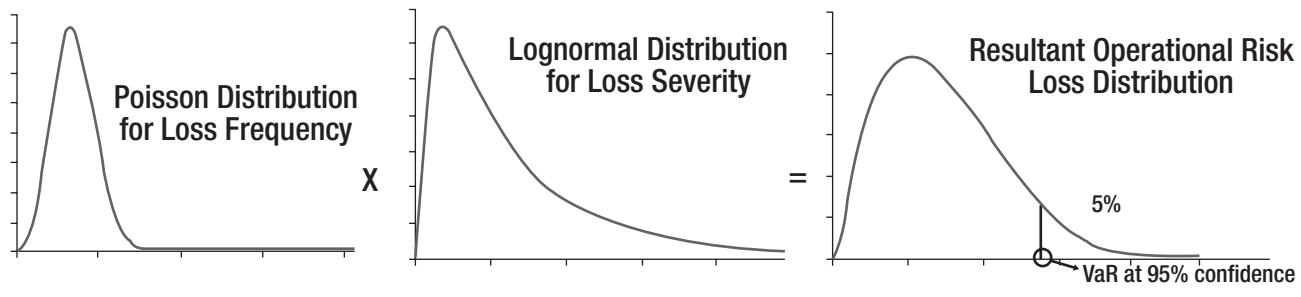
In R, the steps can be performed using the following commands. The initial variables will need to be set by the risk analyst before running these commands:

```
#Initial variables
simulations <- 1000000
lambda <- 0.1
exp_est1 <- 10
exp_est2 <- 80
conf1 <- 0.5
conf2 <- 0.95

#Two estimates for Scenario 1 placed in dataframe s1
s1 <- data.frame(conf=c(conf1,conf2), expert_est=c(exp_est1,exp_est2))
#Setting a function up to calculate the sum of squares
ss <- function(x) {
 x1 <- x[1]
 x2 <- x[2]
 sum((qlnorm(s1$conf,x1,x2) - s1$expert_est)^2)
 }

#Minimizing the sum of squares function a
pp <- optim(c(0,1),ss)
s1mean <- pp[[1]][1]
s1stdev <- pp[[1]][2]
#Calculating the loss distribution function
ld <- rlnorm(simulations,s1mean,s1stdev)*rpois(simulations,lambda)
qt <- quantile(ld, probs=c(0.95, 0.99, 0.995, 0.999))
#Publish everything we calculated thus far
s1
s1mean
s1stdev
ss(c(s1mean,s1stdev))
qt
```

Figure 3—Modeling Operational Risk Losses



4. To calculate an aggregate technology value at risk that includes all scenarios, simulate a loss from all scenarios simultaneously.

CONCLUSION

Scenario analysis, even if carried out without any additional quantification, can be a useful exercise to bring together technology risk practitioners and the business that they serve. It can generate the right conversations and engagement and focus management on issues that truly matter to the organization. It can also help evaluate controls in the context of real business situations, and help identify controls that can be safely dropped without an inordinate increase in the risk. If scenarios are converted to a technology-value-at-risk number, the enterprise gets the additional benefits of being able to evaluate the monetary impact of adding or removing controls.

Yet the approach is not without limitations. Real life is complex, and adverse outcomes inevitably compound. Additionally, the impact from scenarios often extends beyond technology. It is difficult to successfully model strategic, legal and reputational risk areas that often accompany technology risk events. A modeler would need to bear these limitations in mind as part of any scenario analysis.

ENDNOTES

[1] Basel Committee on Banking Supervision, *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework—Comprehensive Version*, *www.bcbs.org*

[2] Solver is a native Microsoft Excel add-in that allows complex problems to be solved using optimization routines. It may be enabled under the Add-Ins menu in Excel.

[3] R is a popular open-source software used for mathematical and statistical analysis. It can be downloaded from *cran.r-project.org*.

[4] Monte Carlo simulations are a statistical method where data points are obtained by repeated random sampling. This allows for simulating complex systems and interactions that may be difficult to express analytically (e.g., as a clean formula).

Preparing for HTML5 Capabilities and Threats

Hongwen Zhang is president and chief executive officer (CEO) of Wedge Networks, an innovative provider of remediation-based deep content inspection for high-performance, network-based web security. Zhang has more than two decades of high-tech leadership experience and is the coinventor and holder of several patents in the area of computing and networking.

The transition to HTML5 provides organizations with a rich, responsive and standardized web application environment that makes it possible to have improved mobile access and dynamic cloud-based applications. Leading organizations and browsers, such as Google, Facebook, YouTube and Skype, have already begun to support the move to HTML5. This movement is revolutionizing the underlying structure of the web and how the content is processed and delivered. HTML5 presents a new portfolio of functionalities that includes richer media, increased online responsiveness and offline operation. However, with so many new features and protocols come new potential threats on a larger attack surface. Specifically, organizations should be advised of the new WebSocket protocol and must understand what security holes it opens up in traditional network protection. This article highlights the key risk factors of HTML5 to bring awareness to business management, information security practitioners, IT professionals, information systems (IS) professionals, audit and assurance professionals, and web developers.

HTML5 RISK FACTORS

HTML5 is likely to replace Adobe Flash and Java Applets as the new industry standard for content delivery. With the expansion of the Internet's reach and versatility come new security challenges for which existing security solutions are unprepared.

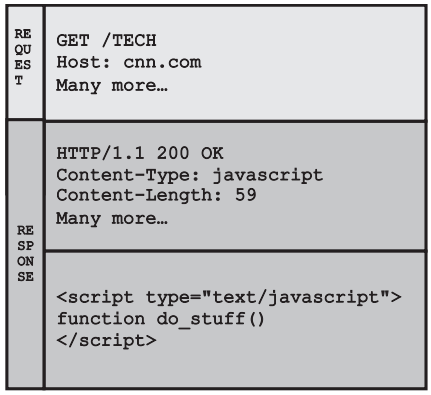
The introduction of HTML5 brings unique risk factors, malware channels, and vehicles for delivery and infections, including:

- **Cross-site delivery/communication**—Cross-site resource sharing is dropping the incumbent "same origin policy," increasing the reach of traditional cross-site scripting attacks among domains.
- **Javascript capabilities**—Powerful client scripting capabilities support threading, asynchronous input/output (I/O), local databases, geolocation and local resource access, resulting in new vectors for botnets, data leakage and geoprivacy issues.
- **WebSocket protocol**—The introduction of a two-way communication protocol—HTML5/WebSocket—makes this version 5 of the HTML specification truly revolutionary. The new version brings enormous benefits that will make the HTML5-fueled Internet more usable and more friendly.

HTML5 WEBSOCKET BENEFITS AND SECURITY RISKS

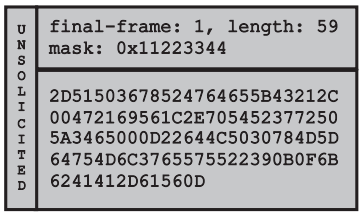
HTML5 WebSocket is a communication protocol that happens to use the same network port used by the familiar HTTP. Unlike HTTP, WebSocket is a full duplex, asynchronous communication protocol for delivering interactive web content. According to WebSocket specifications,[1] this asynchronous ability allows applications such as Stock Ticker to be 500 times more efficient when delivered in HTML5/WebSocket. With the new Internet being defined by the large amount of mobile devices generating tremendous dynamic content that is piped back and forth to gigantic cloud centers, WebSocket will be an enabling tool for developing user-friendly applications.

Figure 1—HTTP Request/Response



Source: Wireshark capture of an HTTP session

Figure 2—WebSocket Message



Source: Wireshark capture of WebSocket session

WebSocket achieves its efficiency by using several clever tricks. Unfortunately, these tricks also invalidate some key assumptions of today's conventional network defense system:

- WebSocket overrides HTTP port. This makes firewalls unable to differentiate WebSocket from HTTP traffic.
- WebSocket is asynchronous, not a request/response-based protocol, confusing web proxies.
- WebSocket payload does not contain URL or application headers (see **figure 1** and **figure 2**). This makes reputation-based defenses helpless.
- WebSocket payload is masked (see **figure 2**). This introduces big obstacles for packet-inspection-based network security solutions.

A security solution capable of addressing HTML5 content must be able to tackle new content packaging, transmission protocols and the rising number of outlets used to deliver malware. Without a network protection conscious of HTML5 WebSocket content, an organization is susceptible to malicious codes transmitted through this channel. According to Forrester Research, "Firms are using more consumer-style web applications…with 84 percent of firms increasing their use of web applications."[2]

Organizations must take back control of the web infrastructure with a scalable, real-time solution that provides information-scanning techniques and enables optimal network performance.

RESEARCH APPROPRIATE SECURITY SOLUTIONS

In addition to existing best practices for web security, such as better coding of web pages, vulnerability management and timely patching of IT assets, organizations must implement a network security solution that is capable of deep content inspection (DCI) in order to preserve the benefits that HTML5 offers. DCI scans and understands the intent of web traffic, from simple coded threats to advanced malware hidden in volumes of data. A comprehensive DCI solution scans through content that is packed in both existing and new standards in the network, applying advanced threat signature matching and heuristic threat analysis to detect noncompliant content and stop malicious content from sneaking in or confidential information from leaking out, thus significantly lowering the end user's risk. As a result, regardless of where end users are and what they click on, their devices of choice are completely secure.

For an organization, the most important and convenient feature of HTML5 is the WebSocket payload. WebSocket allows organizations to transmit data for any application with any payload without a well-formed URL or HTTP headers. Although convenient, WebSocket also creates a new delivery route for malware. With the adoption of DCI solutions to the WebSocket payload, users are protected against malicious attacks. The optimal security solution extracts, scans and stops threats found in WebSocket protocols, blocking the transmission of data for any application.

CONCLUSION

Compared with previous versions, HTML5 is a safer and more effective tool for delivering today's rich web content; however, it also introduces several security risk factors. Organizations need to understand these risk factors and deploy effective tools that scan and understand the intent of all web traffic, regardless of protocol. This ensures that content packed into both existing and new standards, with an emphasis on the increased two-way concurrent traffic found in HTML5, will be understood and that security services can be applied to remediate against any threats.

To maintain network security without disabling the many improvements that HTML5 brings, organizations must adopt deep content inspection to stop the harmful code from infecting their devices and servers and to stop confidential information from being stolen.

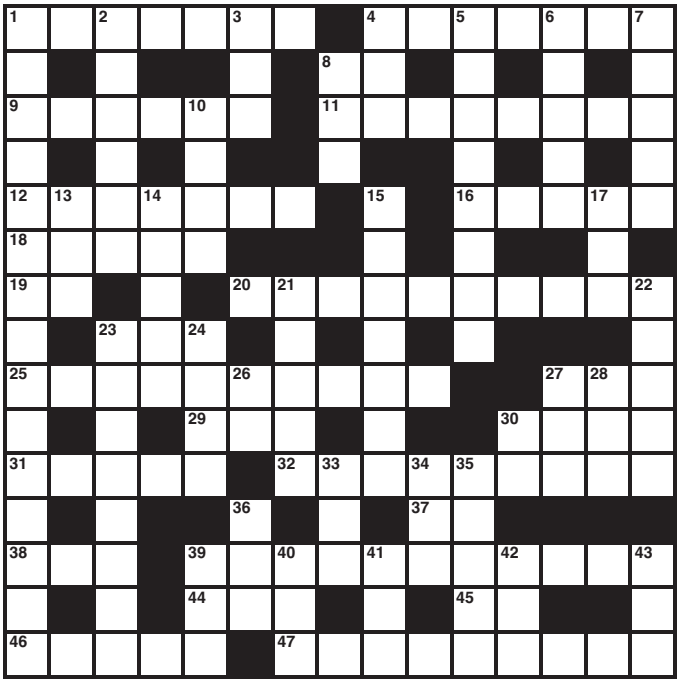
ENDNOTES

[1] WebSocket, *http://www.websocket.org/index.html*

[2] Forrester Research Blogs, "The Consumerization of IT Proceeds Unevenly, From Growth In Tablets To Anemic BYOPC Adoption," *http://blogs.forrester.com/frank_gillett/11-03-24-the_consumerization_of_it_proceeds_unevenly_from_growth_in_tablets_to_anemic_byopc_adoption*

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS
1. Infamous worm
4. Malware intended to disrupt global Internet connections (2 words)
8. Blood group
9. Internet actions that are trackable and used in marketing
11. Responsibility of 4 down
12. Unvarying procedure
16. Storage device
18. Inactive
19. Tellurium symbol
20. Apply maximum concentration and effort toward a project or task (3 words)
23. Photo
25. The P in IDPS
27. Automated program
29. Less than normal
30. ____ item
31. Add up
32. Brings into the best operating state
37. Manner indicated
38. Center of activity
39. New technology, _____ encryption
44. "___ got it!"
45. Battery size
46. Budgeted amount
47. Fail, as a company (3 words)

DOWN
1. Operating system protections (2 words)
2. Specific to one person or thing
3. Type of file
4. Position that has the "keys to the kingdom"
5. Photographic record
6. The Oracle's location
7. Make inoperable
8. Build (on)
10. Come together
13. Unified
14. Distinguishing characteristic
15. Get exhausted due to long-term stress (2 words)
17. Tech exec, for short
21. Amazon's cloud offering
22. Lotus ____
23. Transferable
24. Spreadsheet section
26. Firm, briefly
27. ____ dev
28. "We're number ___!"
30. 51 in Roman times
33. Expert
34. Standards organization
35. Relating to ethical responsibilities
36. Educational Internet ending
39. Concealed
40. Memory unit, for short
41. Flash ____
42. Pay___
43. Limit

(Answers on page 54)

HelpSource Q&A

We invite you to send your information systems audit, control and security questions to:
HelpSource Q&A
bgansub@yahoo.com or
publication@isaca.org

Fax to: +1.847.253.1443
Or mail to:
ISACA Journal
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Gan Subramaniam, CISA, CISM, CCNA, CCSA, CIA, CISSP, ISO 27001 LA, SSCP, is the global IT security lead for a management consulting, technology services and outsourcing company's global delivery network. Previously, he served as head of IT security group compliance and monitoring at a Big Four professional services firm. With more than 16 years of experience in IT development, IS audit and information security, Subramaniam's previous work includes heading the information security and risk functions at a top UK-based business process owner (BPO). His previous employers include Ernst & Young, UK, Thomas Cook (India), and Hindustan Petroleum Corp., India. As an international conference speaker, he has chaired and spoken at a number of conferences around the world.

Q I am trying to audit an access control management system. As an auditor, what are the subcontrols that I must consider and evaluate to assess the effectiveness of the system and the appropriateness of the access privileges granted?

A ISO 27001:2005, the international standard on information security, stipulates this list of access control requirements:

- An inventory of systems to which access is required must exist. These systems must ideally be classified in terms of confidentiality and the sensitivity of the information held or processed within the particular system/application.
- Every system must have a designated information owner who is responsible for making decisions on access. Of course, the owner can delegate the work to someone else.
- The data residing inside the system must be classified as per the enterprise's data classification standard, if one exists.

Access control policies also dictate the authentication modes, which can be single-factor or dual-factor authentication. The nature of information again determines the quantum of factors to be used for authentication. In some extreme cases, more than two may be required.

Access rights must be provided to a specific set of individuals who require access, not to one and all. Designated approvers should approve the granting of such rights. The type of access required, whether ordinary or privileged, must also be identified and limited to types of access (e.g., read or write). Privileged users can do more damage to the system (intentionally or unintentionally), given their unrestricted and unfettered access rights.

A periodic review of access rights must take place. This review must be done by a team or must function outside of IT operations to ensure independence. The review should identify those individuals or groups that have unnecessary access. The results of the review must be provided to key stakeholders, in particular to the owners of the information systems or data.

It is a common pitfall that vendors enjoy privileges equal to employees on systems when they should not. The responsibilities and role of the vendors' representatives must be clearly defined in their contracts. Any contract silent on these issues is inadequate. It is also important to ensure that the vendors' employees' access is discontinued after their termination of employment; this requires properly defined mechanisms to disable access of vendors' staff. The same principle applies for the organisation's own employees; exit management processes must clearly define the roles and responsibilities of stakeholders and access control teams.

Logs must be generated on inappropriate access attempts. In particular, unsuccessful logins must be logged, tracked and reviewed. Action must be taken when such attempts are combined with malicious intent.

Access controls become an issue when generic identifiers (which can indicate the potential sharing of passwords) are allowed to access systems. As a result, the identifiers cannot be tagged to named individuals. Password sharing is one of the worst scenarios in access control because accountability is lost.

Whether we talk about legacy systems or the modern cloud, all of the above principles apply. They are independent of any technology. They apply to user accounts in applications and in operating systems. It is very important that trails exist for granting and disabling access. The trails can be system-based or paper-based, depending on the firm. Some industry regulations require the archiving of access control documents.

Above all, with all the sophisticated access control mechanisms in place, the sharing of passwords amongst users negates the very purpose of access control systems. Security awareness, as always, is a must in order for an enterprise to have an effective access control system.

Whilst auditors may not be able to question the need when it is determined by the business, it is essential that proper rationale be available for granting access.

CPE Quiz

Prepared by Kamal Khan, CISA, CISSP, CITP, MBCS

Take the quiz online:

Quiz #145

Based on Volume 4, 2012—Data Analytics/Mining

Value—1 Hour of CISA/CISM/CGEIT/CRISC Continuing Professional Education (CPE) Credit

TRUE OR FALSE

BELLEHUMEUR ARTICLE

1. Documentation enables organizations to mitigate their risk across several strategic areas, including loss of intellectual capital, data and IT operations, clarity and momentum.

2. With documentation, there appear to be four distinct buckets into which IT departments tend to fall: no documentation, little and sporadic documentation, average documentation, and overdocumentation.

3. IT departments do not know *how* to document. Documentation does not mean writing everything down. It is actually a strategic process that consists of capturing, structuring, presenting, communicating and storing written information. IT professionals tend to struggle with structuring, presenting and communicating.

4. Moving the team and department to the optimized documentation bucket is a three-step process consisting of adopting a strategic process, having the right people, and building a culture of accountability and best practices around effective documentation.

GOLDBERG ARTICLE

5. The Institute of Internal Auditors (IIA) standards regarding risk assessment state:
   2020.A3: The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

   2040.A5: The auditor must identify and consider the expectations of senior management, the board and other stakeholders for internal audit opinions and other conclusions.

6. Internal audit can assist management and the board/audit committee in the ERM process by monitoring, examining, recommending improvements, evaluating and reporting.

7. Without performing a risk assessment, IA is at risk of losing its relevance. IA has a role in helping the organization understand and prepare for the associated risk implications of entering new markets, leveraging new technologies (e.g., social media, cloud) or expanding its business portfolio organically or inorganically.

8. Many internal auditors perform the annual risk assessment and carry out work based on the actual risk to the organization rather than reproduce the work from the prior year or budget hours based on man-hours available.

9. Many organizations, through audit activities, identify and evaluate companywide risk levels by examining trends and comparisons within a single process or system throughout the year.

RAVAL ARTICLE

10. Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

11. The accountability for the creation of business value (BV) is easier to identify than the accountability for IT resources and processes.

12. Roughly, COBIT leans toward the resources and processes focus and Val IT leans toward the BV focus.

HAMIDOVICH ARTICLE

13. In most jurisdictions and organizations, digital evidence is governed by three fundamental principles: relevance, reliability and confidentiality, and all three are important for the digital evidence to be admissible in a court of law, as stated in ISO/IEC 13403789.

14. *Code of Practice for the Implementation of BS 10008* is structured according to a set of five principles of good practice, including understanding the legal issues and executing duty-of-care responsibilities.

ESPIN ARTICLE

15. A hash is the result of processing a block of data, such as a password, through a procedure or algorithm that returns a fixed number of characters.

16. To address the risk of inappropriate access to the SAP systems, consideration should be given to identifying and securing sensitive data and performing a comprehensive SAP security assessment.

ISACA Journal
CPE Quiz
Based on Volume 4, 2012—Data Analytics/Mining

Quiz #145 Answer Form

(Please print or type)

Name _____

_____

Address_____

_____

_____

CISA, CISM, CGEIT or CRISC #_____

Quiz #145

True or False

BELLEHUMEUR ARTICLE

1. _____
2. _____
3. _____
4. _____

GOLDBERG ARTICLE

5. _____
6. _____
7. _____
8. _____
9. _____

RAVAL ARTICLE

10. _____
11. _____
12. _____

HAMIDOVICH ARTICLE

13. _____
14. _____

ESPIN ARTICLE

15. _____
16. _____

Please confirm with other designation-granting professional bodies for their CPE qualification acceptance criteria. Quizzes may be submitted for grading only by current *Journal* subscribers. An electronic version of the quiz is available at *www.isaca.org/cpequiz*; it is graded online and is available to all interested parties.

If choosing to submit using this print copy, please email, fax or mail your answers for grading. Return your answers and contact information by email to *info@isaca.org* or by fax to +1.847.253.1443. If you prefer to mail your quiz, in the US, send your CPE Quiz along with a stamped, self-addressed envelope, to ISACA International Headquarters, 3701 Algonquin Rd., #1010, Rolling Meadows, IL 60008 USA.

Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

You will be responsible for submitting your credit hours at year-end for CPE credits.

A passing score of 75 percent will earn one hour of CISA, CISM, CGEIT or CRISC CPE credit.

Answers—Crossword by Myles Mellor

See page 51 for the puzzle.

S	T	U	X	N	E	T	■	D	N	S	B	O	M	B
E	■	N	■	■	P	■	A	B	■	N	■	M	■	R
C	L	I	C	K	S	■	D	A	T	A	B	A	S	E
U	■	Q	■	N	■	■	D	■	■	P	■	H	■	A
R	O	U	T	I	N	E	■	B	■	S	T	A	C	K
I	N	E	R	T	■	■	■	U	■	H	■	■	I	■
T	E	■	A	■	B	E	A	R	D	O	W	N	O	N
Y	■	P	I	C	■	C	■	N	■	T	■	■	■	O
P	R	O	T	E	C	T	I	O	N	■	■	B	O	T
A	■	R	■	L	O	W	■	U	■	■	L	I	N	E
T	O	T	A	L	■	O	P	T	I	M	I	Z	E	S
C	■	A	■	■	G	■	R	■	S	O	■	■	■	■
H	U	B	■	H	O	M	O	M	O	R	P	H	I	C
E	■	L	■	I	V	E	■	O	■	A	A	■	■	A
S	P	E	N	D	■	G	O	B	E	L	L	Y	U	P

ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

The specialised nature of IT audit and assurance and the skills necessary to perform such audits require standards that apply specifically to IT audit and assurance. One of the goals of ISACA® is to advance globally applicable standards to meet its vision. The development and dissemination of the IT Audit and Assurance Standards are a cornerstone of the ISACA professional contribution to the audit and assurance community. The framework for the IT Audit and Assurance Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IT audit and assurance.
  They inform:
  - IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
  - Management and other interested parties of the profession's expectations concerning the work of practitioners
  - Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.
- **Tools and Techniques** provide examples of procedures an IT audit and assurance professional might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IT auditing work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

COBIT® is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises. It emphasises regulatory compliance, helps enterprises increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework's concepts. COBIT is intended for use by business and IT management as well as IT audit and assurance professionals; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. COBIT is available for download on the ISACA web site, *www.isaca.org/cobit*.

Links to current guidance are posted on the standards page, *www.isaca.org/standards.* **Please note that links to the standards exposure draft and questionnaire are posted at *www.isaca.org/standardexposure*.** The final updated standards are scheduled to be posted in first quarter 2013.

The titles of issued standards documents are:8

IT Audit and Assurance Standards
S1 Audit Charter Effective 1 January 2005
S2 Independence Effective 1 January 2005
S3 Professional Ethics and Standards Effective 1 January 2005
S4 Professional Competence Effective 1 January 2005
S5 Planning Effective 1 January 2005
S6 Performance of Audit Work Effective 1 January 2005
S7 Reporting Effective 1 January 2005
S8 Follow-up Activities Effective 1 January 2005
S9 Irregularities and Illegal Acts Effective 1 September 2005
S10 IT Governance Effective 1 September 2005
S11 Use of Risk Assessment in Audit Planning Effective 1 November 2005
S12 Audit Materiality Effective 1 July 2006
S13 Using the Work of Other Experts Effective 1 July 2006
S14 Audit Evidence Effective 1 July 2006
S15 IT Controls Effective 1 February 2008
S16 E-commerce Effective 1 February 2008

IT Audit and Assurance Guidelines
G1 Using the Work of Other Experts Effective 1 March 2008
G2 Audit Evidence Requirement Effective 1 May 2008
G3 Use of Computer-assisted Audit Techniques (CAATs) Effective 1 March 2008
G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008
G5 Audit Charter Effective 1 February 2008
G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008
G7 Due Professional Care Effective 1 March 2008
G8 Audit Documentation Effective 1 March 2008
G9 Audit Considerations for Irregularities Effective 1 September 2008
G10 Audit Sampling Effective 1 August 2008
G11 Effect of Pervasive IS Controls Effective 1 August 2008
G12 Organisational Relationship and Independence Effective 1 August 2008
G13 Use of Risk Assessment in Audit Planning Effective 1 August 2008
G14 Application Systems Review Effective 1 October 2008
G15 Audit Planning Revised Effective 1 Ma1 2010
G16 Effect of Third Parties on an Organisation's IT Controls Effective 1 March 2009
G17 Effect of Non-audit Role on the IS Auditor's Independence Effective 1 May 2010
G18 IT Governance Effective 1 May 2010
G19 Withdrawn 1 September 2008
G20 Reporting Effective Effective 16 September 2010
G21 Enterprise Resource Planning (ERP) Systems Review Effective 16 September 2010
G22 Business-to-consumer (B2C) E-commerce Reviews Effective 1 October 2008
G23 System Development Life Cycle (SDLC) Reviews Effective 1 August 2003
G24 Internet Banking Effective 1 August 2003
G25 Review of Virtual Private Networks Effective 1 July 2004
G26 Business Process Re-engineering (BPR) Project Reviews Effective 1 July 2004
G27 Mobile Computing Effective 1 September 2004
G28 Computer Forensics Effective 1 September 2004
G29 Post-implementation Review Effective 1 January 2005
G30 Competence Effective 1 June 2005
G31 Privacy Effective 1 June 2005
G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
G33 General Considerations for the Use of the Internet Effective 1 March 2006
G34 Responsibility, Authority and Accountability Effective 1 March 2006
G35 Follow-up Activities Effective 1 March 2006
G36 Biometric Controls Effective 1 February 2007
G37 Configuration and Release Management Effective 1 November 2007
G38 Access Controls Effective 1 February 2008
G39 IT Organisation Effective 1 May 2008
G40 Review of Security Management Practices Effective 1 October 2008
G41 Return on Security Investment (ROSI) Effective 1 May 2010
G42 Continuous Assurance Effective 1 May 2010

IT Audit and Assurance Tools and Techniques
P1 IS Risk Assessment Measurement Effective 1 July 2002
P2 Digital Signatures and Key Management Effective 1 July 2002
P3 Intrusion Detection Systems (IDS) Review Effective 1 August 2003
P4 Malicious Logic Effective 1 August 2003
P5 Control Risk Self-assessment Effective 1 August 2003
P6 Firewalls Effective 1 August 2003
P7 Irregularities and Illegal Acts Effective 1 December 2003
P8 Security Assessment—Penetration Testing and Vulnerability Analysis Effective 1 September 2004
P9 Evaluation of Management Controls Over Encryption Methodologies Effective 1 January 2005
P10 Business Application Change Control Effective 1 October 2005
P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

Standards for Information System Control Professionals Effective 1 September 1999
510 Statement of Scope
.010 Responsibility, Authority and Accountability
520 Independence
.010 Professional Independence
.020 Organisational Relationship
530 Professional Ethics and Standards
.010 Code of Professional Ethics
.020 Due Professional Care
540 Competence
.010 Skills and Knowledge
.020 Continuing Professional Education
550 Planning
.010 Control Planning
560 Performance of Work
.010 Supervision
.020 Evidence
.030 Effectiveness
570 Reporting
.010 Periodic Reporting
580 Follow-up Activities
.010 Follow-up

Code of Professional Ethics Effective 1 January 2011

Advertisers/Web Sites

Leaders and Supporters

ISACA® Journal, formerly *Information Systems Control Journal*, is published by ISACA, a nonprofit organization created for the public in 1969. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Subscription Rates:
US: one year (6 issues) $75.00
All international orders: one year (6 issues) $90.00. Remittance must be made in US funds.

ISSN 1944-1967

ISACA®
Trust in, and value from, information systems

BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

**Over 350 titles are available for sale through the ISACA® Bookstore.
This insert highlights the new ISACA research and peer-reviewed books.
See *www.isaca.org/bookstore* for the complete ISACA Bookstore listings.**

NEW BOOKS...
www.isaca.org/newbooks

Internet and Related Security

Official Certified Ethical Hacker Review Guide, 1st Edition
384 pages, 2010—**14-IT**

Member TBD | Nonmember TBD

Security Considerations for Cloud Computing
80 pages, 2012—**SCC**

Member $35.00 | Nonmember $75.00

Non-English Resources

Principios de auditoría y control de sistemas de información
310 pages, 2011—**1-TCA2**

Member $50.00 | Nonmember $60.00

New 2013 Study Aids
CISA/CISM/CGEIT/CRISC—Page S-4

FEATURED...
www.isaca.org/featuredbooks

COBIT 5 for Information Security*
CB5IS

Member $35.00 | Nonmember $175.00

WCB5IS—e-book – PDF Format

Member $35.00 | Nonmember $175.00

COBIT 5 Implementation*
CB5IG

Member $35.00 | Nonmember $150.00

IT Auditing: Using Controls to Protect Information Assets
15-MIT2

Member $70.00 | Nonmember $80.00

IT Security Metrics: A Practical Framework for Measuring Security and Protecting Data
22MSM

Member $50.00 | Nonmember $60.00

Interpretation and Application of International Standards
95WISA

Member $105.00 | Nonmember $115.00

Fraud Auditing & Forensic Accounting, 4th Edition
88WFA

Member $75.00 | Nonmember $85.00

Implementing & Continually Improving IT Governance
ITG9

Member $55.00 | Nonmember $115.00

Information Security Roles & Responsibilities Made Easy, Version 3.0
2-PS3

Member $495.00 | Nonmember $505.00

IT Governance: Policies & Procedures, 2012 Edition
5-AS12

Member $245.00 | Nonmember $255.00

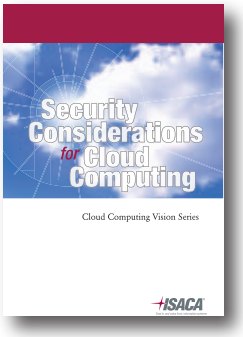
* Published by ISACA and ITGI

ISACA member complimentary download *www.isaca.org/downloads*

All prices are listed in US Dollars and are subject to change

SUPPLEMENT

NEW BOOKS www.isaca.org/newbooks



Security Considerations for Cloud Computing

ISACA

NEW

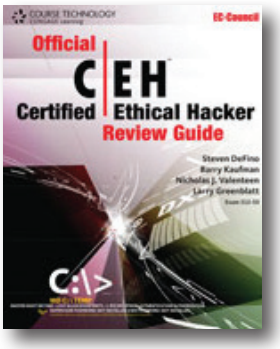
Another publication in the Cloud Computing Vision Series, *Security Considerations for Cloud Computing* presents practical guidance to facilitate the decision process for IT and business professionals concerning the decision to move to the cloud. It helps enable effective analysis and measurement of risk through use of decision trees and checklists outlining the security factors to be considered when evaluating the cloud as a potential solution.

There are five essential characteristics, three types of service models and four major deployment models taken into account relative to cloud computing. To ensure a common understanding of these models, this publication describes the characteristics of each characteristic and model.

This guide is meant for **all** current and potential cloud users who need to ensure protection of information assets moving to the cloud.

80 pages, 2012. **SCC**

Member **$35.00** | Nonmember **$75.00**



Official Certified Ethical Hacker Review Guide, 1st Edition

Steven DeFino

NEW

Get ready for the latest Certified Ethical Hacker exam with the only book authorized by the creators of the certification, EC-Council! This book covers all of the various areas of the very challenging Certified Ethical Hacker (CIEH) exam version 6.1, and includes hundreds of review questions in addition to refresher coverage of the information needed to successfully become a Certified Ethical Hacker. Including helpful at-a-glance quick reference boxes and tables, summaries, review questions and answers, tutorial information and more, this resource is at once succinct and comprehensive. With over 70 Try It Out exercises and challenges, plus assignments that guide the CIEH learner to additional study materials, this book is not just an exam preparation tool. This book helps prepare future Certified Ethical Hackers to proactively protect their organization's systems from malicious hackers. It strengthens readers' knowledge that will help them successfully assess and analyze computer system weaknesses and vulnerabilities—so they can most effectively safeguard the organization's information and assets. This is the ideal resource for anyone looking to refresh their skills in this area, learn more about ethical hacking, or successfully pass the certification exam and become a Certified Ethical Hacker.

384 pages, 2010. **14-IT**

Member **$41.00** | Nonmember **$51.00**

Inventory Reduction Sale

Books offered in the ISACA Bookstore Special Sale may contain dated material, overall these books are still of value.
Sales prices effective while quantities are available.

Visit *www.isaca.org/salesbooks* for available titles and pricing.

* Published by ISACA and ITGI

ISACA member complimentary download *www.isaca.org/downloads*

All prices are listed in US Dollars and are subject to change

Principios de auditoría y control de sistemas de información

NEW

Esta publicación reúne las nuevas prácticas internacionalmente aceptadas para auditoría de sistemas y tecnologías de información y comunicaciones, con un lenguaje claro y sencillo. Se detallan tanto los aspectos de gestión como los de carácter meramente técnico basados en el cuerpo de conocimientos propuesto por ISACA internacional.

310 pages, 2011. **1-TCA2**

Member **$50.00** | Nonmember **$60.00**

EXAM REFERENCE MATERIALS

2013 CISA® EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CISA exam, order ◆
www.isaca.org/cisabooks

CISA Review Manual 2013*

CISA Review Questions, Answers & Explanations Manual 2013*

CISA Review Questions, Answers & Explanations Manual 2013 Supplement*

CISA Practice Question Database v13*

2013 CISM® EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CISM exam, order ◆
www.isaca.org/cismbooks

CISM Review Manual 2013*

CISM Review Questions, Answers & Explanations Manual 2013 Supplement*

CISM Practice Question Database v13*

2013 CGEIT EXAM REFERENCE MATERIALS

◆ To prepare for the June 2013 CGEIT exam, order ◆
www.isaca.org/cgeitbooks

CGEIT Review Manual 2013*

CGEIT Review Questions, Answers & Explanations Manual 2013*

CGEIT Review Questions, Answers & Explanations Manual 2013 Supplement*

2013 CRISC EXAM REFERENCE MATERIALS

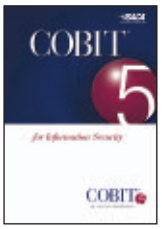
◆ To prepare for the June 2013 CRISC exam, order ◆
www.isaca.org/criscbooks

CRISC Review Manual 2013*

CRISC Review Questions, Answers & Explanations Manual 2013*

CRISC Review Questions, Answers & Explanations Manual 2013 Supplement*

FEATURED PUBLICATIONS
www.isaca.org/featuredbooks



COBIT 5 for Information Security*
CB5IS

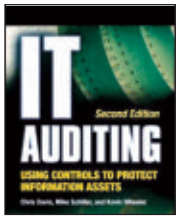
Member $35.00
Nonmember $175.00

WCB5IS—E-BOOK – PDF FORMAT

Member $35.00
Nonmember $175.00

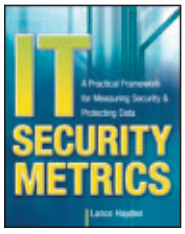
COBIT 5 Implementation*
CB5IG

Member $35.00
Nonmember $150.00



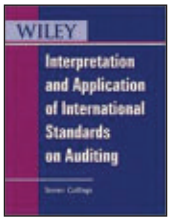
IT Auditing: Using Controls to Protect Information Assets
15-MIT2

Member $70.00
Nonmember $80.00



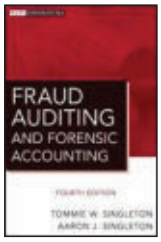
IT Security Metrics: A Practical Framework for Measuring Security and Protecting Data
22MSM

Member $50.00
Nonmember $60.00



Interpretation and Application of International Standards
95WISA

Member $105.00
Nonmember $115.00

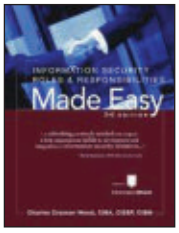


Fraud Auditing & Forensic Accounting, 4th Edition
88WFA

Member $75.00
Nonmember $85.00

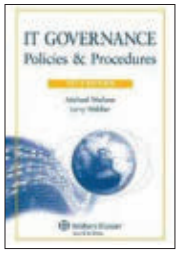
Implementing & Continually Improving IT Governance
ITG9

Member 55.00
Nonmember $115.00



Information Security Roles & Responsibilities Made Easy, Version 3.0
2-PS3

Member $495.00
Nonmember $505.00



IT Governance: Policies & Procedures, 2012 Edition
5-AS12

Member $245.00
Nonmember $255.00

* Published by ISACA and ITGI ISACA member complimentary download *www.isaca.org/downloads* All prices are listed in US Dollars and are subject to change

Code	Title		Nonmember	Member
2013 CISA® EXAM REFERENCE MATERIALS				
◆ To prepare for the June 2013 CISA exam, order ◆				
CISA Review Manual 2013*				
CRM-13	English Edition		$135.00	$105.00
CRM-13C	Chinese Simplified Edition		135.00	105.00
CRM-13F	French Edition		135.00	105.00
CRM-13I	Italian Edition		135.00	105.00
CRM-13J	Japanese Edition		135.00	105.00
CRM-13S	Spanish Edition		135.00	105.00
CISA Review Questions, Answers & Explanations Manual 2013*				
QAE-13	English Edition	(950 Questions)	130.00	100.00
QAE-13C	Chinese Simplified Edition	(950 Questions)	130.00	100.00
QAE-13I	Italian Edition	(950 Questions)	130.00	100.00
QAE-13J	Japanese Edition	(950 Questions)	130.00	100.00
QAE-13S	Spanish Edition	(950 Questions)	130.00	100.00
CISA Review Questions, Answers & Explanations Manual 2013 Supplement*				
QAE-13ES	English Edition	(100 Questions)	60.00	40.00
QAE-13CS	Chinese Simplified Edition	(100 Questions)	60.00	40.00
QAE-13FS	French Edition	(100 Questions)	60.00	40.00
QAE-13IS	Italian Edition	(100 Questions)	60.00	40.00
QAE-13JS	Japanese Edition	(100 Questions)	60.00	40.00
QAE-13SS	Spanish Edition	(100 Questions)	60.00	40.00
CISA Practice Question Database v13 (1,050 Questions)*				
CDB-13	CD-ROM—English Edition		225.00	185.00
CDB-13W	Download—English Edition (no shipping charges apply to download)		225.00	185.00
CDB-13S	CD-ROM—Spanish Edition		225.00	185.00
CDB-13SW	Download—Spanish Edition (no shipping charges apply to download)		225.00	185.00
CAN*	Candidate's Guide to the CISA Exam and Certification (No charge to paid CISA exam registrants)		15.00	5.00
2013 CISM® EXAM REFERENCE MATERIALS				
◆ To prepare for the June 2013 CISM exam, order ◆				
CISM Review Manual 2013*				
CM-13	English Edition		115.00	85.00
CM-13J	Japanese Edition		115.00	85.00
CM-13S	Spanish Edition		115.00	85.00
CISM Review Questions, Answers & Explanations Manual 2012*				
CQA-12	English Edition	(700 Questions)	90.00	70.00
CQA-12J	Japanese Edition	(700 Questions)	90.00	70.00
CQA-12S	Spanish Edition	(700 Questions)	90.00	70.00
CISM Review Questions, Answers & Explanations Manual 2012 Supplement*				
CQA-12ES	English Edition	(100 Questions)	60.00	40.00
CQA-12JS	Japanese Edition	(100 Questions)	60.00	40.00
CQA-12SS	Spanish Edition	(100 Questions)	60.00	40.00
CISM Review Questions, Answers & Explanations Manual 2013 Supplement*				
CQA-13ES	English Edition	(100 Questions)	60.00	40.00
CQA-13JS	Japanese Edition	(100 Questions)	60.00	40.00
CQA-13SS	Spanish Edition	(100 Questions)	60.00	40.00
CISM Practice Question Database v13 (900 Questions)*				
MDB-13	CD-ROM – English Edition		160.00	120.00
MDB-13W	Download – English Edition (no shipping charges apply to download)		160.00	120.00
CGC*	Candidate's Guide to the CISM Exam and Certification (No charge to paid CISM exam registrants)		15.00	5.00
2013 CGEIT EXAM REFERENCE MATERIALS				
◆ To prepare for the June 2013 CGEIT exam, order ◆				
CGM-13*	CGEIT Review Manual 2013		115.00	85.00
CGQ-13*	CGEIT Review Questions, Answers & Explanations Manual 2013 2013 Supplement (120 Questions)		115.00	85.00
CGQ-13ES*	CGEIT Review Questions, Answers & Explanations Manual 2013 Supplement (100 Questions)		60.00	40.00
CACG*	Candidate's Guide to the CGEIT Exam and Certification (No charge to paid CGEIT exam registrants)		15.00	5.00
2013 CRISC EXAM REFERENCE MATERIALS				
◆ To prepare for the June 2013 CRISC exam, order ◆				
CRR-13*	CRISC Review Manual 2013		115.00	85.00
CRQ-13*	CRISC Review Questions, Answers & Explanations Manual 2013 (200 Questions)		60.00	40.00
CRQ-13ES*	CRISC Review Questions, Answers & Explanations Manual 2013 Supplement (100 Questions)		60.00	40.00
CACR*	Candidate's Guide to the CRISC Exam and Certification (No charge to paid CRISC exam registrants)		15.00	5.00

Code	Title	Nonmember	Member
COBIT®			
CB4.1*	COBIT 4.1	190.00	75.00
CB5	COBIT 5	50.00	35.00
COBIT 5: Enabling Processes			
WCB5EP*	E-Book—PDF format (purchase online only)	135.00	FREE
CB5EP*	Print format	135.00	35.00
COBIT 5 Implementation			
WCB5IG*	E-Book—PDF format (purchase online only)	150.00	FREE
CB5IG*	Print format	150.00	35.00
COBIT 5 for Information Security			
WCB5IS*	E-Book—PDF format (purchase online only)	175.00	35.00
CB5IS*	Print format	175.00	35.00
COBIT and Application Controls: A Management Guide			
WCAC*	E-book—PDF format (purchase online only)	55.00	FREE
CAC*	Print format	75.00	35.00
CBX*	COBIT 4.1 Excerpt	5.00	5.00
CPS2*	COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition	110.00	55.00
CBQ2*	COBIT Quickstart, 2nd Edition	110.00	55.00
COBIT Assessor Guide: Using COBIT 4.1			
WCAG*	E-book—PDF format (purchase online only)	80.00	30.00
CAG*	Print format	100.00	50.00
COBIT Process Assessment Model (PAM): Using COBIT 4.1			
WCPAM*	E-book—PDF format (purchase online only)	40.00	FREE
CPAM*	Print format	50.00	30.00
COBIT Self-assessment Guide: Using COBIT 4.1			
WCSAG*	E-book—PDF format (purchase online only)	30.00	FREE
CSAG*	Print format	40.00	25.00
CBSB2*	COBIT Security Baseline, 2nd Edition	40.00	20.00
	Additional Set (5 each) Reference Cards		
	HRC2 Home Users	3.00	2.00
	PRC2 Professional Users	3.00	2.00
	MRC2 Managers	3.00	2.00
	ERC2 Executives	3.00	2.00
	SRC2 Senior Executives	3.00	2.00
	BRC2 Board of Directors/Trustees	3.00	2.00
COBIT User Guide for Service Managers			
WCUG*	E-book—PDF format (purchase online only)	35.00	FREE
CUG*	Print format	50.00	20.00
CB4A*	IT Assurance Guide: Using COBIT	165.00	55.00
ITG9*	Implementing and Continually Improving IT Governance	115.00	55.00
SDG*	SharePoint Deployment and Governance Using COBIT 4.1: A Practical Approach	70.00	30.00
COBIT Online 4.1			
COLB*	Annual Full Subscription + Benchmarking (purchase online at *www.isaca.org/cobitonline*) ISACA members SAVE 75%	400.00	200.00 50.00

▶ **Visit *www.isaca.org/cobitonline* for additional information.** ◀

COBIT Mappings			
WCMCMM*	Mapping of CMMI for Development V1.2 With COBIT 4.0	25.00	FREE
WCMISO*	Mapping of ISO/IEC 17799: 2005 With COBIT 4.0	25.00	FREE
WCMIT3*	Mapping of ITIL V3 With COBIT® 4.1	25.00	FREE
WCMNIST*	Mapping of NIST SP800-53 Rev 1 With COBIT® 4.1	25.00	FREE
WCMPMB*	Mapping of PMBOK to COBIT 4.0	25.00	FREE
WCMSEI*	Mapping of SEI's CMM for Software to COBIT 4.0	25.00	FREE
WCMTOG*	Mapping of TOGAF 8.1 With COBIT 4.0	40.00	FREE
WCMFF*	Mapping FFIEC with COBIT 4.1	25.00	FREE
WCM20000*	Mapping of ISO/IEC 20000 with COBIT 4.1	25.00	FREE
WCMCMM2*	Mapping of CMMI for Development V1.2 with COBIT 4.1	25.00	FREE

Sets of related COBIT products focusing on your professional needs are available—purchase a focus set and save! See *www.isaca.org/cobitbooks* for components included in each Focus Set

Meycor COBIT Suite
Comprehensive software for implementing COBIT 4.1 as an IT governance, security or assurance tool. (see *www.isaca.org/cobit* for descriptions and pricing)

See **NON-ENGLISH RESOURCES** for additional COBIT material.

VAL IT™			
Enterprise Value: Governance of IT Investments			
VITM*	Getting Started With Value Management	40.00	25.00
VITF2*	The Val IT Framework 2.0	90.00	45.00
VITB2*	The Business Case Guide—Using Val IT 2.0	40.00	25.00
VITAG*	Value Management Guidance for Assurance Professionals—Using Val IT 2.0	40.00	25.00
VITS2*	Complete Set	185.00	105.00
39-CRC	The Business Value of IT: Managing Risks, Optimizing Performance and Measuring Results	86.00	76.00
5-RO	A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance	105.00	95.00

Shaded — New Books * Published by ISACA and ITGI ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE

Code	Title	Nonmember	Member
RISK IT AND RISK RELATED TOPICS			
78-WRM	The Failure of Risk Management: Why It's Broken and How to Fix It	55.00	45.00
70-WFR	Fraud Risk Assessment: Building a Fraud Audit Program	84.00	74.00
11-CRC8	How to Complete a Risk Assessment in 5 Days or Less	88.00	98.00
84-WRM	Information Technology Risk Management in Enterprise Environments	105.00	95.00
2-HBS	IT Risk: Turning Business Threats Into Competitive Advantage	45.00	35.00
1-HHOP	The Operational Risk Handbook for Financial Companies	90.00	80.00
5-PL	Risk Management & Risk Assessment	105.00	95.00
55-WRCS	Risks, Controls, and Security: Concepts and Applications	129.00	119.00
RITF*	The Risk IT Framework	95.00	45.00
RITPG*	The Risk IT Practitioner Guide	115.00	55.00
AUDIT, CONTROL AND SECURITY—ESSENTIALS			
48-CRC	Access Control, Security, and Trust: A Logical Approach	100.00	90.00
1-IT9	Accounting Information Systems, 9th Edition	258.00	248.00
93-WAAS	Auditing and Assurance Services: Understanding the Integrated Audit	223.00	213.00
6-PL	Auditing IT Infrastructures	105.00	95.00
76-WSL	Build Your Own Security Lab: A Field Guide for Network Testing	60.00	50.00
43-CRC	Building an Effective Information Security Policy Architecture	94.00	84.00
31-CRC	Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience and ROI	140.00	130.00
79-WCAF	Computer Aided Fraud Prevention and Detection: A Step by Step Guide	74.00	64.00
4-IGI	Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions	110.00	100.00
51-CRC	Data Protection: Governance, Risk Management, and Compliance	86.00	76.00
50-WPM6	Effective Project Management: Traditional, Agile, Extreme, 6th Edition	70.00	60.00
1-ABES	Enterprise Security for the Executive: Setting the Tone from the Top	45.00	35.00
92-WIA	The Essential Guide to Internal Auditing, 2nd Edition	65.00	55.00
71-WCF	Essentials of Corporate Fraud	58.00	48.00
82-WACL	Fraud Analysis Techniques Using ACL	221.00	211.00
11-IT	Guide to Firewalls and VPNs, 3rd Edition	165.00	155.00
5-IGI	ICT Ethics and Security in the 21st Century: New Developments and Applications	190.00	180.00
7-ART	Implementing the ISO/IEC 27001 Information Security Management System Standard	105.00	95.00
2-ABA	Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists	106.00	96.00
83-WIS	Information Storage and Management: Storing, Managing, and Protecting Digital Information	70.00	60.00
4-CRC3	Information Technology Control and Audit, 3rd Edition	100.00	90.00
95-WISA	Interpretation and Application of International Standards on Auditing	115.00	105.00
90-WACS	IT Audit, Control, and Security	95.00	85.00
IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud			
WITCOC*	E-book – PDF Format (purchase online only)	50.00	FREE
ITCOC*	Print Format	60.00	35.00
STDPK*	IT Standards and Summaries of Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals	20.00	15.00
WITAF*	ITAF: A Professional Practices Framework for IT Assurance e-book—PDF (purchase online only)	45.00	FREE
15-MIT2	IT Auditing Using Controls to Protect Information Assets, 2nd Edition	80.00	70.00
IT Control Objectives for Basel II			
WITCOB*	E-book—PDF Format (purchase online only)	35.00	FREE
ITCOB*	Print Format	50.00	20.00
PSOX*	IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition	7.00	7.00
22-MSM	IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data	60.00	50.00
6-ITSOC	IT Strategic and Operational Controls	70.00	60.00
1-IIA	A New Auditor's Guide to Planning, Performing, and Presenting IT Audits	80.00	70.00
7-SYN9	PCI Compliance, Second Edition	70.00	60.00
1-RIA	Practical IT Auditing with current Supplement	445.00	435.00
12-IT	Principles of Information Security, 4th Edition	152.00	142.00
2-SAPP	SAP Security and Risk Management, 2nd Edition	80.00	70.00
28-MSM	Security Metrics: A Beginner's Guide	50.00	40.00
2-BAY*	Stepping Through the InfoSec Program	45.00	35.00
AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS			
18-MAO	Applied Oracle Security: Developing Secure Database and Middleware Environments	70.00	60.00
4-DC	Audit Guidelines for DB2	80.00	70.00
53-CRC	FISMA Principles and Best Practices: Beyond Compliance	90.00	80.00
10-ART	Identity Management: Concepts, Technologies, and Systems	110.00	100.00
Linux: Security, Audit and Control Features			
WLIN*	E-book—PDF Format (purchase online only)	30.00	15.00
PLIN*	Print Format	50.00	35.00

Code	Title	Nonmember	Member
AUDIT, CONTROL AND SECURITY—SPECIFIC ENVIRONMENTS *(cont.)*			
Managing Risk in Wireless Environment: Security, Audit and Control Issues			
WW*	E-book—PDF Format (purchase online only)	40.00	20.00
PW*	Print Format	50.00	35.00
OS390*	OS/390-z/OS Security, Audit and Control Features	70.00	55.00
29-ST4	A Practical Guide to IBM i and i5/OS Security and Compliance	89.00	79.00
1-MPPI	Protecting Industrial Control Systems from Electronic Threats	100.00	90.00
ODB9*	Security, Audit and Control Features Oracle® Database, 3rd Edition	55.00	40.00
ISOA3*	Security, Audit and Control Features Oracle® E-Business Suite, 3rd Edition	75.00	60.00
ISPS3*	Security, Audit and Control Features Oracle® PeopleSoft®, 3rd Edition	80.00	65.00
ISAP3*	Security, Audit and Control Features SAP® ERP, 3rd Edition	75.00	60.00
3-JBSS	Security Strategies in Windows Platforms and Applications	100.00	90.00
NON-ENGLISH RESOURCES			
1-TCA2	Principios de auditoría y control de sistemas de información	60.00	50.00
2-TCA	Administración de la Seguridad de Información	55.00	45.00
CISA Examination Reference Material			
	Study aids available in Chinese Simplified, French, German, Italian, Japanese and Spanish for the December 2012 CISA exam—see page S5		
CISM Examination Reference Material			
	Study aids available in Japanese and Spanish for the December 2012 CISM exam—see page S5		
COBIT 3rd Edition, available at the following web site	Korean Edition—*www.isaca.or.kr*		
COBIT 4.0 Edition, available at the following web sites	German Edition—*www.isaca.ch*		
COBIT 4.1 Edition, available at the following web site	Chinese Simplified Edition - *www.isaca.org/getcobit* French Edition—*www.afai.fr* Hebrew Edition - *www.isaca.org.il* Hungarian Edition—*www.isaca.org/getcobit* Italian Edition - *www.aiea.it* Japanese Edition—*www.isaca.org/getcobit* Portuguese Edition—*www.isaca.org/getcobit* Russian Edition—*www.isaca-russia.ru* Spanish Edition—*www.isaca.org/getcobit*		
1-AOCF	Computación Forense: Descubriendo los Rastros Informáticos	42.00	32.00
Meycor COBIT Suite			
	Meycor CobiT es un software completo e integrado para la implementación de COBIT como una herramienta para el Buen Gobierno de la TI, Seguridad de la TI o Aseguramiento de la TI según COBIT 4.1. (see *www.isaca.org/nonenglishbooks* para descripción y precios)		
INTERNET AND RELATED SECURITY TOPICS			
19-M24	24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them	60.00	50.00
45-CRC	Cloud Computing: Implementation, Management, and Security	90.00	80.00
11-EL	Cyber Attacks: Protecting National Infrastructure	70.00	60.00
1-CAP3	Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, 3rd Edition	48.00	38.00
2-SCC	Cybercrimes: A Multidisciplinary Analysis	199.00	189.00
10-IT	Cybersecurity: The Essential Body of Knowledge	91.00	81.00
4-MGH3	Gray Hat Hacking: The Ethical Hakers Handbook, 3rd Edition	70.00	60.00
23-MHE	Hacking Exposed Web Applications, 3rd Edition	60.00	50.00
2-MCG7	Hacking Exposed 7: Network Security Secrets & Solutions, 7th Edition	60.00	50.00
17-MHE2	Hacking Exposed Wireless: Wireless Security Secrets & Solutions, 2nd Edition	60.00	50.00
49-CRC	Honeypots: A New Paradigm to Information Security	150.00	140.00
29ST-3	The Little Black Book of Computer Security, 2nd Edition	35.00	25.00
21-MMS	Mobile Application Security	60.00	50.00
86-WNS	Network Security Bible, 2nd Edition	70.00	60.00
10-MOC2	Network Security: The Complete Reference, 2nd Edition	80.00	70.00
59-WNS	Network Security Fundamentals	82.00	72.00
1-GL	NMAP Network Scanning: The Official NMAP Project Guide to Network Discovery and Security Scanning	60.00	50.00
1-WCNR	No Root for You: A Series of Tutorials, Rants and Raves, and Other Random Nuances Therein	33.00	23.00
14-IT	Official Certified Ethical Hacker Review Guide, 1st Edition	41.00	51.00
56-WPC	Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft	106.00	96.00
1-HA	Scrappy Information Security: The Easy Way to Keep the Cyber Wolves at Bay	30.00	20.00
SCC*	Security Considerations for Cloud Computing	75.00	35.00
30-CRC	Securing Converged IP Networks	100.00	90.00
24-MSIEM	Security Information and Event Management (SIEM) Implementation	75.00	65.00
27-MSC	Securing the Clicks: Network Security in the Age of Social Media	50.00	40.00
2-JBSF	System Forensics, Investigation, and Response	100.00	90.00
29-MWAS	Web Application Security: A Beginner's Guide	50.00	40.00

Shaded — New Books * Published by ISACA and ITGI ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE

Code	Title	Nonmember	Member
IT GOVERNANCE AND BUSINESS MANAGEMENT			
94-WIFRS	An Executive Guide to IFRS: Content, Costs and Benefits to Business	50.00	40.00
3-PAGE	7 Steps to Better Written Policies and Procedures	30.00	20.00
4-PAGE	Best Practices in Policies and Procedures	36.00	26.00
1-ITG*	Board Briefing on IT Governance, 2nd Edition	7.00	7.00
6-SYN	Business Continuity and Disaster Recovery Planning for IT Professionals	70.00	60.00
BMIS*	The Business Model for Information Security	60.00	45.00
54-WCIO2	CIO Best Practices: Enabling Strategic Value with Information Technology, 2nd Edition	75.00	65.00
WCCS*	Creating a Culture of Security (e-book)	50.00	FREE
11-ITDG	The Data Governance Imperative	50.00	40.00
37-CRC	Digital Privacy: Theory, Technologies, and Practices	90.00	80.00
89-WEG	Empowering Green Initiatives with IT: A Strategy and Implementation Guide	60.00	50.00
9-ART	Enterprise Information Security and Privacy	109.00	99.00
13-IT	Ethics in Information Technology, 4th Edition	101.00	91.00
23-WIT	The Executive's Guide to Information Technology, 2nd Edition	110.00	100.00
10-VH	Foundations of IT Service Management Based on ITIL® V3	65.00	55.00
3-VH	Frameworks for IT Management	65.00	55.00
85-WF101	Fraud 101: Techniques and Strategies for Understanding Fraud, 3rd Edition	65.00	55.00
64-WGRC	Governance, Risk and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices	173.00	163.00
7-ITGR	Green IT in Practice, 2nd Edition	60.00	50.00
20-MHE	Hacking Exposed Malware and Rootkits: Malware & Rootkits Secrets & Solutions	60.00	50.00
67-WHF	Human Factors in Project Management: Concepts, Tools, and Techniques for Inspiring Teamwork and Motivation	62.00	52.00
1-IBM	The IBM Data Governance Unified Process	35.00	25.00
WGOALS*	Identifying and Aligning Business Goals and IT Goals (E-book—PDF purchase online only)	35.00	20.00
4-ID	Implementing Information Technology Governance: Models, Practices and Cases	110.00	100.00
46-CRC	Implementing the Project Management Balanced Scorecard	90.00	80.00
10-ITISQ	Implementing Service Quality based on ISO/IEC 20000	35.00	25.00
2-ITG*	Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition	7.00	7.00
Information Security Governance: Guidance for Information Security Managers			
3-ITG*	Information Security Governance: Guidance for Information Security Managers	50.00	25.00
W3ITG*	E-book—PDF Format (purchase online only)	45.00	FREE
WSH*	Information Security Harmonisation: Classification of Global Guidance (E-book—PDF format purchase online only)	40.00	FREE
1-BS12	Information Security Policies Made Easy, Version 12	805.00	795.00

Code	Title	Nonmember	Member
IT GOVERNANCE AND BUSINESS MANAGEMENT *(cont.)*			
2-PS3	Information Security Roles & Responsibilities Made Easy, Version V3	505.00	495.00
50-CRC	Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement	90.00	80.00
3-IGI	Information Technology Governance and Service Management: Frameworks and Adaptations	205.00	195.00
80-WITM8	Information Technology for Management: Improving Strategic and Operational Performance, 8th Edition	212.00	202.00
81-WIC	Internal Controls Policies and Procedures	95.00	85.00
12-VH	IT Financial Management	65.00	55.00
3-ITGD	IT Governance: Guidelines for Directors	60.00	50.00
4-ITIG	IT Governance: A Pocket Guide	25.00	15.00
5-AS12	IT Governance: Policies & Procedures, 2012 Edition	255.00	245.00
WGPM*	IT Governance and Process Maturity (E-Book—purchase online only)	30.00	FREE
8-ITHP	IT Governance to Drive High Performance: Lessons from Accenture	25.00	15.00
5-ITOC	IT Outsourcing Contracts: A Legal and Practical Guide	40.00	30.00
11-VH	IT Outsourcing: Part 1 Contracting the Partner	41.00	31.00
12-ITPM	IT Project Management: 30 Steps to Success	30.00	20.00
25-MIPM	IT Project Management: On Track from Start to Finish, 3rd Edition	60.00	50.00
91-WKPI	Key Performance Indicators (KPI): Developing, Implementing, and Using Winning KPIs, 2nd Edition	60.00	50.00
52-CRC	Lean IT: Enabling and Sustaining Your Lean Transformation	62.00	52.00
26-MDM	Master Data Management and Data Governance, 2nd Edition	70.00	60.00
9-VH	MOF—Microsoft Operations Framework V4.0: A Pocket Guide	32.00	22.00
MIC*	Monitoring Internal Control Systems and IT	70.00	55.00
2-ITO	Outsourcing IT: A Governance Guide	60.00	50.00
3-JR	A Practical Guide to Reducing IT Costs	60.00	50.00
6-RO	Principles and Practice of Business Continuity: Tools and Techniques	109.00	99.00
1-IS	The Privacy Management Toolkit	505.00	495.00
Security Awareness: Best Practices to Secure Your Enterprise			
WSA*	E-book—PDF Format (purchase online only)	35.00	20.00
PSA*	Print Format	50.00	35.00
75-WSO	The Sarbanes-Oxley Section 404 Implementation Toolkit: Practice Aids for Managers and Auditors, 2nd Edition	105.00	95.00
13-VH	The Service Catalog	66.00	56.00
9-ITSIA	Swanson on Internal Auditing: Raising the Bar	60.00	50.00
77-WTS	Technology Scorecards: Aligning IT Investments with With Business Performance	60.00	50.00
4-ITG*	Unlocking Value: An Executive Primer on the Critical Role of IT Governance	7.00	7.00
2-ITPI	Visible OPS Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps	32.00	22.00
87-WWC	World Class IT: Why Businesses Succeed When IT Triumphs	48.00	38.00

Shaded — New Books * Published by ISACA and ITGI ALL PRICES ARE LISTED IN US DOLLARS AND ARE SUBJECT TO CHANGE

FOUR EASY WAYS TO PLACE AN ORDER:

Order online at *www.isaca.org/bookstore*

Mail completed form with payment:
ISACA/ITGI
1055 Paysphere Circle
Chicago, IL 60674-1055 USA

Fax completed order form with credit card number and expiration date to +1.847.253.1443

Phone: +1.847.660.5650
Monday-Friday, 8:00 am-5:00 pm Central Time (Chicago, Illinois, USA) Personal service—please have credit card number available. We will confirm availability and expected delivery date.

Send electronic payments in US dollars to: Bank of America, ABA #0260-0959-3
ISACA Account #22-71578
S.W.I.F.T code BOFAUS3N

RETURN POLICY

All purchases are final. No refunds or exchanges.

PUBLICATION QUANTITY DISCOUNTS

Academic and bulk discounts are available on books published by the ISACA and IT Governance Institute. Please call +1.847.660.5501 or +1.847.660.5578 for pricing information.

DELIVERY

Orders normally ship within 2-3 business days upon receipt of payment. Once shipped, delivery time can vary between 2-7 business days.

CUSTOMS

Customers are responsible for any custom duties/taxes/VAT charges levied by the country of destination. See *www.isaca.org/shipping* for further information.

SUPPLEMENT

ISACA®
Trust in, and value from, information systems

Customer Order Form

Order Online at *www.isaca.org/bookstore*

OFFICE USE ONLY

Vol. 6-12

U.S. Federal I.D. No. 23-7067291

PLEASE NOTE: READ PAYMENT TERMS AND SHIPPING INFORMATION BELOW. ALL ORDERS MUST BE PREPAID.

Please return to: ISACA, 1055 Paysphere Circle, Chicago, IL 60674, USA
Phone: +1.847.660.5650 Fax: +1.847.253.1443 E-mail: *bookstore@isaca.org*

Your contact information will be used to fulfill your request, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. To learn more, please visit *www.isaca.org* and read our Privacy Policy.

Customer Information

Name _____
FIRST MIDDLE LAST/FAMILY

ISACA Member: ☐ No ☐ Yes Member Number _____

Company Name _____

Address: ☐ Home ☐ Company

_____

_____

City _____ State/Province _____

Country _____ Zip/Mail Code _____

Phone Number ( ) _____

Fax Number ( ) _____

E-mail Address _____

Shipping Information (If different from customer information)

If shipping to a PO Box, please include street address to ensure proper delivery.

Name _____
FIRST MIDDLE LAST/FAMILY

Company Name _____
(IF PART OF SHIPPING ADDRESS)

Address: _____

_____

_____

City _____ State/Province _____

Country _____ Zip/Mail Code _____

Phone Number ( ) _____

E-mail Address _____

Code	Title/Item	Quantity	Unit Price	Total

Thank you for ordering from ISACA. **All purchases are final.**

Subtotal	
Sales Tax: Add sales tax if shipping to: Louisiana (LA), Oklahoma (OK)—4%	
Wisconsin (WI)—5%	
Florida (FL), Minnesota (MN), Pennsylvania (PA), South Carolina (SC), Texas (TX), Washington (WA)—6%	
California (CA), New Jersey (NJ), Puerto Rico (PR), Tennessee (TN)—7%	
Illinois (IL)—9%	
For all orders please include shipping and handling charge—see chart below.	
TOTAL	

Payment Information—Prepayment Required

☐ Payment enclosed. Check payable to "ISACA" in US dollars, drawn on US bank.

☐ Bank wire transfer in US dollars. Date of transfer _____

☐ Charge to ☐ Visa ☐ MasterCard ☐ Discover ☐ American Express ☐ Diners Club

Credit Card # _____

Exp. Date _____

Print Cardholder Name _____

Signature of Cardholder _____

Shipping & Handling Rates for Orders

All orders outside the US are shipped Federal Express Priority.

For Orders Totaling	Outside US	Within US
Up to US $30.00	US $10.00	US $5.00
US $30.01 to US $50.00	US $15.00	US $7.00
US $50.01 to US $80.00	US $20.00	US $8.00
US $80.01 to US $150.00	US $26.00	US $10.00
Over US $150.00	17% of Total	10% of Total

No shipping charges apply to *Meycor COBIT*.
No shipping charges apply to CISA Practice Question Database v12—download.
No shipping charges apply to CISM Practice Question Database v12—download.

Shipping details *www.isaca.org/shipping*
International customers are solely responsible for paying all custom duties, service charges, and taxes levied by their country.

All purchases are final. **Pricing, shipping and handling, and tax are subject to change without notice.**

Connect. Recruit. **Win.**

2012 ISACA
Member Get A Member

When ISACA grows, members benefit. More recruits mean more networking, more connections, more resources, and more chances to win valuable prizes!

Connect

For each new member who credits you as their recruiter (by entering your ID#), you are entered to win one of our Monthly Prizes. Plus, a Top Recruiter Grand Prize will be awarded to the individual who recruits the most new full-dues paying* members to ISACA.

Winners will have the opportunity to receive global recognition in *@AGlance* and on the ISACA website for encouraging colleagues to join ISACA.

Recruit

- Colleagues or new college graduates invested in professional growth
- Someone interested in taking a CISA®, CISM®, CGEIT® or CRISC™ exam
- A full-time student majoring in fields including: information systems, business administration, accounting, information technology, engineering, computer science

** Full-dues includes US $135 ISACA International dues, plus chapter dues if applicable.*

TO LEARN MORE

Contact *mgam@isaca.org* or visit *www.isaca.org/mgam-journal6*.

MEMBER GET A MEMBER
Growing our future together.

Win!

GRAND PRIZE

The Top Recruiter will receive either a 2013 ISACA conference or exam registration plus travel expenses or study materials *(maximum value US $1500).* Winner will be awarded in January 2013.

MONTHY PRIZE DRAWINGS

Monthly Prize Winners will continue to be announced through December 2012.

One Professional Member and one Student member who have recruited at least one new Member during each month will be eligible to receive a prize *(value US $50)*. There will be two winners each month.

ISACA®
Trust in, and value from, information systems

Visit us on Stand 218 at the 2012
ISACA IT GRC conference in Las Vegas

AdaptiveGRC™
Flexible. Interconnected. Comprehensive.

Integrated solutions to help manage your IT GRC

"WHAT I REALLY LIKE ABOUT THIS SOLUTION IS THAT IT COMBINES CONTROL MATERIAL AND FUNCTIONALITY THAT YOU DON'T FIND ANYWHERE ELSE"
HEAD OF TECHNOLOGY AUDIT & ASSESSMENT FROM A FORTUNE 50 COMPANY

Unequalled information security risk profiling and assessment system to monitor and report against primary regulations and standards for all of your key internal and external systems:

- Touch of a button status reporting – by region, regulation, function, risk, etc.;
- Built-in process automation to increase productivity and massively reduce administration effort;
- 'Ask once/satisfy many' design to ensure a lean but appropriate experience by your customer and stakeholder groups.

Our unique GRC data warehousing capabilities can also unlock the value from your existing security and compliance applications.

C&F is a full service technology company, with strong data warehousing and business intelligence capabilities. Our other core product is Customer Relationship Management.

www.adaptivegrc.com

adaptive@candf.pl **US:** +1 678 591 6965 **UK:** +44 207 022 4884 **Poland:** +48 22 323 73 60