Volume 1, 2014

ISACA® Journal

Data Privacy

Featured articles:

SCADA Cybersecurity Framework

Key Considerations in Protecting Sensitive Data Leakage Using Data Loss Prevention Tools

Auditing for PII Security Compliance

And more...

ISACA®
Trust in, and value from, information systems

WWW.ISACA.ORG

ISACA®

Trust in, and value from, information systems

"I'M RECOGNIZED FOR **MY CERTIFICATION.**

I'M VALUED FOR **WHAT I DO WITH IT."**

— KETAN DHOLAKIA, CISM, CRISC

MANAGING PARTNER, MACLEAR
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2008

Getting an ISACA® certification doesn't just say you're well read or well connected. It announces that you have the expertise and insight to speak with authority. The credibility that it adds lets you create value for your enterprise. Your certification is more than a credential, it's a platform that can elevate your career.

Register at *www.isaca.org/register14-Jv1*

INFLUENCE MORE

UPCOMING EXAM DATE:
14 June 2014

Early Registration Deadline: 12 February 2014
Final Registration Deadline: 11 April 2014
Save US $50 when you register early.

CISA® Certified Information Systems Auditor®

CISM® Certified Information Security Manager®

CGEIT® Certified in the Governance of Enterprise IT®

CRISC™ Certified in Risk and Information Systems Control™

Register early to save US $50!
www.isaca.org/register14-Jv1

KEEP YOUR CAREER ON TRACK

Regis University's College of Professional Studies 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. Our School of Computer and Information Sciences 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) - choose the courses that most interest you

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 19 consecutive years.

COMMITTEE ON NATIONAL SECURITY SYSTEMS CNSS SYSTEMS SECURITY FOR THE 21st CENTURY

BEST COLLEGES U.S.News & WORLD REPORT REGIONAL UNIVERSITIES WEST 2014

REGIS UNIVERSITY
School of Computer & Information Sciences

LEARN MORE

www.informationassurance.regis.edu/ISACA
877.820.0581

VOLUME 1, 2014

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.

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 1 February 2014.

An Integrated Approach to Enterprise Risk
Munir A. Majdalawieh, Ph.D.

Building Information Security Professionals
Jason Andress, Ph.D., CISM, CISSP, GPEN, ISSAP

Importance of Forensic Readiness
Dauda Sule, CISA

Integrating Security Analytics Into GRC Programs
Yo Delmar, CISM, CGEIT, CMC

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.

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

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

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

Steven J. Ross, CISA, CISSP, MBCP, is executive principal of Risk Masters Inc. 2014 marks the 15th anniversary of Ross' popular *Journal* column. Ross can be reached at *stross@riskmastersinc.com*.

Extra, Extra, Read All About It

Item: An apparent cyberattack paralyzed the computers of three South Korean television channels and crippled the networks of two of the country's largest banks.

Item: Cyberspies have stolen the top-secret blueprints for the Australian Security Intelligence Organization's new headquarters.

Item: Twitter has experienced technical problems, probably as a result of a cyberattack by the so-called Syrian Electronic Army (SEA).

How do I know all this? I read it in the newspapers.[1]

DISCLOSED CYBERATTACKS

The issue here is not that cyberattacks occur. I have hacked that to death in previous columns.[2] I find it interesting that reports of these crimes are reported in the media with such frequency that individual cyberattacks are barely newsworthy any longer. In earlier times, it has been my experience that companies and government agencies preferred not to have any publicity about successful (or even unsuccessful) penetrations of their information systems. They feared exposure of their systems' weaknesses, potential liability and simple embarrassment. So what has caused organizations to go public today?

The easiest answer is that the target of many attacks is a web site, the face an organization places before the world. When a web site is taken down, there is no way to hide the fact that it has occurred; thus, the organization has no alternative but to be forthcoming. For example, when the web sites of several US banks were brought down, many issued public apologies.[3] In many cases, the media have pointed to national governments or terrorist groups as the sources of the attacks.[4]

If cyberattacks are cast as acts of undeclared war, it makes the victims seem a bit heroic, as frontline fighters in the war against…what exactly? More to the point, it deflects attention from the inability of these companies to anticipate, defend against and prevent the success of these attacks.

UNDISCLOSED ATTACKS

I am particularly curious about what is not reported. Perhaps there is a positive reason, inasmuch as those that were successful in preventing attacks, if such exist, do not make the news. Noticeably, when the attackers get too close to the bone, organizations are less likely to talk about the events. For example, one victim of a particularly destructive wave of attacks "would not talk about the recent attack there, its origins or its consequences. [It] has openly acknowledged previous denial-of-service attacks. But the size and severity of the most recent one apparently led it to reconsider."[5]

Web sites are important but not nearly as valuable as an organization's databases, particularly those that contain customer information. Have these been targeted? I would think they probably have been. Have they been successful? We have only negative evidence that they have not, since an occurrence of corporate amnesia probably would have been reported. Or perhaps, there were successful attacks and organizations have not been forced to recover from replicated or backed-up data.

I am aware of two instances of widely reported, partially successful cyberattacks, both of which were interpreted as being politically inspired. The destruction of data on 30,000 personal computers at Saudi Aramco was widely reported and was attributed to a foreign government.[6] The same sort of attack occurred at RasGas, a Qatari producer of liquefied natural gas.[7] In both cases, the companies denied serious impact on their core business activities. Are there many—or any—other, similarly successful attacks that have not been publicly reported?

REPORTED AND UNREPORTED RISK

It is by no means evident that organizations are completely open about cyberevents that they have experienced or might in the future. A recent report from Willis, a global insurance organization, indirectly underscores this point.[8] Willis surveyed the regulatory reports of the

Fortune 1000[9] for disclosures regarding their cyberexposures. It found that only 21 percent of the top 500 companies and 15 percent of the second tier cited exposure to cyberterrorism. Overall, 12 percent of the larger companies and 22 percent of companies ranked between 501 and 1,000 mentioned cyberrisk at all. Willis surmised that the difference between the larger and relatively smaller companies might be that smaller companies feel that they are less likely targets of attacks or that they need more time to identify their cyberexposures.[10]

It is fair to assume that had the companies in the Fortune 1000 experienced actual attacks, they would be sensitive to their exposure, but would they report the fact to the US Securities and Exchange Commission? The public is left to ponder whether these companies have, in fact, not been attacked or if they have been, but have failed to report the incidents. In either case, the fact that 17 percent of the largest US companies do not see cyberthreats affecting them is troublesome in itself.

Sadly, cyberthreats are a part of business life in the 21st century. Nonetheless, Willis states that only a small percentage of companies in the Fortune 1000 have purchased stand-alone cybercoverage, indicating a lack of perceived risk (or a perception of the quality and cost of the insurance coverage). The absence of any statements on the claims history against those policies is itself revealing. I have always felt that companies that have insurance against cyberattacks might not tell the media when such an event occurs, but that they would tell their insurers. To borrow from American humorist Will Rogers, if all I know is what I read in the papers, then what is not there may be more important than what is.

ENDNOTES

[1] To be honest, I read it on the newspapers' web sites. Specifically: Lewis, Leo; "Cyber-attack Cripples South Korean Banks and TV Stations," *The Times*, UK, 21 March 2013, *www.thetimes.co.uk/tto/news/world/asia/article3718137.ece*. Dupont, Alan; "Cyber Attacks Much More Widespread," *The Australian*, 29 May 2013, *www.theaustralian.com.au/national-affairs/opinion/cyber-attacks-much-more-widespread/story-e6frgd0x-1226652546742#*. *Le Figaro*, "Twitter victime d'une cyber-attaque," 28 August 2013, *www.lefigaro.fr/flash-eco/2013/08/28/97002-20130828FILWWW00192-twitter-victime-d-une-cyber-attaque.php*. While my usual source for news is *The New York Times*, in this case, I deliberately looked at respected journals from around the world to show that reporting on cyberattacks is a global phenomenon.

[2] Outrageous pun. My apologies.

[3] NPR, "PNC Bank's Website Is Victim of Cyber Attack," 28 September 2013, *www.npr.org/2012/09/28/161934801/business-news*. Wells Fargo, "We apologize to customers who may be experiencing limited access…," Twitter.com, 25 September 2013, *https://twitter.com/WellsFargo/status/250687157604347904*

[4] For a few examples, see: Perlroth, Nicole; "Hackers May Have Had Help With Attacks on U.S. Banks, Researchers Say," *The New York Times*, 27 September 2012, *http://bits.blogs.nytimes.com/2012/09/27/hackers-may-have-had-help-with-attacks-on-u-s-banks-researchers-say/?_r=0, blames Izz ad-Din al-Qassam*. Perlroth, Nicole; Quentin Hardy; "Bank Hacking Was the Work of Iranians, Officials Say," 8 January 2013, *www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html*

[5] Perlroth, Nicole; David Sanger; "Cyberattacks Seem Meant to Destroy, Not Just Disrupt," *The New York Times*, 28 March 2013, *www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html*

[6] Mahdi, Wael; "Saudi Arabia Says Aramco Cyberattack Came From Foreign States," Bloomberg, 9 December 2012, *www.bloomberg.com/news/2012-12-09/saudi-arabia-says-aramco-cyberattack-came-from-foreign-states.html*

[7] Osgood, Patrick; "Cyber Attack Takes Qatar's RasGas Offline," ArabianBusiness.com, 30 August 2012, *www.arabianbusiness.com/cyber-attack-takes-qatar-s-rasgas-offline-471345.html#.UmVFShbD_Dc*

[8] Willis, "Willis Fortune 1000 Cyber Disclosure Report," August 2013

[9] While this study looked at the submissions of US-based companies only, there is little reason to believe that the results would have been different if it were based on companies in other countries. Moreover, many of the Fortune 1000 are multinationals, thereby incorporating much of the rest of the world.

[10] *Ibid.*, p. 2

Process Automation From the Cloud

Jeff Rauscher, director of solutions design for Redwood Software (*www.redwood.com*), has more than 31 years of diversified management of information systems (MIS)/IT experience working with a wide variety of technologies including SAP, HP and IBM. Rauscher has worked in operations management, data center relocation, hardware planning, installation and de-installation, production control management, quality assurance, and customer support.

Cloud-based solutions are in demand everywhere. They provide fast, flexible, elastic and affordable ways to build in competitive advantage. Process automation enabled by the cloud is an important next step for IT innovation. It enables business and IT leaders to apply and control repeatable activities anywhere, anytime—easier than ever. In a recent article on CIO.com, Bernard Golden explains:

> *The key thing to understand about cloud computing is that it substitutes automation for manual effort. Instead of doling out work to a system administrator, who then manually completes the task and makes the resource available, cloud computing uses resource [application program interfaces (APIs)] and an orchestration engine to drive the same task.*[1]

Here are some real-world examples of how leading companies get the results they need from automation enabled by the cloud.

CASE STUDY NO. 1: SAP SYSTEM COPY AND FINANCIAL CLOSE AUTOMATION IN THE CLOUD

SAP AG, the world leader in enterprise software applications, provides solutions that run businesses of every description. To support any SAP-enabled enterprise, the company recommends conducting a system copy process at several stages of its life cycle. Most enterprises perform a system copy regularly to create test, demo and training systems. Also, a company may need to conduct a system copy if it changes its operating system and/or database and requires a migration of its SAP® system.

This process, although critical for stability and improvement, can be time consuming and difficult—especially if it is conducted manually. At one large, international media company, an outsourced SAP system copy process created problems that led IT leadership to automate it—and greatly improve it—using a cloud-based service.

The SAP manual system copy process originally took up to eight days to complete. It was an extremely hands-on process for which an outsourcer charged a hefty sum. Manual errors plagued the process and it often had to be repeated when the results were not optimal. This, of course, cost the media firm more time and money every time a problem occurred. The company needed a way to support the system copy process accurately, quickly and effectively without requiring a massive manual effort, incurring high cost or being subject to so many errors.

Another area the organization struggled to improve was the financial close. Corporate leadership had little visibility into this process as it occurred. Problems were often only found after the entire process had run. Like system copy, the financial close involved a lot of manual tasks and interdepartmental communications between an outsourcer and the media company to keep it moving. It was difficult to manage and expensive to do, and it lacked transparency.

The media firm explored its options and found that automating both processes using a cloud-based service would give it the speed, accuracy and overall quality it required. It also enabled the organization to monitor the processes more closely than before, because the processes themselves no longer needed to be outsourced. Automation was provided as a service that corporate and IT leadership could monitor and control autonomously. Since it was a service, it did not require additional IT resources to keep it working. Because it was delivered through the cloud, it was quick to implement and could be used across technologies, corporate silos and physical locations.

As the company began to convert from manual, outsourced processes to cloud-based automation, it noticed a rapid change. It dramatically reduced the time it took to run a system copy to a fraction of the original eight-day window. The financial close took half the time, and stakeholders could all know where the process was at any point simply by checking a web-enabled monitor. The company saved tremendous amounts of time and money while it enabled more thorough analysis of the processes and continuous improvement.

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:

CASE STUDY NO. 2: CLOUD AUTOMATION FOR THE SUPPLY CHAIN

An international electronic parts provider needed to coordinate core supply chain tasks—including inventory processes, order-taking, order-to-cash and delivery fulfillment—from many different and disparate applications across several global time zones. The company originally relied on a traditional, local software-based job scheduling tool to coordinate the processes from order to fulfillment, but this came with significant risk and limitations.

The process ran with a required 24-hour latency built-in, which made it slow. Also, aligning processes across various platforms was a complex manual procedure, which made it even slower. Any task changes resulted in even more time delays and costly manual fixes. This led to poor response time and customer service issues. This, in turn, began to limit the company's business growth. The company found that regardless of the time, manpower and funds it invested to improve its situation, it could not achieve the consistency and visibility it needed to coordinate operations on a global scale. Corporate leadership looked for a solution.

This organization started its transformation by implementing a cloud-based automation service to connect and coordinate every step in the supply chain and order fulfillment process. Almost instantly stakeholders could monitor, control and manage every step of the supply chain, including stock replenishment, price refresh, stock take, ordering, invoicing and order-to-pack.

> "Automation delivered as a service through the cloud gives business and IT the flexibility and power they need to grow."

The order-to-pack cycle that originally took at least 24 hours was now completed in less than 20 minutes. Web orders were processed in three minutes. The company quickly eliminated manual processes and streamlined operations. It developed a consistent task automation template for all countries that accommodated global time zone functionality—with much less effort than before.

The firm cut operational and administration costs while it reduced expenses from outsourced processes. In the end, the total cost of the cloud-based solution was far less than the price of maintenance for its original job-scheduling tool. It was also more scalable, flexible and easily connected to any application within the enterprise. The company has now successfully expanded the business on a global scale and plans on implementing cloud-based automation wherever it finds repeatable processes.

CONCLUSION

These are just two examples of how automation delivered as a cloud service has started to revolutionize the way companies use automation to their advantage. This approach provides a new perspective on infrastructure and process efficiency wherever it is applied. As with cloud storage, computational power, sharing applications and information, automation delivered as a service through the cloud gives business and IT the flexibility and power they need to grow without worrying about the usual software or infrastructure challenges. In the next few years, companies will continue to use the cloud to run every process faster, more accurately and with more control.

ENDNOTES

[1] Golden, Bernard; "Why Cloud Computing Offers Affordability and Agility," CIO.com, 18 June 2013, *www.cio.com/article/735074/Why_Cloud_Computing_Offers_Affordability_and_Agility?page=1&taxonomyId=3024*

Understanding the Cybercrime Wave

Tommie Singleton, CISA, CGEIT, CPA, is the director of consulting for Carr Riggs & Ingram, a large regional public accounting firm. His duties involve forensic accounting, business valuation, IT assurance and service organization control engagements. Singleton is responsible for recruiting, training, research, support and quality control for those services and the staff that perform them. He is also a former academic, having taught at several universities from 1991 to 2012. Singleton has published numerous articles, coauthored books and made many presentations on IT auditing and fraud.

The fact is that cybercrime has superseded much of organized crime in the past few decades. There are still gangs—organized gangs—but they are considerably different. First, the gang members are not geographically in the same place frequently. Second, they are likely to be international in nature. Third, the gang relies on technology skills rather than brute force or trickery to perpetrate its crimes. Fourth, while the gangs are usually still after money in the end, the means to get there is significantly different from the past. Because of their scope and level of risk (the danger of a serious malicious attack), as compared to a few years ago, cybercrimes could be viewed as a crime wave in recent years.

First, the term "cybercrime" needs to be defined using a definition that is widely and generally accepted. According to one authoritative source, cybercrimes (or cyberattacks) generally refer to criminal activity conducted via the Internet.[1] Examples of cybercrimes include stealing an organization's intellectual property (IP), confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the Internet, and disrupting a country's critical national infrastructure.[2]

In February 2013, 178 million Americans watched 33 billion online videos.[3] This statistic reflects the value of intellectual property available on the Internet in movies alone. For example, Netflix is paying Disney and Epix a total of US $350-400 million a year in licensing fees for content.[4]

Next, all IT auditors need to grasp the scope of this problem. According to the Ponemon Institute, the average annualized cost of cybercrime for respondents to its 2012 survey was US $8.4 million globally, US $8.9 million inside the US.[5] This is an increase of 6 percent from the last survey. The respondents also report that they experienced 1.8 successful attacks per week per entity, an increase of 42 percent from 2011.[6] The survey results show a positive relationship between size and annualized cost of cybercrimes. However, smaller organizations had a significantly higher *per capita* cost (US $1,324) than larger organizations (US $305). Statistics such as these indicate that cybercrimes are on the increase.

Finally, the IT auditor needs to understand the phases or components of a cybercrime attack. First, there is the tool or tools used by the cybercriminal, including a denial-of-service (DoS) program, a virus and a Trojan. Next is the delivery methodology. The term used for the delivery methodology is vector. Examples of a vector are phishing emails, drive-by web sites, vulnerabilities that allow unauthorized access to systems or data, and advanced persistent threats (APTs). Finally comes the purpose or objective of the cybercriminal—the crime. Examples include theft of IP, theft of funds or disruption of systems.

Cybercriminals are often external to the victim, but according to the Ponemon Institute, one of the three most costly attacks is associated with malicious insiders.[7] A typical insider cybercrime would be an employee stealing funds via automated clearinghouse (ACH), electronic funds transfer (EFT) or wire transfer. Ultimately, organizations must protect themselves from external and internal threats and risk.

The basics to be understood about cybercrime include the types of potential losses (who the victims are, what gets stolen and how victims suffer), basic remediation, trends and resources.

TYPES OF POTENTIAL LOSSES DUE TO CYBERCRIMES

Who Are the Cybercriminals' Victims?

The nature of the victims of cybercriminals is generally a function of whether a person or entity has something the cybercriminals can steal that will satisfy their goal, which is usually money (see **figure 1**). So, naturally, a favorite target victim is the financial institution. Part of that is driven by the fact that financial institutions

are warehouses for money, but they are also a favorite target because a common scheme of the cybercriminal is falsifying debit/credit cards. There is also a growing number of DoS attacks on banks to disrupt banking services and the financial infrastructure of the US.

Figure 1—Verizon 2013 Breach Report	
Targets	**%**
Financial	37%
Retail trade	24%
Manufacturing, transportation and utilities	20%
Professional services	20%
Larger organizations	38%
Source: Verizon, "2013 Data Breach Investigations Report," 2013	

This leads to another favorite target of cybergangs: anyone who has large files of debit/credit card data, such as financial institutions and retail trade. The 2007 T.J. Maxx breach led to the theft of more than 45 million debit/credit card numbers and US $100 million in fraudulent charges. The case, prosecuted by the US Department of Justice, was supposedly the largest to date for hacking and identity theft. Eleven conspirators were accused of hacking into unsecured wireless networks of a very large set of retail chains. A similar event occurred with the CardSystems Solution breach. In that case, about 40 million credit cards were exposed to the hacker. The point is, where there are millions of debit/credit card data bytes, cybercriminals are attracted. But they may also be attracted to thousands of card data bytes in small and medium-sized enterprises (SMEs) where the data may not be encrypted or are otherwise unsecured.

For those in government, there is a specific threat from cybercriminals: nation-state-sponsored terrorism and attacks. It is reported that some governments are hiring full-time hackers to attack government data, content and IP (e.g., weaponry) and to attack businesses as well (with the same target of data/content/IP). This situation presents a difficult and dangerous challenge for those tasked with protecting the data, content and IP from such threats on behalf of a government agency.

Some cybercrimes target SMEs because of the lower likelihood that those organizations would have adequate information security controls to prevent the crime. For instance, a corporate account takeover cybercrime[8] is focused on SMEs. Thus, if the auditee is an SME, it has some risk associated with corporate account takeover and other schemes targeting SMEs and the IT auditor should be in a position to assist management in trying to defend itself against such attacks.

What Do Cybercriminals Steal?

Cybercriminals are after almost anything that is of value in the current crime world (see **figure 2**). Sometimes the target is related to eventually stealing funds. Sometimes it is about causing harm to an entity. Sometimes it is to gain fame and possibly recognition that will lead to a high-paying job. But usually, the eventual objective is to steal money.

That objective could be met by stealing an individual's or entity's bank credentials. It could be more sophisticated by involving personally identifiable information (PII), which can be used to open false accounts, loans and other methods of impersonating someone for illicit financial gain.

Figure 2—Illustrative List of What Cybercriminals Steal and Why	
Initial Target	**Immediate Objective**
Bank credentials ACH/EFT/wire transfer access	• Access bank funds and steal them.
PII	• Open credit card accounts. • Apply for loans. • Access medical treatment. • Access utilities.
Debit/credit card data	• Access victim's credit. • Sell data on the black market.
IP/data/content	• Gain a hostage or blackmail. • Sell to competitors. • Avoid paying for IP. • Disrupt/sabotage an entity. • Access confidential business information.

A more direct path is to steal debit/credit card data that can either be skimmed onto a blank or discarded credit card and used to access the victim's credit, or can be used online to buy any variety of things that the criminal could then turn around and sell or use. Debit/credit card theft is sometimes the end objective of stealing PII.

While the first three cybercrime objectives in **figure 2** are fairly well known, the last one does not seem to draw as much attention: IP, data and/or content. IP has an immediate value to the criminal. But cybercriminals continue to invent ways to get money related to data and content. One new method is the cryptolocker virus.

The cryptolocker virus scheme works as follows: The cybercriminal infects an entity's computer system with the cryptolocker, usually via a phishing email or drive-by web site. The virus then generates a private and public key and proceeds to encrypt all of the data on a server or network. Then, the cybercriminal sends what is basically a hostage message saying he/she will provide the private key for US $300-$500, knowing that it will cost much more to get the data back, even if the entity does have an effective business continuity plan (BCP) including current backups of data. The problem is, if the cybercriminal is able to infect an entity's system once, what is to prevent him/her from doing it again? And what other malware did the cybercriminal place on the system before executing the cryptolocker virus? No matter what the victim decides, the entity will need serious and costly entitywide security changes.

Sometimes a cybercriminal is out for nonmonetary satisfaction. For instance, those who employ DoS or distributed DoS attacks do not receive monetary gain; instead, they desire high-profile attention. Other objectives might be distributing a virus (for a similar fame objective) or disrupting a government infrastructure or private service (e.g., a major web site).

What Are the Damages From a Cybercrime?

It begins with the end game—loss of funds, usually from a financial institution's account. Sometimes that is stolen directly (e.g., corporate account takeover, ACH/EFT/wire transfer frauds), and other times it is taken indirectly—stealing the victim's identity and opening accounts.

There is also the collateral damage from the attack, which is twofold. First, the entity has likely suffered some damage or loss to data or systems. There is a cost to recover or restore data, systems or computerized services. For example, in the cryptolocker virus, once the data are encrypted with a public/private key, the entity must spend resources to recover the data—whether by restoring a backup or paying a ransom. Second, a breach in the entity's systems has been exploited.

Whether or not the entity knew about it before the attack, following an attack, it is in the entity's best interests to fix the security problem to prevent it from occurring again. The cost of such security fixes can be significant.

Collateral damage can come in other forms as well, for example, local or regional fines or penalties and the costs associated with complying with laws. Further, if the entity suffers loss of debit/credit card data or PII of customers, the customers may sue the victim in court for damages. Finally, there is the damage to the public image of the victim. Once the public finds out that customers had their debit/credit card data or PII stolen from a particular entity, others may think twice about doing business with that organization.

HOW TO DEFEND AGAINST CYBERCRIMES: THE POINT OF ENTRY

Like so many audits IT auditors perform, the best way to defend against cybercrimes is to conduct an effectual risk assessment. That process should lead to the identification of a risk ranking. Once that process is completed, the entity must set a threshold of risk, addressing those risk areas at or above that threshold.

While it may be an oversimplification, the remediation starts with understanding where the original point of entry is for identified risk and finding an effective remediation to prevent and detect an intrusion. For instance, on a corporate account takeover, the point of entry is when the cybercriminal attacks (purposely and individually selected) an accounting officer with a phishing email or drive-by web site. Thus, one possible solution is to have a computer dedicated to online transactions (ACH, EFT and wire transfers) that never accesses email or the web.

Another key to remediation is to understand the tools and vectors that have a high risk for the auditee and think through how to remediate that particular tool or vector. Fortunately, there are a lot of resources available to IT auditors.

CYBERCRIME TRENDS

There are some facts over the last few years that show some trends in the current crime wave. First, cybercrimes have gone from broad-based attacks, such as mass-phishing emails, to targeting victims, such as in spear phishing. Yet, cybercrime goes beyond spear phishing. The corporate account takeover crime scheme is based on targeting the victim with specificity. One factor in this targeting is the fact that these techno-gangs are often targeting SMEs because they believe SMEs are likely to have less information security in place than a larger business. Similar targeting takes place in the theft of debit/credit card data. Cybercriminals are targeting the card processors, banks and other entities that are likely to have files with thousands, if not millions, of card data bytes. While these institutions are large, the technical skills of criminals such as Albert Gonzalez (T.J. Maxx breach) demonstrate just how savvy these criminals are when it comes to IT; he stole almost 200 million debit/credit cards in a span of four years using sophisticated IT techniques and tools.[9] Another example is the advanced persistent threat (APT) vector. It is referred to as "persistent" because the cybercriminal identifies a specific target and then hammers at that target over and over to perpetrate the desired cybercrime.

RESOURCES FOR CYBERCRIME REMEDIATION

ISACA has a wealth of resources available on this subject, including frequent articles and a column (Information Security Matters by Steven J. Ross) on the subject in the *Journal*. It also has books, webinars and conferences on the topic.

There are also plenty of best practices that can be found with a search engine for specific aspects of cybersecurity (e.g., logical access controls, passwords, firewalls, BCP, encryption). And there are a number of reliable reports, standards and frameworks available from authoritative sources, many of which are updated annually:

- Microsoft Security Intelligence Report
- Verizon Data Breach Investigations Report
- Ponemon Institute (various reports on cybersecurity)
- Govinfosec web site
- The Business Model for Information Security (BMIS) from ISACA
- US National Institute of Standards and Technology (NIST) standards

CONCLUSION

The evidence supports that a new crime wave has begun in recent years: cybercrime. It is no longer a question of *if* your organization will be attacked, but *when* it will be attacked. The costs of cybercrimes are significant in a variety of ways.

For IT auditors to be prepared to respond to the risk, they need to understand how a cybercrime is perpetrated: one or more tools, one or more vectors, and the final result (the crime). To conduct an effective risk assessment regarding cybercrimes, the IT auditor needs to understand who the victims are likely to be, what is likely to be the object of the cybercriminal and the potential damages that could result from various cybercrimes.

The most costly attacks are those associated with DoS, malicious insiders and web-based attacks.[10] Mitigation for such attacks requires enabling technologies such as security incident and event management (SIEM); intrusion prevention systems; application security testing; and enterprise governance, risk management and compliance (GRC) solutions. The loss or misuse of information is the most significant consequence of a cyberattack.[11]

All that said, the good news is there are remediation solutions. And there is a wealth of resources to aid IT auditors in defending their organizations against this crime wave. However, it will take education and some diligence in developing controls and defenses to thwart cybercrimes.

ENDNOTES

1 Ponemon Institute, "2012 Cost of Cyber Crime Study: United States," October 2012

2 *Ibid*.

3 comScore, "comScore Releases February 2013 U.S. Online Video Rankings," 14 March 2013, *www.comscore.com/Insights/Press_Releases/2013/3/comScore_Releases_February_2013_U.S._Online_Video_Rankings*

4 Seeking Alpha, "Netflix: Rising Content Costs Stump Growth," 1 February 2013, *http://seekingalpha.com/article/1150191-netflix-rising-content-costs-stump-growth?source=google_news*

[5] *Op cit*, Ponemon Institute. The sample was of 56 organizations in various industry sectors in the US, but many are multinational firms.

[6] For an example of IP cybercrime, research the "Megaupload" case and its founder, Kim Dotcom, who was arrested in January 2012 on cybercrime charges.

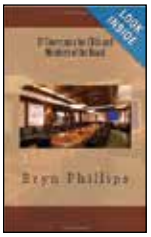
[7] *Op cit*, Ponemon Institute

[8] The corporate account takeover generally follows this pattern: A cybergang identifies a target, an SME or small to medium-sized government agency. It then targets an accounting officer who is likely responsible for online banking, particularly ACH/EFT/wire transfers. It sends a phishing email to that person in hopes of infecting his/her computer with a Trojan. It steals banking credentials from that person. It sets up money mules to handle stolen cash. It uses a tool to grab control of the infected computer and log onto the bank account from the accounting officer's own computer using his/her credentials. The bank's system of controls suspects nothing. The criminals begin to transfer funds out of the bank about US $10,000 at a time to money mules, until the account is empty. The money mules keep a fee (usually about 5 percent) and send the rest on to the gang's main bank in a distant country.

[9] *Miami Herald*, "Identity Theft: Miami Hacker Cyberthief of the Century?," 23 August 2009

[10] *Op cit*, Ponemon Institute

[11] *Ibid*.



By Bryn Phillips

Reviewed by Ibe Kalu Etea, CISA, CRISC, ACA, CFE, CRMA, ISO 9001:2008 QMS, a corporate governance, internal controls, fraud and enterprise risk assurance professional. He also serves as a member on the advisory council of the Association of Certified Fraud Examiners (ACFE).

IT Governance for CEOs and Members of the Board

The evolving dimensions of compliance matters, IT management performance, risk frameworks and corporate governance models have created a huge knowledge gap between IT-savvy executives and nontechnical corporate business leaders. Often the process of justifying IT investments by a chief information officer (CIO) or designate to his/her board tends to be an uphill task, even for such critical items as spending on business continuity and disaster recovery systems. This has necessitated requirements for even-toned publications that create an easy path for non-IT board and senior executives to quickly grasp the salient issues related to IT governance in an easy read.

IT Governance for CEOs and Members of the Board lays an interesting foundation that will appeal to all types of board directors, putting nascent IT governance requirements in focus with the right degrees of detail. Creating a balance between detail and depth, the author, Bryn Phillips, addresses governance, compliance and risk issues with relevant reference to risk frameworks such as COBIT, ITIL and King III.

Simplifying the broad concepts of governance at the board level, Phillips deciphers the synergies between IT governance terminology and board decision-making activities from the strategic to operational domains. This fine balance between strategy and implementation in a pragmatic style should endear this book to a diverse array of executives and professionals who should not have to undertake IT courses to get the crux of modern IT governance issues.

The book is written in a simple, narrative style, ensuring that readers' interests are stimulated page after page. Further still, the book does not deviate from its primary focus: introducing the critical relevance and requirements of IT governance in modern business models. The fact that it is a basic reference book that is suitable for a nontechnical audience does not strip its value, as it applies current trends in IT governance to the boardroom, which is the source of IT investments. As a result, it is also a good reference for IT practitioners on how to present their viewpoint to less technology-focused senior stakeholders.

The book commences with an easy-to-understand definition of IT governance, summarizing some key frameworks in a fairly straightforward manner. Elements of IT governance are then explained, and the importance of sustainability and green IT as an emerging corporate social responsibility (CSR) initiative is explained in a practical, thought-provoking manner.

The rest of the book serves as a reminder of the connection between the US Sarbanes-Oxley Act, and other similar legislation worldwide, and IT governance, touching on the key sections of the framework and the application of IT technology from a controls and risk mitigation standpoint to Sarbanes-Oxley implementation.

The ordering of the book's chapters takes a seminar-type approach in which the reading audience is keenly involved with end-of-chapter to-do actions for board members and decision makers and to-demand requirements for CIOs and other key stakeholders of an enterprise.

This involved, hands-on approach in communicating a rather technical subject to a diverse audience results in a simple and excellent reference for nontechnical corporate stakeholders and boards.

EDITOR'S NOTE

IT Governance for CEOs and Members of the Board is available from the ISACA Bookstore. For more information, see the ISACA Bookstore Supplement in this *Journal*, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

Big Data: A Revolution That Will Transform How We Live, Work, and Think

By Viktor Mayer-Schonberger and Kenneth Cukier

Reviewed by Upesh Parekh, CISA, a governance and risk professional with more than 10 years of experience in the fields of IT risk management and audit. He is based in Pune, India, and works for Barclays Technology Centre, India. He can be reached at *upeshparekh@hotmail.com.*

In today's digital age, there is an explosion of data everywhere. Google processes more than 24 petabytes of data per day. Data bytes are being generated every minute—from the mobile call to a loved one at the end of the day to buying groceries for the month. How are these data bytes being used?

Some of the leading companies in the world and entrepreneurial start-ups are making good use of these data. They are being used to arrive at shocking and seemingly innocuous conclusions like "a car painted orange is highly likely to be in good shape for a used car deal" or when airline ticket prices are going to be favorable to the buyer.

Big data is considered to be the next hype cycle. It is claimed to be the biggest development since the Internet, promising to turn the world upside down. *Big Data: A Revolution That Will Transform How We Live, Work, and Think* explains the concept of big data, the impact it has made, the changes in mind-set it will require and the flipside of its incorrect application.

Written by Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* is shortlisted for the *Financial Times* and Goldman Sachs Business Book of the Year Award. It is full of examples, stories and anecdotes, which make it a very interesting read. It is a business book demonstrating the value IT can bring to the business.

Until now, business has been blinded by a couple of limitations while making decisions: nonavailability of data and a lack of processing/computation power to process large amounts of data. With increasing digitization, declining costs of computational power and development of tools capable of organizing large amounts of data, an altogether new insight is available for decision making.

With the insight provided by big data, companies can make many business decisions such as what should be stocked next to a torch when a hurricane is forecasted in a big market and health authorities can be alerted about possible outbreaks of diseases in a particular geography.

The application and power of the concept is unlimited. Election results in a democratic country can be forecasted. Expenditure patterns of any individual or section of individuals can be predicted. Vehicle traffic on a road can be anticipated and, in an agriculture economy, big data can estimate rainfall by manipulating numerous data points.

However, some old concepts will have to be shelved to make effective use of big data. Correlation is just one such concept. Our mind is tuned to establish the causal effect. This fixation with causality needs to be reduced because in a big data world, *why* is not important so long as *what* is established. For example, one would not be able to establish why orange cars are in better shape than other cars.

These amazing predictions, forecasts and insights are based on the analysis of vast amounts of data. That said, these data were not shared or intended to be used for these purposes. Thus, the concept of big data gives rise to the issue of data privacy. One's digital life has given to the outside world a window into one's life, and the power of big data is correlating this view of a person's life with many other data points, of which one is not even aware, resulting in possible views of one's innermost thoughts, which one may not want to share. This risk needs to be considered and the control environment needs to adapt to it.

There are other perils to big data as well, which are elaborated on in *Big Data: A Revolution That Will Transform How We Live, Work, and Think.*

EDITOR'S NOTE

Big Data: A Revolution That Will Transform How We Live, Work, and Think is available from the ISACA Bookstore. For more information, see the ISACA Bookstore Supplement in this Journal, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

Feature

SCADA Cybersecurity Framework

Samir Malaviya, CISA, CGEIT, CSSA, works with the Global Consulting Practice-GRC practice of Tata Consultancy Services and has more than 17 years of experience in telecommunications, IT, and operation and information risk management. Malaviya is currently leading an engagement for a large investment bank in New York, USA. Malaviya can be reached at *samir.malaviya@tcs.com* or *samir.malaviya@gmail.com.*

Supervisory control and data acquisition (SCADA) systems are rapidly changing from traditional proprietary protocols to Internet Protocol (IP)-based systems. Modern IP-based SCADA systems are now inheriting all the vulnerabilities associated with IP. Attempts are being made to fight new threats to SCADA systems by players in the industrial world; however, the current approach is frequently reactive or compliance-based. This article proposes a comprehensive model for establishing a framework for securing SCADA systems. The proposed framework's components are aligned to existing IT security best practices—keeping in mind the challenges and requirements unique to SCADA systems.

The current trend in SCADA is Transmission Control Protocol/Internet Protocol (TCP/IP)-based systems. This is a huge transformation from traditional proprietary protocols. The advantage of TCP/IP in terms of cost-efficiency, effectiveness and interoperability will accelerate the inevitable trend of adoption of TCP/IP for SCADA. Since vulnerabilities in TCP/IP are widely known, governments and the general public are becoming more and more concerned about various doomsday scenarios of large-scale cyberattacks. Federal governments and industry bodies are reacting to these threats by prescribing various regulations and standards. Cyberthreats are evolving while some of the compliance programs in place provide only point-in-time snapshots of security postures of organizations.

SCADA SYSTEMS

Most critical infrastructure, including major utilities infrastructure, industrial networks and transport systems, are controlled by SCADA systems. SCADA systems are smart, intelligent control systems that acquire inputs from a variety of sensors and, in many instances, respond to the system in real time through actuators under the program's control. The SCADA system can function as a monitoring/supervisory system, control system or a combination thereof.

SCADA VS. IT SECURITY REQUIREMENTS

Moving to IP-based systems provides tremendous economic advantages in a time of intense competition. Consequently, more and more systems are expected to move toward IP-based systems. For example, the advantages of migrating from a proprietary radio-based network to an IP-based network include shared network resources across multiple applications, network improvements such as added redundancy and capacity across all applications, shared network management systems, and having to maintain only one skill set for onsite support staff. However, all known vulnerabilities and threats associated with traditional TCP/IP are available for exploitation, making it a challenge for the SCADA security community. Although all risk factors associated with IT systems apply to SCADA systems, it is not possible to completely superimpose an IT security framework on SCADA systems. **Figure 1** describes the potential differences between IT security and SCADA security.

GOVERNING SCADA SECURITY

Industry organizations are developing standards for their vertical industries. These include, for example:

- **Electric:** North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- **Chemicals:** Chemical Industry Data Exchange/American Chemistry Council (CIDX/ACC)
- **Natural gas:** American Gas Association 12 (AGA 12)
- **Oil and liquids:** American Petroleum Institute (API)
- **Manufacturing:** International Society for Automation/International Electrotechnical Commission (ISA/IEC 62443) (formerly ISA 99)

Figure 1—SCADA Vs. IT Security		
Category	**Information Systems**	**Control Systems**
Risk impact	• Loss of data	• Loss of life, production
Risk management	• Recover by reboot • Safety a nonissue	• Fault tolerance essential • Explicit hazard analysis expected
Reliability	• Occasional failures tolerated • Beta test in field acceptable	• Outages unacceptable • Quality assurance testing expected
Performance	• High throughput demanded • High delay and jitter accepted	• Modest throughput acceptable • High delay a serious concern
Security	• Most sites being insecure • Little separation among intranets on same site • Focus on central server security	• Priority to functionality and reliability • Tight physical security • Information systems network integrated with plant network • Focus on central server as well as edge control device stability
System operation and change management	• Generic, typical operating systems • Straightforward upgrades • Changes using automated deployment tools	• Proprietary operating systems • Software changes in consultation with vendors only
Communications	• Standard communications protocols • IT networking practices	• Mix of proprietary and standard communication protocols • Networks requiring the expertise of control engineers
Component lifetime	• Lifetime on the order of three to five years	• Lifetime on the order of 15-20 years

Some governments have come up with their own regulations and standards, e.g., the US National Institute of Standards and Technology (NIST), the UK Center for Protection of National Infrastructure (CPNI) and The Netherlands Center for Protection of National Infrastructure (CPNI).

However, compliance to standards/regulations does not guarantee continuous security, but it does provide a snapshot of required controls at a point in time.

As new threats are identified almost daily, SCADA systems require a dynamic risk-based approach to keep pace with evolving threat scenarios.

IT security and risk professionals who have worked in traditional areas such as banking, finance or telecommunications are facing the same challenges of continuously evolving threats and risk. Most traditional IT security frameworks are modeled on standards/guidelines from ISACA, NIST or the International Organization for Standardization (ISO).

CONSTRUCTS OF A SCADA SECURITY FRAMEWORK

An ideal SCADA security framework should have the following characteristics:

- Comprehensive and evolving to meet a changing threat profile
- Meets the availability requirements of SCADA systems
- Meets the risk management and performance requirements typical of SCADA systems
- Scalable to meet different standards and regulations as applicable

The proposed SCADA security framework can be subdivided into the following areas:

1. **Governance, risk and compliance administrative controls**—Utilized for setting up the rules of engagement; includes policies, standards, exception management, and risk and compliance frameworks. Because these controls are not technical in nature, they are often described as administrative controls.

2. **SCADA controls**—This area is designed to cater to specific SCADA requirements. Some of the SCADA security requirements are specific to the SCADA world.
3. **Data and application security**—SCADA data, proprietary applications development and maintenance are covered in this area. One of most important areas covered here is change management.
4. **System assurance**—This area covers unique SCADA security requirements such as system resilience and secure configurations.
5. **Monitoring controls**—As SCADA protocol and applications are weak by design, monitoring becomes one of the important areas of the SCADA security framework.
6. **Third-party controls**—Most SCADA systems are supplied by third parties, including vendors and partners, necessitating a separate area for third-party security in the SCADA security framework.

These areas of the SCADA security framework further expand into 22 subsections. The six areas and underlying 22 subsections are presented in **figure 2**.

ADMINISTRATIVE CONTROLS

Controls that are not implemented using tools and technology are defined as administrative controls. The GRC framework is covered here. The following subsections are included in this area:

1. **Organizational leadership and security organization**—Organizational leadership takes complete ownership of SCADA security and sets the direction at the top to provide the necessary funding, structure and buy-in for the SCADA security program. Without involvement of organizational leadership, important programs such as the SCADA security program cannot succeed. Security organization refers to setting up the SCADA security organization with clearly defined roles and responsibilities.
2. **Policy, standards and exceptions**—The "rules of the game" are set by the policies and standards. Policies and standards provide direction to the organization and to the organization's constituents and their expectations. These rules are to be followed by all with the goal to protect the organization. The expectation is to have separate SCADA security policies and standards to complement the organization's policies and its IT security policies. Deviations from policies and standards are recorded as exceptions. In the SCADA world, availability and stability are the most important criteria to be considered. Deviations, such as security controls not being implemented on time, need to be recorded as an exception, and necessary compensatory controls need to be implemented.
3. **Risk assessments**—The risk profile of an organization is gauged using this important tool, available to management. Risk assessments also help an organization to dynamically respond to emerging threats and risk at periodic intervals.
4. **Compliance framework**—Most of the industries where SCADA systems are in use are heavily regulated. A well-designed compliance framework allows an organization to meet its compliance requirements seamlessly.

Figure 2—SCADA Security Framework

Administrative Controls	SCADA Controls	Data and Application Security	System Assurance	Monitoring Controls	External Controls
Organizational leadership and security organization	Asset management	Data security	System resilience	Incident management	Vendor security management
Policy, standards and exceptions	Identity and access management	Application security (development and maintenance)	Secure configuration	Threat monitoring	Partner security management
Risk assessments	Vulnerability management	Change management	Business continuity and disaster recovery planning	Forensics	
Education and training	SCADA network security controls	Malicious code detection/prevention			
Compliance framework	Physical security				

SCADA CONTROLS

As described in **figure 1**, IT risk and SCADA security have different priorities and requirements. Some of the unique requirements for SCADA cybersecurity are:

1. **Asset management**—Identification and classification of SCADA assets and specifically SCADA cyberassets are covered by this area.
2. **Identity and access management**—Account administration, authentication and authorization, password management, and role/attribute-based access to SCADA systems are covered by this area.
3. **Vulnerability management**—The majority of SCADA systems are supplied by vendors. SCADA systems are built on popular operating systems (OSs), such as Windows, and use TCP/IPs, which are inherently insecure. However, there are unique challenges faced by SCADA, including availability requirements, performance requirements and low bandwidth associated with SCADA systems. Vulnerability management in SCADA needs to be treated as a separate discipline, distinct from vulnerability management associated with IT in general.
4. **SCADA network security controls**—The SCADA network needs to be protected from other networks including the corporate network. The controls that help in achieving the goal of securing a SCADA network are covered by this subsection.
5. **Physical security**—SCADA systems are often connected and spread across wide areas. Remote technical unit (RTU) devices are often placed at a long distance from programming logic controller (PLC)/SCADA control centers. This is a unique challenge for physical security in the SCADA security framework.

DATA AND APPLICATION SECURITY

Well-known incidents such as Stuxnet and Flame have created widespread interest in SCADA data and application security. This area's subsections include the following controls for data, application, change management and malicious code detection/prevention controls:

1. **Data security**—SCADA data are often communicated in open text without encryption. Although confidentiality is not a top priority for SCADA, integrity and availability are of concern for SCADA security professionals. Data security covers availability, integrity and confidentiality controls associated with the protection of data.
2. **Application security**—SCADA applications present a unique challenge for security professionals. SCADA applications are often developed by third-party vendors that have provided SCADA hardware devices. These applications are often built without following standard system development life cycle (SDLC) processes. Security is not a priority for SCADA application developers, whose only priority often is making the system work. The scope for SCADA security developers is to provide secure guidelines to vendors and to teams evaluating the purchase of new SCADA devices, and to complete static/dynamic analysis and penetration testing. SCADA security professionals are expected to provide guidelines to application security professionals as the approach for SCADA vulnerability testing/pen testing needs a different approach than traditional IT testing.
3. **Change management**—The challenge in change management for SCADA is to ensure that change does not disrupt the functioning of devices, as often the impact can be the threat of loss of life. Due to this, change management is another uniquely challenging field for SCADA security professionals.
4. **Malicious code detection/prevention**—Malicious code including a virus/malware/trojan can be extremely harmful to SCADA systems and underlying infrastructure. It is important to protect applications from malicious codes.

SYSTEM ASSURANCE

The foremost priority for SCADA systems is to ensure availability of systems. With this goal in mind, the following subsections are covered in this area:

1. **System resilience**—Ensuring that SCADA systems are always available requires the system to be designed with a resilience goal in mind. System resilience includes designing resilient architecture for SCADA systems, ensuring goals are met during normal operations, incidents and changes to systems.
2. **Secure configuration**—SCADA systems and the communication protocols are inherently insecure. Ensuring underlying systems are built securely is of paramount importance. System hardening/patches are covered by this subsection.
3. **Business continuity/disaster recovery planning (BCP/DRP)**—Systematic and orderly recovery from disasters and business continuity processes is covered by this subsection.

MONITORING CONTROLS

As described earlier, SCADA applications and protocols are inherently insecure. Other known issues with SCADA systems are the following challenges associated with applying patches—a result of which is monitoring compensatory controls:

1. **Incident management**—Established and documented incident management processes are the keys to ensuring orderly handling of incidents. Most regulations also stress efficient processes for incident management and incident reporting.
2. **Threat monitoring**—SCADA applications and protocols are inherently insecure; lack of awareness and dependency on vendors for applying patches, wide area networks and the need for segregation for SCADA networks make threat monitoring one of the most important sections in SCADA security controls. Often, monitoring is used not only for detection and prevention, but in many cases, it is also applied as a compensatory control.
3. **Forensics**—Often SCADA system breaches have serious impact on an entire geographic area. Forensics helps in unearthing and establishing incidents.

THIRD-PARTY CONTROLS

Third-party vendors often supply SCADA systems. For SCADA security professionals, controls related to third parties, including vendors and partners, are critical:

1. **Vendor security management**—Vendors play important roles in SCADA. SCADA devices and applications are often supplied by vendors. Many times vendors manage the infrastructure, including IT maintenance, SCADA systems, IT and SCADA networks, and/or managed security service providers. Vendor security is an important area to establish necessary controls over vendors and SCADA security for an enterprise. One control for vendor management is contract management, ensuring security is part of standard contracts and specifications for vendors and reviewing and evaluating vendors for security.
2. **Partner security management**—In today's interconnected world, organizations that rely on SCADA networks are often interdependent. Partner security management, in which rules of engagement between partners are established, caters to this area.

SCADA SECURITY FRAMEWORK USE CASES

The SCADA security framework can be used by organizations to set up their SCADA organization, SCADA security policies/standards and risk control framework, which can be further used for risk assessments and benchmarking the organization's SCADA security.

Organizations can build upon the SCADA security framework to frame short-, medium- and long-term security plans, selecting appropriate tools and technology to secure SCADA networks and devices.

CONCLUSION

SCADA/industrial control systems come with their own unique challenges and require a thoughtful approach for the security community to provide a comprehensive solution to meet security needs in this area. A cybersecurity framework is an important area; however, its implementation is a first step in the journey to establish a reliable and comprehensive cybersecurity solution for SCADA systems. The next steps in this framework include:

1. Creation of controls mapping to each subsection with clearly measurable goals
2. A maturity model for benchmarking organizations' SCADA security posture
3. A technical implementation blueprint

An ideal implementation of the SCADA security framework would include a GRC tool, an identity access management (IAM) tool set, network segmentation and security monitoring—a sound recipe for continuous control monitoring.

REFERENCES

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), *www.nerc.com/page.php?cid=2%7C20*

PCSF Congress of Chairs, *Cyber Security Combined Glossary Project*, "AGA 12 Series," *http://ics-cert.us-cert.gov/practices/pcsf/groups/d/1176393761-combined_glossary_2007_03_28.pdf*

Phinney, Tom; "ISA/IEC 62443: Industrial Network and System Security," International Society for Automation/International Electrotechnical Commission, *www.isa.org/autowest/pdf/Industrial-Networking-and-Security/Phinneydone.pdf*

UK Center for Protection of National Infrastructure (CPNI), *www.cpni.gov.uk/advice/cyber/Critical-controls/*

National Institute of Standards and Technology (NIST), *Guide to Industrial Control Systems (ICS) Security*, NIST SP 800-82, *http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf*

Panetta, Leon; US Defense Secretary speech reference on Industrial Control Security, 2012

Key Considerations in Protecting Sensitive Data Leakage Using Data Loss Prevention Tools

Nageswaran Kumaresan, Ph.D., CISA, CRISC, CGMA, CIA, is a lead IT auditor at General Motors Company (GM) and has significant experience in managing several high-profile global audits within GM, including data loss prevention system implementation and policy enforcement. Before GM, he worked at IBM Consulting, PricewaterhouseCoopers and Deutsche Bank.

Protecting digital assets and intellectual property (IP) is becoming increasingly challenging for organizations. Looming patent challenges and court battles to claim ownership of IP illustrate the importance of protecting IP to gain a competitive advantage. A report by the US Patent and Trademark Office published in 2010 estimated US $5.06 trillion in value added, or 34.8 percent of US gross domestic product (GDP) generated, by IP-intensive industries in the US.[1] In addition, organizations handle sensitive personal, financial and business data, some of which are governed by laws and regulations in local as well as international jurisdictions. Organizations are expected to take adequate measures to protect data from loss or leakage.

Recent studies describe external hacking as the primary cause of data loss in the corporate world;[2, 3] however, organizations have few mechanisms to assess and report data losses through internal sources. Mature technology architectures, such as firewalls, intrusion detection systems, vulnerability scanning and penetration testing, are primarily designed to protect the network from external threats. Capturing internal data loss or leakage requires different architectures focusing on data handling within the organization as well as data outflow. Every day, a large amount of digital data flows outward in the form of email, data uploads, file transfers and instant messages from an organization's networks. Internal data loss threats can be due to insider sabotage of IT, insider theft of IP or sensitive data, insider fraud, or human negligence or error.[4] Large percentages of internal data losses are due to user negligence as opposed to malicious intent.[5, 6] Negligent or accidental data losses by internal sources occur due to poorly understood data practices, lack of effective policies or guidelines, or user error.[7] Data loss prevention (DLP) technology solutions focus on accidental or malicious data losses, primarily from internal sources, by defining policies within the system to prevent or detect sensitive data going outward.

Disponibile anche in Italiano
www.isaca.org/currentissue

DLP technology solutions have evolved in various forms since 2006/2007[8] as a comprehensive corporate approach to prevent, detect and respond to unauthorized dissemination of various sensitive data through an organization's network. DLP has been identified as one of the 20 most critical control requirements for secure organizations.[9] However, recent surveys indicate that DLP technology adoption and use in the industry are low, and often unsuccessful.[10] Surveys have also revealed DLP solutions being implemented only for limited areas, such as web and email monitoring, and not as an integrated solution.[11]

Some common issues are not considered adequately during DLP solution implementation. Ten key considerations that could help organizations plan, implement, enforce and manage DLP solutions, thereby adding value to the organization, are described here.

DLP SOLUTIONS: HOW THEY WORK

DLP solutions use content-level scanning and deep content inspection (DCI) technologies to identify the sensitivity of the content and prevent or block sensitive data from leaving the organization's network. Integrated DLP solutions also support data or media encryption, malware-related data harvesting, monitoring of access to sensitive data storage, and data discovery and classification. Targeted end points, data storage and data transfer gateways are monitored, and certain activities or data movements are blocked by defining and deploying appropriate DLP policies.

Broadly, DLP solutions target activities at three levels:

- **Client level (in-operation)**—Policies are defined and deployed, targeting end points used by employees for their day-to-day business operation. User activities that violate predefined policies are monitored or blocked by DLP agents installed in user end-point terminals.

- **Network level (in-transit)**—DLP policies focus on data movements outside the organization's network. Data transmitted from one location to the other are monitored and, if required, blocked by the DLP system at the network or email gateways. Transmitted data packets are inspected using deep packet-level review techniques to verify the nature of the content in transit. Data transfers using email (SMTP), web (HTTP/HTTPS) and file transfer (FTP/FTPS) are verified against policies to prevent or detect sensitive data leakage.
- **Storage level (at-rest)**—The targets here are the static data stored in servers. Sensitive data stored in repositories are scanned based on specific rules, using crawlers to identify the location and assess the sensitivity of the data and the appropriateness of the location in accordance with the policy. Discover scans are used to classify or tag the files and then monitor their access.

10 KEY CONSIDERATIONS

Based on lessons learned by reviewing previous DLP implementations, these are 10 key considerations that could help organizations successfully implement a DLP solution as a data protection mechanism:

1. **Implement a holistic approach and value proposition for DLP based on a risk assessment**—DLP solutions should be considered as part of an overall information security mechanism and data protection strategy. It is important to understand the existing security architecture and assess how a DLP solution could add protection. The assessment should consider what data the organization wants to protect, the security risk based on the current and future security architecture, the total cost, and value-added benefits of introducing DLP. An objective cost-benefit analysis valuing the cost of data loss, total cost of implementation and management, and potential benefits provides the value proposition for a DLP solution. A DLP value proposition and go/no-go decision should be based on an objective risk-based assessment and analysis, considering current and future business direction.
2. **Involve the right people with the right organization model**—Business teams have large stakes in preventing and detecting sensitive data flows. The requirement or the need for establishing DLP policies can come from several sources: corporate policies (from senior management), risk assessments (from risk management), recent security events (from IT security, legal, compliance management) and *ad hoc* threats/concerns. DLP policies should comply with legal and data privacy requirements. Representatives from key departments such as research and development, engineering, finance, compliance, and legal can contribute toward developing policies based on their respective risk. Involving the right people with defined roles and responsibilities from inception is one of the key success factors. The DLP team should include representatives who are responsible for data protection, data owners and those from key functions, IT, and various business units. Team members should be given appropriate training on the DLP system, its use and limitations to enable them to contribute to the implementation effectively. The team lead should have a good understanding of organizational and business requirements and the DLP system and be empowered to handle DLP-related issues.
3. **Identify sensitive data and understand how they are handled**—Content-centric data protection technologies such as DLP rely heavily on proper classification of sensitive information. DLP policies are defined to primarily target sensitive documents and their handling within an organization. Streamlining sensitive data handling practices from creation to archiving and deletion through policies and practices should be a necessary step for successful DLP enforcement. The identification and classification of sensitive data according to the policies and guidelines of the organization are important steps for executing a comprehensive data protection strategy. Understanding how those sensitive data are handled, exception scenarios, and what scenarios should be prevented or blocked is also required for defining DLP policies. Policies and procedures should provide clear guidance to employees on appropriate and inappropriate practices. Training and awareness programs could help to achieve this goal.

4. **Provide a phased implementation based on progress**—DLP solutions provide a wide variety of implementation options, allowing organizations to focus on high-risk areas. Email, web and USB/flash-drive monitoring are the most widely used options in DLP.[12] The initial pilot implementation should be restricted to a region or division. A phased approach, prioritizing the modules and targeting key end points, provides an opportunity to learn from experience before wider deployment. An implementation road map should be planned, with appropriate milestones and checkpoints to review progress, including go/no-go decisions. Modules could be first piloted in a small group or target area to fine-tune the policies and minimize the business impact. The implementation team should review the initial results objectively, including improvement opportunities, benefits and operational impact.
5. **Minimize the impact to system performance and business operations**—DLP gathers data from numerous end points and consumes considerable network bandwidth. Agents installed in the end points and in packet-level monitoring in network gateways can also impact user performance. Poorly defined policies can trigger a large number of events and impact user performance. This can create dissatisfaction among users and adversely impact the DLP program. The phased implementation discussed previously, coupled with adequate policy-level testing, could help minimize the impact on performance and promote a positive user experience. The DLP infrastructure and the network capacity must be planned adequately to minimize the impact to the business. Adequate testing of policies in a test environment can help in understanding the effectiveness of the policy and the potential impact on the business before wider deployment. Periodic monitoring and measurement of the impacts on system performance and users can help to assess an overall negative impact resulting from poorly tuned DLP policies.
6. **Create meaningful DLP policies and policy management processes**—Creating relevant and meaningful policies is central to the DLP strategy. **Figure 1** depicts typical DLP operational activities in an organization. Policies are created to monitor or block (prevent) sensitive data from leaving an organization's network. A structured policy request and review process can help to ensure that policies defined are meaningful and relevant and do not overlap with existing policies. Policy changes or modifications should be handled through a controlled process. DLP policies also need a periodic review to adapt to changing technologies, business practices and new risk scenarios. Establishing a policy life cycle management process (**figure 2**) from request to modification/deletion and involving the right people are necessary for successful implementation. The process should include a robust change management activity, including emergency changes to cope with specific *ad hoc* threats. Before deploying widely, policies need to be tested in a test or restricted environment to ensure that they are working as intended and not causing an adverse impact.
7. **Implement effective event review and investigation mechanisms**—Events triggered by policy violations and the resulting activity logs (when blocking or monitoring) are key outputs from a DLP tool that provide valuable information and insight. An effective and responsive review mechanism is required to realize the benefits of the solution. Response rules can be defined in the system to respond in a particular way to each case. Alerts can also be configured for specific

Figure 1—Common DLP Operational Activities

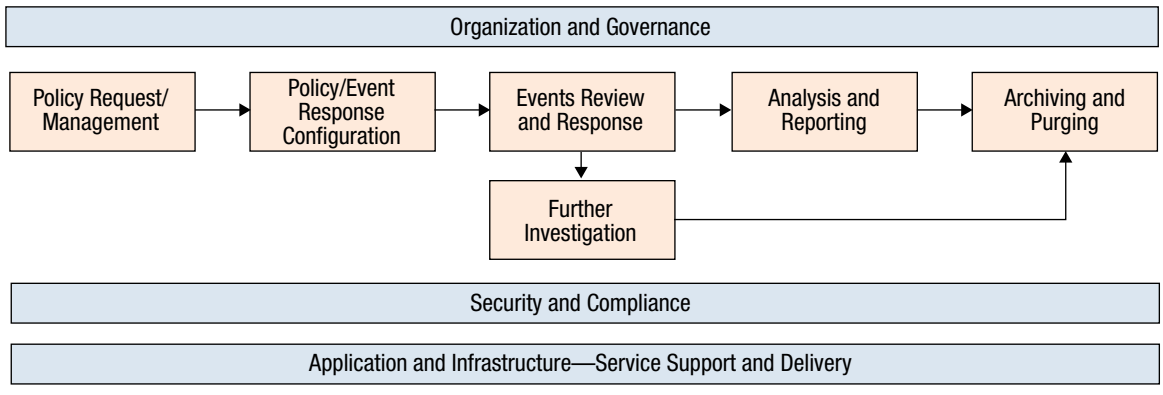
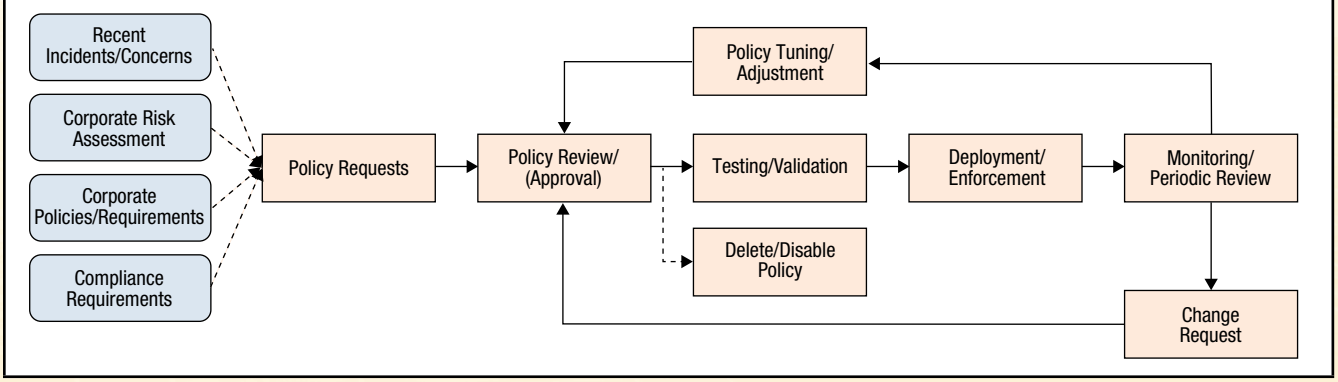


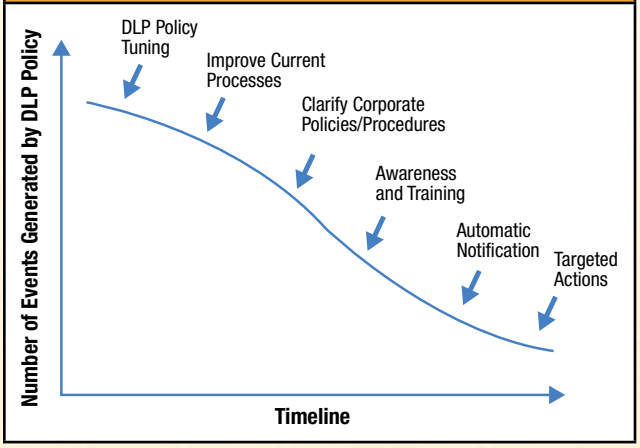
Figure 2—DLP Policy Management Process



events. A representative and responsive event review team should review critical events and take appropriate actions in a timely manner to prevent a negative impact to the business. Serious incidents may require a detailed investigation, preferably by a separate team. Data that are no longer required should be purged to free up storage space. Appropriate risk-based event response rules should be established for each policy defined to identify and prioritize unusual events. An event review team should have adequate knowledge of business risk. Feedback on event reviews to policy owners can provide useful information to fine-tune the policies and take effective actions to reduce the noise (wrongly identified cases) in the events triggered. Event reviews and investigations need to be handled with care, following established procedures to comply with policies, laws and regulations.

8. **Provide analysis and meaningful reporting**—Events triggered from DLP policies provide useful insight on where, when and how the sensitive data are stored and handled within the organization. Events can be analyzed by breaking them down into individual policies, departments, regions and trends. The aggregate picture could provide insights on current data-handling practices and where the organization needs additional awareness and training. An effective DLP program can strengthen current practices when they require improvement. A meaningful analysis and reporting process can help policy owners to improve the effectiveness of their DLP policies. Event profiles and trends can also help to create or refine policies and guidelines. Periodic reporting should be set up to communicate data loss patterns and trends to stakeholders to improve control practices and modify the policies, if required. Developing the right indicators (metrics) and appropriate pattern and trend analysis to capture the changes and exceptions is one of the critical factors for successful analysis. Generally, data loss events should progressively reduce for each policy, if supported by awareness programs and other management actions (**figure 3**).
9. **Implement security and compliance measures**—A DLP system collects a large amount of data, some of which may be personal in nature. The handling of personal data collected should comply with data privacy laws and regulations of the countries in which the data are collected. The data can also be business sensitive; therefore, it is critical to manage the DLP system and the data captured securely and in compliance with applicable laws and regulations. As with other technologies, DLP has its own limitations in preventing or detecting every data loss event in a dynamic technology world. Thus, it is necessary to understand the potential high-risk scenarios in which DLP technology can be circumvented for malicious reasons and to work with IT security teams to design robust security countermeasures. Secure and controlled practices for creating, updating and deleting policy configurations and event management within the DLP system and appropriate segregation of duties should strengthen the overall security. Based on the implementation scope, it is important to know the applicable data privacy requirements and take appropriate measures such as employee notification and consent, if required. The DLP team should be part of the corporate security governance structure and work closely with other security teams to ensure data protection.

Figure 3—Effective DLP Policy Enforcement



10. **Implement an organizational data flow and oversight mechanism**—Data sharing and cross-sectional data flows of business information are the lifelines of an innovative organization. Every day in the course of normal business operations, organizations share data with several groups, such as suppliers, clients, research partners, regulators and dealers. While organizations have to protect loss or leakage of sensitive data, they must also make sure that DLP solutions do not hinder legitimate data flow inside or outside the organization. An oversight team should review the business benefits of DLP on an ongoing basis and also verify its impact on legitimate data flow within the organization. The business benefits of a DLP program need periodic verification by an oversight team. Rapidly changing technology landscapes can also impact the DLP solution's effectiveness; DLP may not be able to capture all exceptions. The oversight team needs to review the overall cost and benefits of the DLP program on a periodic basis. The oversight team can also provide strategic direction for the DLP program based on periodic reviews.

CONCLUSION

Ensuring that the organization takes adequate measures to protect against information loss or leakage is an important responsibility of the IT department. Management has to provide assurance to its stakeholders that measures are in place to protect sensitive corporate digital assets, including IP, as well as personal and financial data. A comprehensive and integrated DLP solution should provide reasonable controls to protect data loss from internal sources. At the same time, successfully implementing a DLP solution for a larger organization needs careful planning, systematic implementation and effective processes. The identified 10 key considerations show in different stages what can impact the success of a DLP solution to deliver business value for an organization. Although not all of them are applicable to every organization, consideration of the applicable points can improve the success of DLP solution implementation and policy enforcement.

ENDNOTES

[1] US Patent and Trademark Office, "Intellectual Property and the U.S. Economy: Industries in Focus," Economics and Statistics Administration, March 2012, *www.uspto.gov/news/publications/IP_Report_March_2012.pdf*

[2] KPMG, "Data Loss Barometer: A Global Insight Into Lost and Stolen Information," 2012, *www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Documents/data-loss-barometer.pdf*

[3] Verizon, "Data Breach Investigations Report," 2012, *www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf*

[4] Janes, Paul; "Information Assurance and Security Integrative Project: People, Process, and Technologies Impact on Information Data Loss," SANS Institute, 7 November 2012, *www.sans.org/reading_room/whitepapers/dlp/people-process-technologies-impact-information-data-loss_34032*

[5] *Op cit*, KPMG

[6] ISACA, *Data Leak Prevention*, white paper, September 2010, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Data-Leak-Prevention.aspx*

[7] CSIS, "20 Critical Security Controls, Version 4.1," SANS Institute *www.sans.org/critical-security-controls/guidelines.php*

[8] Kanagasingham, Prathaben; "Data Loss Prevention," SANS Institute, 2008, *www.sans.org/reading_room/whitepapers/dlp/data-loss-prevention_32883*

[9] *Op cit*, CSIS

[10] Forrester, "Rethinking DLP: Introducing the Forrester DLP Maturity Grid," September 2012, *www.forrester.com/Rethinking+DLP+Introducing+The+Forrester+DLP+Maturity+Grid/fulltext/-/E-RES61231*

[11] Ashford, Warwick; "Why Has DLP Never Taken Off?," *ComputerWeekly*, 22 January 2013, *www.computerweekly.com/news/2240176414/Why-has-DLP-never-taken-off*

[12] *Op cit*, Janes

Challenges and Benefits of Migrating to COBIT 5 in the Strongly Regulated Environment of EU Agricultural Paying Agencies

Giuseppe Arcidiacono, CISA, CISM, CGEIT, PMP, is a computer engineer with more than 10 years of experience. Arcidiacono is the head of the IT department at Agenzia Regione Calabria per le Erogazioni in Agricoltura (ARCEA), a European Commission Accredited Paying Agency (pursuant to Commission Regulation EC No. 885/2006).

The European Union selected COBIT® as one of the three internationally accepted standards[1] to be used to provide information security and control over its agricultural paying agencies.[2] This brings the question, what are the challenges and benefits of migrating to COBIT® 5[3] in the strongly regulated environment of the European Union (EU) agricultural paying agencies?

The EU agricultural paying agencies are accredited organizations delegated to execute three main functions in respect of the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD) expenditure:

1. Authorize and control payments to establish that the amount to be paid to a claimant is in conformity with EU community rules.
2. Execute payments to pay the authorized amount to the claimant or, in the case of a rural development, pay the community cofinancing.
3. Account for payments and record all payments in the agency's separate accounts for EAGF and EAFRD expenditures, in the form of an information system, and prepare periodic summaries of expenditures, including declarations to the European Commission (EC).

Compliance with a set of accreditation criteria is designed to ensure that the paying agency provides sufficient guarantees to:

- Check the eligibility of aid applications before any payment is made
- Keep accurate and exhaustive accounts
- Ensure that required checks by regulation sectors are made
- Make sure all requisite documents are properly kept, accessible and presented in a timely manner

COBIT 5, the latest edition of the ISACA framework, provides EU paying agencies with a great opportunity to rethink their governance and management of enterprise IT (GEIT) while adapting their own information security system and migrating to a new, well-structured and comprehensive standard.

While the International Organization for Standardization (ISO) and British Standards Institution (BSI) standards are specialized "old-style" frameworks that are based on domains, checklists, control objectives and measures, COBIT 5 goes beyond; it focuses not only on the IT function and IT security, but supports the implementation of a comprehensive governance and management system for enterprise IT and information by:

- Enabling IT to be governed and managed in a holistic manner for the entire organization
- Taking in the full end-to-end business and IT functional areas of responsibility
- Considering the IT-related interests of internal and external stakeholders

The main reasons for a paying agency to migrate to COBIT 5 (either from COBIT® 4.1 or from one of the other two guidelines/standards) can be described best by analyzing how the five COBIT 5 principles fit within the paying agency context.

PRINCIPLE 1: MEETING STAKEHOLDER NEEDS

One of the most important concerns in a paying agency is managing many stakeholders and actors who play, at different levels, a role in these organizations and have dissimilar (and sometimes conflicting) perspectives and expectations.

A paying agency's key stakeholders include:

- **Director/top management**,[4] who ensure that:
  - Accounts presented to the EC give a true, complete and accurate view of the expenditure
  - There is a system in place that provides reasonable assurance on the legality and regularity of the underlying transactions, including that the eligibility of demands and, for rural development, the procedure for attributing aid are managed, controlled and documented in conformity with Community rules

- **Internal key users**, mainly from core business departments, who provide aid to make payments correctly, ensure that payments are fully recorded in the accounts, and submit the requested documentation within deadline and in the manners stipulated in EU rules
- **Final claimant**, who should receive claims as soon as possible
- **European Commission**, which accredits, monitors and controls paying agencies. The EC can impose financial corrections on the member state under the conformity clearance procedure.
- **Certification bodies**,[5] which conduct their examination of a paying agency according to internationally accepted auditing standards and taking into account any guidelines on the application of the standards established by the EC
- **Internal auditors**,[6] who have to verify that procedures adopted by the agency are adequate to ensure that compliance with Community rules is verified and the accounts are accurate, complete and timely

It is neither straightforward nor simple in this context to negotiate and decide among different stakeholders' value interests.

It is fundamental to:

- Gather and analyze quantitative and qualitative information to determine whose interests should be addressed
- Identify the interests, expectations and influence of the stakeholders and relate them to the mission of the agency
- Identify stakeholder relationships that can be leveraged to build coalitions and potential partnerships

PRINCIPLE 2: COVERING THE ENTERPRISE END-TO-END

A paying agency's processes are complicated and often cross-departmental. They are regulated by EC laws that establish requirements, rules and specific mandatory steps and require that many roles and responsibilities are set.

All of these processes are IT-related: It is fundamental to integrate GEIT into enterprise governance. In other words, paying agencies have to treat information and related technologies as assets that need to be dealt with, just like any other asset, by everyone in the enterprise.

The EC requires that, at all levels, the daily operations and controls activities of the agency be monitored on an ongoing basis to ensure a sufficiently detailed audit trail.

PRINCIPLE 3: APPLYING A SINGLE, INTEGRATED FRAMEWORK

As previously mentioned, paying agencies must comply with a strict baseline defined by Commission Regulation (EC) No. 885/2006.

To be accredited, a paying agency, as defined also in article 6 of Regulation (EC) No. 1290/2005, must have an administrative organization and a system of internal control that comply with the criteria set out in annex I to EC 885/2006 ("accreditation criteria") regarding:[7]

- Internal environment
- Control activities
- Information and communication
- Monitoring

COBIT 5 helps with compliance because it aligns with other relevant standards and frameworks at a high level (both enterprise- and IT-related) and can, therefore, serve as the overarching framework for GEIT.

Using COBIT 5 makes it easier for a paying agency to comply with accreditation criteria by placing every piece in a cohesive whole and helping stakeholders understand how various frameworks, good practices and standards are positioned (relative to each other) and how they can be used together.

PRINCIPLE 4: ENABLING A HOLISTIC APPROACH

The COBIT 5 framework describes seven categories of enablers that individually and collectively influence whether GEIT will work and how they are driven by the goals. The seven enablers are:

- Processes
- Organizational structures
- Culture, ethics and behaviors
- Principles, policies and frameworks
- Information
- Services, infrastructure and applications
- People, skills and competencies

In the paying agencies' environment, some of these enablers assume a major value, particularly:

- EU regulations require all paying agency activities to be organized in well-structured processes and described by formally adopted manuals. All processes have to achieve certain objectives and produce a set of outputs in support of achieving overall organizational goals.
- The internal organization is one of the most important accreditation criteria for paying agencies. The agency's organizational structure must provide for clear assignment of authority and responsibility at all operational levels and for separation of the three functions (authorization and control of payments, execution of payments, and accounting). The responsibilities of the three functions are to be defined in an organizational chart and include technical internal audit services.

- Information is pervasive throughout paying agencies. Information is required for keeping the agency running and well governed. Although information is not a key product of the agency, European regulations mandate that information security measures be adapted to the administrative structure, staffing and technological environments of each individual paying agency. The financial and technological efforts are to be in proportion to the actual risk incurred.
- Paying agencies have to comply with many people-related requirements. They have to respect the following:
  - Appropriate human resources must be allocated to carry out the operations, and the technical skills required at different levels of operations must be present.
  - The division of duties must be such that no official has responsibility for more than one of the responsibilities for authorizing, paying or accounting of sums charged to funds, and no official can perform one of those tasks without his work coming under the supervision of a second official.
  - The responsibilities of each official must be defined in writing.
  - Staff training must be appropriate at all levels of operation, and there must be a policy for rotating staff in sensitive positions.
  - Appropriate measures must be taken to avoid a conflict of interest.

PRINCIPLE 5: SEPARATING GOVERNANCE FROM MANAGEMENT

Paying agencies do not have a board, but the EC requires that they make a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organizational structures and serve different purposes. Management runs the organization from day to day, while governance sets policy, exercises oversight and strategically guides the organization. The separation of governance and management involves a division of both duties and personnel.

CONCLUSION

Migrating to COBIT 5 can bring many benefits to EU accredited paying agencies.

In particular, COBIT 5 could help paying agencies ensure that adequate governance structures are in place and increase the level of capability and adequacy of the relevant IT processes, with the expectation that as the capability of an IT process increases, the associated risk will proportionally decrease and efficiencies and quality will increase.

In addition, the following benefits could be reached:

- Maximizing the realization of activities' improvements through IT while mitigating IT-related risk to acceptable levels
- Support of the strategic objectives by key investments and optimum returns on those investments, thus aligning IT initiatives and objectives directly with the agency's mission
- Compliance with EU accreditation criteria
- A consistent approach for measuring and monitoring progress, efficiency and effectiveness as required by the EC[8]
- Lowered cost of IT operations and/or increased IT productivity by accomplishing more work consistently in less time and with fewer resources

ENDNOTES

[1] The other two guidelines are: ISO/IEC 27002 *(www.iso.org/iso/catalogue_detail?csnumber=50297)* and Bundesamt for Sicherheit in der Informationstechnik, IT-Grundschutzhandbuch (the IT Baseline Protection Manual) *(https://www.bsi.bund.de/english/publications)*.

[2] European Commission Regulation (EC) No. 885/2006

[3] ISACA, COBIT 5, USA, 2012, *www.isaca.org/cobit*

[4] Guideline No. 4 on the statement of assurance to be provided by the director of a paying agency pursuant to article 8(1)(c)(iii) of Council Regulation (EC)NO 1290/2005

[5] Commission Regulation (EC) No. 1290/2005 of 21 June 2005

[6] European Commission, Directorate-General for Agriculture and Rural Development, Guidelines for the Certification Audit, Guideline No. 3—Audit Strategy

[7] Accreditation criteria cover the four basic areas of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model.

[8] Annex I of Commission Regulation (EC) No. 885/2006 states: "Ongoing monitoring is built into the normal, recurring operating activities of the paying agency."

Auditing for PII Security Compliance

Derek Mohammed, Ph.D., CISA, CISM, is an assistant professor who teaches undergraduate and graduate courses in information security and assurance at a private liberal arts university in Texas, USA. Prior to joining academia, Mohammed worked extensively in both the public and private sectors to improve the security of critical information systems. His research focuses on IT auditing and security compliance.

As business and individuals increasingly rely on information technology, more and more data that identify them exist across various information systems. Some elements of data are very personal and could be harmful if placed in the wrong hands. This type of information is known as personally identifiable information (PII). The US Government Accountability Office defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."[1]

There are laws and regulations designed to protect PII in digital form. Examples of laws include the US Family Educational Rights and Privacy Act, the US Health Insurance Portability and Accountability Act (HIPAA),[2] the Privacy Act in Australia, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, and the Data Protection Directive in the European Union.

Despite regulations for protecting PII, data leakage of PII is remarkably common. During the week of 11-17 April 2011, for example, Identity Finder posted nine reports of PII being stolen, lost or somehow exposed. Of these nine, one incident involved hacking into an international firm's IT system to steal customer PII in order to extort that firm for money. Another incident involved the theft of PII by someone authorized to access the data. Yet another incident involved unauthorized access to credit card data due to a security flaw. The remaining six incidents were more typical. Three incidents involved the theft or loss of computer or data storage containing unencrypted PII, two incidents involved the accidental disclosure of PII to the public or a third party, and one incident involved an employee failing to destroy PII records before discarding them in the trash.[3] Altogether, these nine incidents affected four million people and all were revealed during a single, typical week.

Disponibile anche in Italiano
www.isaca.org/currentissue

It is important to note that the vast majority of PII security breaches are preventable. Systems can be strengthened to prevent unauthorized access, and employee screening and training can be improved to prevent PII data leakage due to theft, loss or improper handling. However, very often it is not until after an incident has occurred that an organization makes a thorough review and necessary changes to practices regarding PII security. To reduce the number of PII data security breaches, organizations must embrace the concept of auditing for regulatory compliance and security for PII so that issues can be addressed preemptively.

GOVERNANCE-LEVEL AUDIT

An audit for privacy security compliance must start at the top. An organization's ability to establish a governance program that effectively addresses and manages IT risk is the key to successful PII security, as well as IT security in general. Without proper governance, controls for protecting PII may be uncoordinated, overlapping, gapped or absent. It is crucial that an organization's senior management understand their PII risk factors and compliance requirements. To address this need, many organizations create an executive-level position, such as chief information security officer or chief compliance officer, that is responsible for identifying, assessing, tracking and addressing IT risk.[4] If such a position exists, an auditor's first stop should be a visit to this individual's office to ask these broad questions:

- **Are PII compliance requirements identified and understood?** An auditor must know that an organization has identified and understands the regulations that define and mandate security for PII. Different regulations have their own variations of how protected information is defined and treated. For example, HIPAA addresses security for protected health

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:

Enjoying this article?

- Read *Privacy and Big Data* and other ISACA white papers.

  www.isaca.org/ white-papers

- Discuss and collaborate on privacy/data protection and audit tools and techniques in the Knowledge Center.

  www.isaca.org/knowledgecenter

information (PHI), which it defines as any information that identifies an individual and relates that individual to past, present or future physical or mental health; the provision of health care; or past, present or future payments for health care.[5] Therefore, the level of security that is needed to protect PII will vary and depend on the regulatory body that mandates protection.

- **What are the organization's requirements for handling PII?** After an organization has a clear picture of how PII is legally defined, it can examine *where* the protected information supports critical business processes. PII should only be captured, stored and maintained where absolutely necessary. Wherever possible, PII should be eliminated from business processes or de-identified. De-identifying PII means removing or obscuring enough attributes so that the information no longer identifies an individual.[6] This enables an organization to continue to support a business function that relies on data derived from PII without having to incur the added risk associated with maintaining and processing PII within that function. The PII security compliance auditor should verify that the organization has properly applied the legal definition of PII in identifying its requirements for handling PII and verify that the organization has an established process for reviewing requirements and recommending elimination or de-identification of PII.
- **Has the organization conducted a risk assessment for PII?** An organization should categorize its PII by the level of impact of a disclosure of information. Depending on the organization's industry and the nature of PII, there are various factors that could be evaluated to determine the risk associated with each piece of PII. Potential factors include *how* identifiable the information is, the *quantity* of PII records, and the *sensitivity* of the data fields (for example, a social security number or a credit card number are more sensitive data than a person's shopping habits or marital status).[7] The auditor must verify that an accurate risk assessment has been conducted and that various PII pieces are being treated with the appropriate levels of confidentiality.
- **Are all necessary controls for communicating PII addressed in the organization's security policy?** The auditor must review the organization's security policy to ensure that it addresses the required security measures for protecting PII in compliance with laws and/or regulations. The policy should clearly state goals that support adequate PII security and align with the organization's compliancy requirements, business requirements and risk assessment, and from which effective standards, procedures and guidelines can be derived. The security policy should also call for monitoring compliance, enforcing sanctions against violators, and testing the effectiveness of controls through routine monitoring and security testing.

PROCEDURAL-LEVEL AUDIT

The next level the auditor should examine is the procedural level. This is the level in which strategic goals for PII security are translated into standards, procedures and guidelines. In addition, the definition of PII; the strategic goals; and the standards, procedures and guidelines are communicated to all employees at this level. The auditor must verify whether standards, procedures and guidelines align with and support policy goals for PII security, and that communication to employees is adequate and effective. The questions to ask at this level are:

- **Do standards, procedures and guidelines support the security policy goals?** The auditor should review all standards, procedures and guidelines to ensure that they effectively support the goals of the organization's security policy. This policy should address all PII security concerns, including, for example, proper access control, encryption, labeling and destruction. However, the scope of this review cannot be limited to standards, procedures and guidelines specific to PII, as any security

> "Any security measure affects the security of PII."

measure affects the security of PII. For example, a lenient password reset procedure could allow unauthorized access to a workstation or database containing PII or a gap in physical security could allow someone to steal physical records or a device containing unencrypted PII.

- **Are all employees and/or users trained on how to identify and handle PII?** Procedures should be in place to ensure that all employees are trained before they are exposed to PII. While there should be focused training for those directly dealing with PII, all employees across the organization should know how to identify PII and initiate the appropriate response to a PII security breach. The auditor must identify how policies, standards, procedures and guidelines are being communicated across an organization.[8] The auditor must determine if the communication methods are effective and if there is sufficient accountability. For example, simply having a poster next to the coffee station describing PII and how to handle the information would likely be insufficient communication if the organization intends to enact sanctions against employees who violate handling procedures. What if an employee does not drink coffee? Formal training followed by a signed statement of understanding that is kept on file by human resources and that includes proper handling procedures and consequences for noncompliance would be much more appropriate in this scenario.
- **Are there effective plans and procedures for response to a PII security incident?** Extensive preparation is often the determining factor when a security incident is not handled properly. The development of a PII security incident response plan forces relevant entities within an organization to make well-thought-out decisions on how to handle many details of a security incident. Decisions could include how to sanitize the situation, how to report the incident and how to compensate those affected. These decisions should be integrated into policies and procedures for response to a PII security incident.[9] The auditor should verify that such plans have been developed and are continually reviewed to ensure that every imaginable scenario is considered.

OPERATIONAL-LEVEL AUDIT

The final phase of the audit is where PII security compliance auditors conduct their own security testing and monitoring to assess the effectiveness of the controls. This is essentially testing to ensure that PII security is functioning properly. Organizations can have robust policies, procedures and training for protecting PII, but if employees at the lower level do not understand the training and/or are not following the procedures, or if unexpected security loopholes allow for unauthorized access, the organization's investment in PII security will have been made in vain. A PII security audit is not complete without verifying that security measures are in place and effective in day-to-day operations. The questions to ask at this level are:

- **Is PII found out of bounds?** Monitoring for PII should include data at rest and data in transit and should not be limited to business processes that use PII, but should span the entire organization to include the organization's information systems (IS) perimeters. The auditor must verify that no PII can be found in business processes where it is not required and that encryption is effectively used when PII is in transit to at-risk areas, such as beyond the organization's internal network, or is being stored in at-risk areas, such as on an employee laptop (prone to theft). The auditor must also scrutinize business processes that deal with PII to verify if more PII is being collected and stored than absolutely necessary.

In monitoring data at rest, PII can reside in less-than-obvious places such as in metadata, deleted files or files marked for deletion, alternate data streams, graphical files, print spool files, link or shortcut files, RAM and page files, and the operating system registry hive. Additionally, there are many ways in which a nefarious user can obfuscate PII to prevent successful monitoring, such as by modifying file extensions. For these reasons, the best tools to monitor PII at rest during an audit are forensic tools.[10]

> "PII can reside in less-than-obvious places."

After monitoring is complete, the auditor can determine the effectiveness of the organization's internal monitoring process. The auditor should verify whether logging is enabled for all critical systems and whether the organization has adequately assigned the task of monitoring for execution. The auditor should also use monitor logs to verify if users are handling PII in accordance with procedures.[11]

- **Are access controls to PII being enforced?** The auditor must verify whether access controls within an organization prevent unauthorized access to PII. Only authenticated users who are authorized may have access to PII. Only individuals who require access to support critical business processes should be authorized, and the auditor should verify that authorized individuals have undergone the required vetting. Testing should also include penetration testing to ensure that controls are effective and prevent unauthorized access from outside of the organization. The auditor should also verify that controls prevent privileged escalation attacks that enable unauthorized users from accessing PII, and that authorized user authentication meets adequate standards and guidelines to prevent an unauthorized user from gaining access to an authorized user's account.
- **Is training effective? Are procedures being implemented and followed?** There are a few ways that an auditor can verify whether employee training is effective. The auditor can simply interview employees and ask them to describe PII and follow the various security procedures with the employee. The auditor should review logs and verify whether employees' activity matches their descriptions and that these match with the legal regulations and the organization's security policy, standards, guidelines and procedures. Employees failing to follow procedures could mean that training is ineffective, or it could mean that sanctions are not harsh enough or are too laxly enforced, or it could be a combination of the two. If auditors identify failures to follow proper procedures, they must focus on identifying the cause of the breakdown in processes, rather than correcting each individual incident.

CONCLUSION

Conducting an audit for PII security compliance is a daunting and laborious task. It is not possible to limit PII auditing to specific sections or business processes of an organization and still have the audit remain effective. Likewise, it is not possible to limit the scope of a PII audit to a particular level and still judge the effectiveness of security controls. By using a three-level, top-down approach, auditors can efficiently cover an entire organization and avoid having to duplicate efforts or repeat processes due to deficiencies at higher levels.

ENDNOTES

[1] US Government Accountability Office, "Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information," Report 08-536, USA, May 2008, *www.gao.gov/new.items/d08536.pdf*

[2] Pan, Yin; Bill Stackpole; Luther Troell; "Computer Forensics Technologies for Personally Identifiable Information Detection and Audits," *ISACA Journal*, vol. 2, 2010, *www.isaca.org/archives*

[3] Identity Finder, Identity Theft News, *www.identityfinder.com/news/*

[4] Rai, Sajay; Phillip Chukwuma; "Top 10 Security and Privacy Topics for IT Auditors," *ISACA Journal*, vol. 2, 2010, *www.isaca.org/archives*

[5] Yale University, *HIPAA Policy 5100: Protected Health Information Security Compliance*, 20 April 2011, *www.yale.edu/ppdev/policy/5100/5100.pdf*

[6] McCallister, Erica; Tim Grance; Karen Scarfone; Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*, National Institute of Standards and Technology, April 2010, *http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf*

[7] *Ibid*.

[8] *Op cit*, Rai

[9] *Op cit*, McCallister

[10] *Op cit*, Pan

[11] *Op cit*, Rai

Risk Management in 4G LTE

Daksha Bhasker, CISM, has more than a decade of experience in the telecommunications industry and has worked in various roles in business intelligence, strategy planning, product management, business management operations and controls. For the past six years, she has been in a governance role at Bell Canada covering Sarbanes-Oxley compliance, complex technical solutions and security risk management.

Fourth-generation Long Term Evolution (4G LTE) is an open architecture, all Internet Protocol (IP), broadband wireless data technology designed to offer users access to technology-agnostic seamless roaming across carriers and geographic regions. The recent proliferation of promising wireless technologies has quickly been followed by torrents of new mobile malware and cyberthreats.

4G LTE is expected to exceed US $340 billion in service revenues by 2017.[1] According to the Global mobile Suppliers Association (GSA), 415 mobile network operators (MNOs) are rushing for a slice of revenues, with 248 commercial deployments in 87 countries by the end of 2013.[2] The business benefits of 4G LTE (see **figure 1**) are attractive to a global base of MNOs and subscribers.

To this point in time, mobile devices have been primarily used for voice traffic and have seen relatively low volumes of cyberattacks. However, with growth in mobile data traffic on LTE and increased computing power on smart devices, mobile technologies are becoming concerted targets for cyberattacks. McAfee reported a 4,000 percent increase in mobile malware in 2012 (over 2011) with up to 37,000 variants.[3] The Cisco Visual Networking Index (VNI) forecasts monthly global mobile data traffic to surpass 10 exabytes in 2017 with 4G carrying 45 percent.[4] With the number of entrants, size and market momentum building around 4G LTE, data on this platform need rigorous protection.

Risk management encompasses managing not only external attacks, but also inherent security risk and vulnerabilities resulting from network architecture, operations and service deployment.

While the 3rd Generation Partnership Project (3GPP) incorporates security into the LTE System Architecture Evolution (SAE), it also prescribes options for addressing various security vulnerabilities by means of network deployment and operations that are discretionary to MNOs. This creates inconsistencies among the hundreds of MNOs in the security implementation in 4G LTE services and introduces various risk. Further variations in business objectives, business models, network deployment, operations and regional legislation introduce risk that needs to be evaluated and appropriately managed (**figure 2**).

Figure 1—Value of 4G LTE Technology

Lower Capex and Opex for MNOs:
- Flat architecture with fewer network nodes
- Spectral efficiency
- All IP based with IPv6 support
- No need to maintain circuit-switched network

Better Service Experience for Subscribers:
- High bandwidths of 300 Mbps peak downlink and 75 Mbps peak uplink
- Low latency
- Interworking support with existing 2G, 3G and non-3GPP technologies
- IP multimedia subsystem (IMS) offering voice, data, video convergence, content and applications, e.g., VoLTE, telepresence, gaming

Security:
- 3GPP standard TS 33.401 defining the security architecture and prescribing deployment options

Source: 3rd Generation Partnership Project (3GPP), "3GPP—The Mobile Broadband Standard," 2013, *www.3gpp.org/LTE*

Figure 2—Risk Management 4G LTE

Risk management is the ultimate objective of all information security activities and this is no different with 4G LTE services.

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:

BUSINESS OBJECTIVES AND STRATEGIES

Products and services in the marketplace are sustained only when they successfully address a market need and create value. All players entering the 4G LTE market has unique strategies based on the needs of their respective target markets and business plans. The goal of risk management is to support entities in meeting these business objectives. For the 450 MNOs entering the 4G LTE market in 2013, these objectives are numerous and diverse. A variation in business objectives is likely to result in inconsistent security levels in LTE networks and services offered and a threat to the consistent seamless-roaming service promise of LTE. Examples include:

> "The goal of risk management is to support entities in meeting…business objectives."

- **Market protection strategy**—As mobile data traffic volumes increase to unprecedented levels, some MNOs will adopt 4G LTE to alleviate problems of network congestion and bandwidth bottlenecks on their current infrastructure. These MNOs are likely to implement 4G LTE in high-density hot zones, with network upgrades to 4G in phases over the longer term. These deployments are typically multimode operations with 4G in the hot zones where subscribers fall back to lower-speed legacy technologies once outside the zone. Such MNOs are inclined to offer 4G as an extension of their existing 3G networks and introduce security risk as they work through interoperability issues between various access technologies within their own infrastructure and operations. The business objectives of such MNOs focus on subscriber retention rather than acquisition. MNOs in this type of deployment strategy encounter operational, performance and security management issues that are threats to the quality of subscriber experience. Poor service quality can result in MNOs losing their customer base, risking their primary business objective of market protection.
- **Market leadership strategy**—MNOs with market leadership objectives opt for full 4G LTE network rollouts. These MNOs capitalize on the service quality of LTE as a competitive differentiator. 4G LTE service might be used by the MNOs as a substitution for fixed broadband, capturing market share from wireline competitors. A large-scale rollout would allow MNOs to decommission or phase out circuit-switched networks, reaping the reduced cost per megabyte advantage of LTE. These MNOs would position 4G LTE as a premium service, implement security architectures as recommended by the 3GPP and promote the full suite of feature-rich capabilities of 4G LTE. While this deployment has a robust security infrastructure, the MNO assumes financial risk of upfront capital and operational expenses to achieve business objectives. Should there be inadequate market take rate, these MNOs may not achieve targeted returns on investments.
- **First-to-market strategy**—On the other hand, MNOs with the primary objective of speed to market are known to turn up the basic infrastructure and cut corners by deferring deployment of expensive security infrastructure. This approach presents serious security vulnerabilities for the MNO's operations, partnering MNOs and the subscriber, and can cost the MNO its reputation and its business.

Since the security thresholds and risk in each MNO's business is diverse, MNOs entering peering and partnership agreements to allow seamless mobility to subscribers must be particularly cautious around associated security risk.

BUSINESS MODELS

MNOs develop business models based on business objectives. The 4G LTE architecture and design lend themselves to several new, disruptive models. With each new model come associated challenges, threats and risk:

- **Infrastructure sharing model**—3GPP designed 4G LTE with options for network sharing and continues to evolve it under the TS 23.251 standard. Sharing options include radio access network (RAN) sharing, backhaul sharing and partial to complete core network sharing. Drivers for network sharing range from reduced infrastructure and operating costs and greater geographic coverage, to spectrum sharing, where compelled by regulations or scarcity. Ovum forecasts

that, by 2015, 30 percent of all LTE networks will involve some form of active network sharing.[5] In network sharing models, MNOs need to consider management protocols for shared resources and load balancing between cells of operators with shared infrastructure. Operations including configuration management, performance management, security management, maintenance and fault management in shared infrastructure bring complexity and operational threats as multiple MNOs need to collaborate efficiently to deliver service. Likewise, rate plans and billing according to usage of shared resources require a level of sophistication to ensure accurate billing to the subscriber and accurate revenue sharing among MNOs. This brings additional layers of risk management requirements.

- **Value added reseller/distributor model**—LTE, through the IP multimedia subsystem (IMS), offers an array of bandwidth-rich applications to subscribers. MNOs who want to move away from the business of solely being broadband pipe providers have the opportunity to partner with application and content providers—positioning themselves as distributors. This includes media content such as video on demand (e.g., Netflix), broadcast video, voice-over LTE and gaming. This business model requires the development of supporting network infrastructure for peering, content and application distribution with quality-of-service (QoS) (i.e., availability, latency, jitter) management. Operating models, revenue sharing, customer relationship management and billing arrangements need to be determined, each bringing its own share of business risk.

NETWORK INTEROPERABILITY AND PERFORMANCE

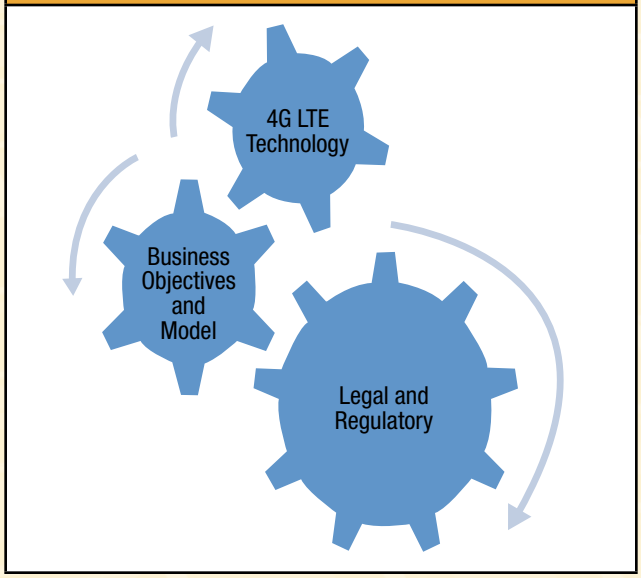
As 4G LTE service is delivered via an ecosystem of MNOs and content and application providers, network interoperability and performance are essential considerations:

- **Interworking**—4G LTE appears to be the chosen technology to heal the global rift between wireless access technology camps (CDMA and GSM) and create seamless technology-agnostic wireless roaming in the future. The 4G LTE architecture, in essence, is an ecosystem of interconnected MNOs and service provider networks. A subscriber moving from operator A's cell into adjacent operator B's cell is processed via prearranged handover parameters. Interoperability and security parameters between peering operators bring potential security risk. Misconfigurations in interconnecting network elements create vulnerabilities and present potential access points for attackers and possible performance degradation.
- **QoS management**—4G LTE offers voice, data and video convergence with QoS management for each application to ensure appropriate bandwidth allocation and latency requirements. As these services could transit through multiple carriers to get to the subscriber's device, consistency of QoS through peering points and network elements is critical to maintain service quality. Since many of these bandwidth-guzzling applications have low latency requirements, misconfigured or underprovisioned network elements can cause delays beyond the service tolerance thresholds that result in a poor experience for the subscriber.
- **Traffic management**—Aside from the high-bandwidth user traffic, signalling traffic on LTE is estimated to be 40 percent higher per LTE subscriber than on 3G networks. An inherent vulnerability in 4G LTE is the management of large volumes of user and signalling traffic. If not properly managed via scalable networks and load balancing, signalling floods can cause service degradation and bring the network down, analogous to a denial-of-service (DoS) attack.

REGIONAL LAWS AND REGULATIONS

Technologies succeed in the marketplace when they are founded on sound business models. No matter how rich the potential of a technology, business decisions shape the service sets, features and operations of a technology. In turn, no matter how strategic or brilliant the business proposition, legislation and regulations supersede business decisions (**figure 3**). 4G LTE offers seamless

Figure 3—Legislation and Business Define Technology



global roaming to subscribers. In addition, the all-IP service through the IMS can deliver services and applications to the mobile subscriber from various parts of the globe. The global dimension of 4G LTE warrants that MNOs pay particular attention to regional legislation and regulations.

MNOs collect, store, secure and treat subscribers' personal information under the prevailing local privacy legislation, often pushing legal verbiage to obtain subscriber consent to protect them against potential lawsuits. However, in the global context, there are numerous regions with little to no privacy legislation.[6] Should a subscriber's personal data from a country where privacy rights are established transfer into regions where there is minimal privacy legislation, the breach in privacy could have serious legal consequences for the MNO. High volumes of data traffic, applications and content on 4G LTE make it more vulnerable than its preceding technologies that primarily carried voice traffic.

Lawful interception (LI) is the process in which an MNO is legally sanctioned to intercept the communication of private individuals or organizations and provide information to law enforcement officials.[7] While 3GPP offers LI-permissive architecture for LTE, its deployment varies in accordance with applicable national or regional laws. In many countries, an LI requires a court order, while in other countries, government surveillance is the norm. To prevent legal violation, MNOs should ensure that their architecture and operations are in accordance with the prevailing regional legislation, keeping in mind that 4G LTE carries over-the-top applications and content globally.

RECOMMENDATIONS FOR MANAGING RISK IN 4G LTE

Risk management is a comprehensive science specific to individual entities and, thus, cannot be detailed completely here; however, there are certain key recommendations pertaining to security risk management in 4G LTE to keep in mind:

- Security should be an integral part of the 4G LTE service launch from the early stages of planning to design and deployment.
- Security architecture and associated security budgets should be earmarked and aligned with business objectives.
- Since 4G LTE involves a myriad of players, a clear understanding of the business strategy and objectives of selected partners in the service chain must be obtained.
- MNOs need to be particularly savvy about articulating security standards to their subscribers as consistency in security levels resides in managing security architectures, parameters and thresholds with partners and service providers in the LTE ecosystem and MNOs do not have unilateral end-to-end control over this.
- In 4G LTE, MNOs should negotiate strong agreements with partners, setting out clear security standards, parameters of interoperations, sharing arrangements and subscriber handover.
- Depending on the operator's network architecture and peering network arrangements, MNOs should budget for ample interoperability testing, configuration and performance management, considering the seamless technology-agnostic service promise of 4G LTE.
- 4G LTE network architecture and service offerings must be designed in context to a ubiquitous global framework while respecting regional legislation.
- Due to the all-IP converged traffic, 4G LTE networks need to be designed and architected with care toward QoS management. A failure on one service can adversely implicate multiple converged services. Since large volumes of data and signalling traffic are expected on 4G LTE, rapidly scalable networks with load balancing and redundancy are critical.

CONCLUSION

Architecturally robust new wireless technologies, such as 4G LTE, bring enormous service potential to the market; however, they are vulnerable to security threats and risk. If threats from external attackers were not enough, everything from business objectives, business models and network operations to security infrastructure and legislation must be scrutinized by risk management to ensure business success. From the perspective of users (consumers and businesses) who are migrating data traffic to 4G LTE services, inquiring about the MNO's security standards, business models and operations is a worthwhile pursuit. No matter how advanced the technology, risk management is essential to ensuring security.

> "No matter how advanced the technology, risk management is essential to ensuring security."

AUTHOR'S NOTE

Opinions expressed in this article are the author's and not necessarily those of her employer.

ACKNOWLEDGMENT

The author would like to thank Tyson Macaulay, vice president global telecommunications strategy, McAfee (Intel), for inspiration, guidance and insights shared.

ENDNOTES

[1] Juniper, press release, 13 February 2013, *www.juniperresearch.com/viewpressrelease.php?id=528&pr=363*

[2] Global mobile Suppliers Association (GSA), "GSA Evolution to LTE Report: 163 Commercial Networks Launched; 415 Operators Investing in LTE," 7 April 2013, *www.gsacom.com/news/gsa_375.php*

[3] McAfee, "McAfee Threat Report: Fourth Quarter 2012," McAfee Labs, USA, 2012

[4] Cisco, "Cisco VNI—Mobile Data Forecast 2012-2017," Cisco, 2013, *www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html*

[5] Ovum, "Mobile Network Sharing: A post-recession reality," September 2010, *www.researchandmarkets.com/reports/1396699/mobile_network_sharing_a_postrecession_reality*

[6] Forrester, "Privacy and Data Protection by Country," 2013, *http://heatmap.forrestertools.com*

[7] ETSI, "Lawful Interception," 2013, *www.etsi.org/index.php/technologies-clusters/technologies/security/lawful-interception*

Stefan Beissel, Ph.D., CISA, CISSP, is an IT security officer responsible for the management of security-related projects and compliance with the Payment Card Industry Data Security Standard (PCI DSS) at EVO Payments International.

Meeting Security and Compliance Requirements Efficiently With Tokenization

The processing of sensitive data requires compliance to standards and laws that include high demands on data security. Companies that process sensitive data do not always need the specific data content in every processing step. Sometimes only the unique identification of the data is required. Tokenization replaces sensitive data with unique strings that cannot be converted back to the original data by an algorithm. Systems that use these strings do not need to handle sensitive data anymore. Therefore, the scope of systems that must meet compliance and audit requirements can be reduced via tokenization.

BASICS OF TOKENIZATION

Tokenization strings are surrogates used to uniquely identify a piece of data and contain no information beyond the token. The fact that sensitive data are replaced with tokens reduces the number of systems that work with sensitive data and, therefore, the risk of compromise. Systems that only process tokens are not required to meet as high security requirements as those that process sensitive data. As a result, the scope of systems that must be compliant to standards and laws is reduced.

Examples for compliance requirements are the Payment Card Industry Data Security Standard (PCI DSS) and the numerous national laws for the protection of personal data, e.g., the Federal Data Protection Act in Germany (BDSG). PCI DSS was released by the PCI Security Standards Council (PCI SSC), a panel of five credit card companies. PCI DSS is a standard that aims to improve the security of cardholder data and includes requirements for data security and related audit methods. PCI DSS is required when cardholder data or authentication data are stored, processed or transmitted. In particular, the primary account number (PAN) is the defining factor in the applicability of PCI DSS requirements. Tokenization can be used to replace PANs and, thus, restrict the applicability of PCI DSS.

To prevent the compromise of systems that contain personal data, all personal data can be replaced by tokens. This approach is ideal for all data processing operations that deal with ambiguous information and less with the actual content of data, e.g., data mining.

GENERATING TOKENS

Before a token is generated, a fundamental decision has to be made about whether the token will be used once or several times. If a token will be used once, a single token is created for each data value, for example, by a sequential number. If a token will be used several times, the same token is created for the same data value. In the latter case, the same token occurs several times in the processing systems and allows cumulative evaluations. The frequency of use must be considered in the generation technique. While encryption and hashing automatically create the same token for the same data value, token generation with numbers needs an additional mechanism that checks whether a token has already been created for the same data value and provides the token for reuse.

Encryption techniques are used to change data by algorithms to a form called ciphertext, so that the data have no similarity to their original form of representation, called plaintext, but can be converted back to their original state by a key.[1, 2] Because tokens generated with ciphertext can be converted to their original state, encryption techniques are less suitable to generate tokens. According to the PCI SSC,[3] encryption techniques are a way to generate tokens, but this does not mean that sensitive data are completely protected against decoding to cleartext. Therefore, encrypted data should not be processed in uncertain environments and should not be taken out of the PCI DSS environment that includes all protected systems.

Hashing is a technique originally used for ensuring the integrity of data. When data are transmitted, hashing can ensure that the

data have not been tampered with or corrupted during transmission.[4, 5] Using hashing with a data packet creates a digital fingerprint (hash value or message digest) that is as unique as possible. Therefore, hash values can be used as tokens. Depending on the algorithm used, the risk of collisions is present[6] and the uniqueness of the token is no longer ensured. The best known hashing algorithms are MD5 and SHA-1. MD5 was developed by Ron Rivest in 1991 and uses a hash value with a size of 128 bits. MD5 is now generally considered insecure as a result of collisions. SHA-1 was released by the US National Institute of Standards and Technology (NIST) in 1994 and is a revision of SHA. SHA-1 hash values have a size of 160 bits. Extensions with larger hashes are SHA-2, released in 2001, and SHA-3, released in 2012.

Other techniques for the generation of tokens are the use of a serial number or a random number that is generated using a pseudo random number generator.[7] In principle, any string may be used as a token as long as it creates a unique identification, allows almost no collisions and cannot be converted by an algorithm to its original state.

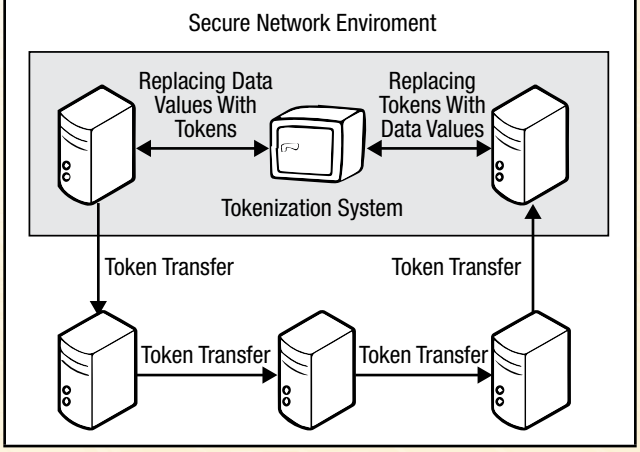
Tokens can be generated not only for individual data, but also for data sets that consist of a combination of two or more data values. Prior to the generation of the token, a data value may be further attached to the primary data value like a salt. A salt is a string that is appended to an existing string before encryption or hashing.[8]

ASSIGNMENT OF TOKENS

Since tokens are unique, each token can be associated with its original data. This mapping is performed by a tokenization system. Since the mapping is not possible with only the use of mathematical algorithms, the tokenization system must maintain mapping data. Where sensitive data must be present only in certain process steps and not continuously, tokens can be used partially, and, when necessary, the tokens are allocated to the original data values by the tokenization system.

The tokenization system must be set up in a secure network environment (see **figure 1**). When in use, all systems that contain tokens, but no sensitive data, can be removed from the secure network environment. The secure network environment contains only systems with increased security requirements, for example, specified by PCI DSS.

Figure 1—Limiting the Secure Environment



Therefore, tokenization systems must be well protected. They include mapping data that allow the assignment of a token to the original data and their compromise can affect all token processing systems. In addition to the tokenization requirements of the PCI SSC (listed in the Regulation and Sampling section of this article), strong cryptography is needed for the encryption of sensitive data.[9] Examples of acceptable encryption algorithms are AES (128 bits and higher), TDES (minimum double-length keys), RSA (1024 bits and higher), ECC (160 bits and higher) and ElGamal (1024 bits and higher).

AUDITING A TOKENIZATION SYSTEM

To assure that a tokenization system complies with IT security requirements, audits should be conducted. The main protection objectives of IT security are confidentiality, integrity and availability. Regulation and cost-effectiveness should also be taken into account when defining audit objectives.

Confidentiality

Maintaining confidentiality requires that data cannot be viewed by unauthorized persons and thus cannot be compromised. Physical and logical access controls prevent unauthorized penetration into the area where the hardware of the tokenization system can be found and into virtual spaces where tokens are assigned to sensitive data. A segmentation of the network can be used to control and limit access from insecure network segments to the secure network segment in which the tokenization system is located. This can be

achieved, for example, by using a firewall that filters network traffic. Furthermore, routers with access control are also suitable by generating a virtual local area network (VLAN). Encryption of data contained in the tokenization system prevents captured data from being read by, for example, the recording of network traffic or the theft of a hard drive from the tokenization system. Basically, the data packets can be encrypted individually by, for example, Pretty Good Privacy (PGP) encryption of files or the data transfer can be encrypted completely by using an encrypted communication channel with, for example, Secure Shell (SSH), a virtual private network (VPN) or Secure Sockets Layer/Transport Layer Security (SSL/TLS). A hard-disk encryption can be implemented with software, which can be operating system (OS) vendor software, such as Bitlocker, or third-party software, such as Truecrypt, and with hardware containing encryption modules. Secure deletion ensures that deleted files cannot be recovered by unauthorized persons. In addition to rendering the physical media useless by destroying or degaussing, there are software solutions that offer repeated overwriting of the data.

By monitoring the logs at the tokenization system, irregularities in system behavior can be detected. Such a detection indicates attacks or technical malfunctions (log management). Recognized irregularities can be reported through alerts to system administrators who initiate measures. Automation is possible through the use of intrusion detection systems (IDS) (for automatic monitoring and alerting) and intrusion prevention systems (IPS) (for response to identified attacks, e.g., by a dynamic adjustment of access rights). Antivirus software prevents malicious software from starting and changing files or tapping data. Malicious software includes viruses that are active when executed by the user, worms that spread independently by exploiting vulnerabilities and Trojans that are disguised as harmless programs. The components of the tokenization system must be protected against software vulnerabilities. To protect them against vulnerabilities, the system must be hardened. Standard parameters are adjusted, and all features and services that are not required are uninstalled or disabled to offer no unnecessary points of attack. Security updates from software vendors must be installed periodically (patch management). In addition, vulnerability scans provide information on existing vulnerabilities of the system. Increased security awareness among users reduces the risk of users being victims of social engineering. In addition, security awareness reduces the risk of careless users storing sensitive data outside the secure environment. The measures that are used to protect confidentiality also serve to protect integrity. If data are compromised by an attacker or malicious software, they can often be damaged or tampered with as well.

Integrity

Integrity means that data are not tampered with or damaged by unauthorized persons. To ensure the integrity of data within the tokenization system, three principles should be applied. The need-to-know principle states that users should have only as much permission on the tokenization system as they absolutely need to carry out their duties, to prevent unauthorized manipulations beyond their tasks. The separation-of-duties principle states that one person should not be responsible for all aspects of a business process, to ensure that unauthorized manipulations can be noticed by colleagues. The rotation-of-duties principle states that responsibilities are exchanged regularly between users, to ensure that a user can be replaced and unauthorized manipulations of colleagues can be noticed.

Internal company policies and work instructions should be used to implement these principles.

Availability

Availability means that users or systems that are authorized to access data can access these data at any required time. The availability of a tokenization system can be guaranteed by hardware and infrastructure that are ready for use and have sufficient capacity to process all requests as quickly as necessary. Attackers can compromise the availability by flooding the tokenization system with requests and, thus, cause a denial of service. Protection against an attacker can be achieved with a web application firewall, which is designed specifically to protect web applications. Capacity planning

can prevent a strong utilization of the systems due to personal growth, for example. Capacities are also at risk due to external influences, such as environmental disasters. Business continuity management is necessary to guarantee the operation of the tokenization processes in case of disturbances. A part of business continuity management is disaster recovery, which ensures the quickest possible restoration of the tokenization system after a total system failure.

Regulation and Sampling

Tokenization systems can be used in various fields, such as health care and finance, for the implementation of data privacy requirements to ensure PCI DSS compliance. So far, only the PCI SSC has published special security requirements for tokenization systems.[10] In addition, general security requirements of the PCI DSS are valid.[11] These requirements relate primarily to confidentiality. The protection of integrity and availability is the responsibility of the company after evaluating the cost/benefit aspects.

The control measures that result from the security requirements (see **figure 2**) can be verified by using sampling techniques. There is a basic distinction between statistical and nonstatistical sampling methods.[12] For the verification of one control measure, different sampling techniques are usable in most cases.

The selection of sampling techniques should be based on current risk assessments. When considering access controls, discovery sampling (statistical) can be used, in which case samples are taken until a user account with too powerful permissions has been discovered. With compliance sampling (statistical), a sufficient password complexity of user accounts is verified. And with judgmental sampling (not statistically),

Figure 2—Security Requirements

Security Requirement	Control Measurement	Regulation
Access control	Active Directory, LDAP, kerberos	PCI DSS (p. 44 ff. and 51), Tokenization Guidelines (p. 10 f.)
Network segmentation	Firewall rules, VLAN	PCI DSS (p. 10 f.), Tokenization Guidelines (p. 10)
Control of communication	Firewall rules	PCI DSS (p. 20 ff.)
Encryption of internal data transmission	PGP, SSH, VPN, SSL/TLS	Not available
Encryption of external data transmission	PGP, SSH, VPN, SSL/TLS	PCI DSS (p. 35)
Encryption of files	Encryption software	PCI DSS (p. 31)
Encryption of hard drives	Encryption software, hardware modules	PCI DSS (p. 31)
Secure deletion of media	Secure deleting, physically destroying, degaussing	PCI DSS (p. 28)
Logging, monitoring and alerting	Log management, IDS/IPS	PCI DSS (p. 55 ff.), Tokenization Guidelines (p. 11)
Antivirus software	Client software, virus walls	PCI DSS (p. 37)
Protection against vulnerabilities	Hardening, patch management, vulnerability scans	PCI DSS (p. 24 ff., 38 f., 60)
Security awareness	Training, information	PCI DSS (p. 67)
Need-to-know principle	Policies, work instructions	PCI DSS (p. 44 f.)
Separation-of-duties principle	Policies, work instructions	Partially in PCI DSS (p. 40)
Rotation-of-duties principle	Policies, work instructions	Not available
Capacities	Planing and monitoring	Not available
Protection against denial-of-service attacks	Web application firewall	Indirectly in PCI DSS (pp. 20 ff. and 43)
Business continuity management	Business continuity plan, disaster recovery plan	Partially in PCI DSS (p. 68)

Source: PCI Security Standards Council, *PCI DSS Tokenization Guidelines*, 2011, *www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf*; PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard—Requirements and Security Assessment Procedures, Version 2.0*, 2010, *www.pcisecuritystandards.org/documents/pci_dss_v2.pdf*

risky user accounts such as unnecessary administrator accounts can be determined manually.

Cost-effectiveness

For credit card processing companies, it is necessary to set up a PCI-DSS-compliant environment because the failure of passing the annual PCI audit would result in significant revenue losses. In addition, loss of reputation and possible fines by credit card companies can be expected. However, there is design freedom in the determination of control measures for the PCI-DSS-compliant environment. Companies can decide between different technologies or products such as PGP, SSH, VPN or SSL/TLS for encryption of external data transfer. Other companies that are bound only in relation to data privacy and want to define their own level of security have even greater design freedom.

To assess the performance of a tokenization system, the investment costs and running costs must be compared to the potential savings. The capital costs of a tokenization system include the costs of new hardware and software, installation and network segmentation using routers or firewalls. In addition, organizational activities, such as the creation of work instructions and guidelines, have to be considered. The running costs include maintenance of the system and administration. Potential savings result from the fact that the scope of the secure network environment can be more limited. Audits and reviews can be more focused on the secure network environment and, therefore, can be performed more efficiently. The administration effort in the less-secure network environment is reduced because fewer requirements must be implemented, for example, on the topics of hardening, encryption and logging.

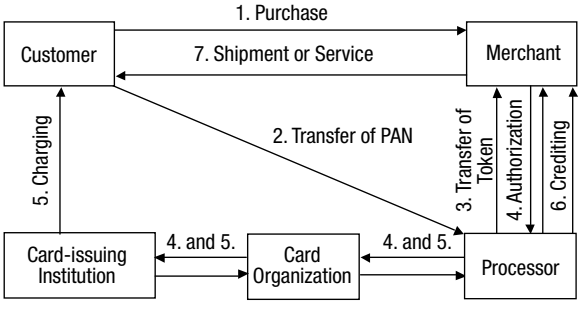
If the implementation of tokenization is desired, its sustainability should also be taken into consideration. If planned business changes can influence the processed data, the tokenization system should be designed to be scalable. This could be the case if, for example, outsourcing of the data processing is planned and, therefore, no more tokenized data are processed internally. In addition, technological developments can result in insecure cryptographic algorithms due to higher available computing power. Cryptographic algorithms need to be regularly evaluated and replaced, as necessary.

USE CASE E-COMMERCE

An exemplary use case for a tokenization system is the integration of an e-commerce merchant, who accepts credit card payments through a web store. The flow of a transaction in e-commerce begins with the customer who makes a purchase at the online store and pays with his/her credit card. After the customer has communicated his/her card information to the merchant, the transaction is routed through the processor to the card organization, which performs an authorization request to the card-issuing institute. If the following authorization response is positive, the payment is approved. The merchant then receives a confirmation and the payment amount is charged to the customer. Then the merchant ships the purchased goods or provides the desired service. The settlement of the payment is made by the card-issuing institution, which charges the payment amount to the end user and credits it to the card organization. The card organization forwards the credit to the processor, who transfers the accumulated credits in contractually agreed payment cycles to the merchant.

The storage, processing or transmission of PANs by the merchant require the application of PCI DSS. It is most advantageous for the merchant organization to keep payment data outside of its network by using tokenization without having to change any technical processes.[13] In a token-based method, the merchant must ensure that the web session is redirected to the systems of the processor, e.g., by using a plug-in, before the payment information is entered by the customer. The customer enters his/her PAN and, thus, sends it directly to the processor, which operates a tokenization system. The processor assigns the PAN in its tokenization system to a multiusable token and sends the token to the merchant (**figure 3**).

Figure 3—Token-based E-commerce Transaction Flow



Specifications for the composition of a PAN are given in ISO 7813. According to these specifications, a PAN consists of a six-digit issuer identification number (IIN), a variable account number with at most 12 individual digits and a check digit, which is generated by the Luhn algorithm. For example, a PAN "4000300020001000" is converted by the SHA-1 hashing algorithm to the token "c4caec101d38c68005fa56806153bcbcb70586c0." The technical processes of the merchant do not have to be changed if length and format of the token do not infringe on any technical restrictions (i.e., specified data types in databases). Within the infrastructure of the merchant, the token can then be treated in the same way as the PAN. The merchant can determine if the same PAN is used again for a purchase based on the uniqueness of the token without knowing the actual PAN. Subsequent transactions by existing consumers can be handled without storing the PAN in the network of the merchant. In addition, consumers who often cause chargebacks can be identified by the token before completing the transaction. Chargebacks are reversals that are mandatory by law in case of invalid authorizations (§ 675j BGB and § 675p); however, they are also performed as an optional service provided by the card organizations if requested by the cardholder.

> "Tokenization facilitates a more restrictive handling of sensitive data without adjusting business processes."

CONCLUSION

The scope of systems that handle sensitive data and, therefore, must meet compliance and audit requirements can be reduced by using tokenization. Tokenization facilitates a more restrictive handling of sensitive data without adjusting business processes. Therefore, tokenization offers potential savings. When implementing a tokenization system, security provisions and cost-effectiveness should be taken into consideration.

ENDNOTES

1 Buchmann, J.; *Einführung in die Kryptographie, 5th Edition*, Germany, 2010
2 Schmeh, K.; *Kryptografie: Verfahren, Protokolle, Infrastrukturen, 4th Edition*, Germany, 2009
3 PCI Security Standards Council, PCI DSS Tokenization Guidelines, 2011, *www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf*
4 *Op cit*, Buchmann
5 *Op cit*, Schmeh
6 *Op cit*, Buchmann
7 Stapleton, J.; R. S. Poore; "Tokenization and Other Methods of Security for Cardholder Data," *Information Security Journal: A Global Perspective*, vol. 20, iss. 2, 2011, p. 91-99
8 Ertel, W.; *Angewandte Kryptographie, 3rd Edition*, Germany, 2007
9 PCI Security Standards Council, *Glossary of Terms, Abbreviations, and Acronyms, Version 1.2*, 2008, *www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf*
10 *Op cit*, PCI Security Standards Council, 2011
11 PCI Security Standards Council, *Payment Card Industry (PCI) Data Security Standard—Requirements and Security Assessment Procedures, Version 2.0*, 2010, *www.pcisecuritystandards.org/documents/pci_dss_v2.pdf*
12 ISACA, *IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals*, 2013, *www.isaca.org/Knowledge-Center/Standards/Documents/ALL-IT-Standards-Guidelines-and-Tools.pdf*
13 *ISO & Agent*, "HP Upgrades Tokenization of Payment Data," vol. 8, iss. 11, 2012, p. 17

Privacy Audit—Methodology and Related Considerations

Muzamil Riffat, CISA, CRISC, CIA, CISSP, PMP, has more than 10 years of experience in software development, IT audit and security. He has worked for consultancy, private, semi-government and government organizations. He holds several general and vendor-specific professional certifications. Riffat is currently responsible for IT audit function in a large government organization.

Auditors should consider key risk and control points when performing privacy audits. The following methodology draws heavily on concepts presented in ISO 31000:2009 *Risk management—Principles and guidelines*.

WHY CONDUCT A PRIVACY AUDIT?

Before considering the details of the privacy audit methodology, it is important to consider the reasons for conducting a privacy audit and the difference between confidentiality and privacy.

The objective of a privacy audit is to assess an organization's privacy protection posture against any legislative/regulatory requirements or international best practices and to review compliance with the organization's own privacy-related policies. The scope involves evaluating procedures undertaken by an organization throughout the typical information life-cycle phases: how information is created or received, distributed, used, maintained and eventually disposed of. As information and data have transformed from being scarce to superabundant, the privacy audit presents the status of risk associated with potential information misuse and recommends initiatives that can limit an organization's liability or reputational risk.

THE DIFFERENCE BETWEEN CONFIDENTIALITY AND PRIVACY

Although frequently used interchangeably, confidentiality and privacy have distinct meanings. In this context, *confidentiality* can be referred to as the protection of information sharing without the express consent of the owner. *Privacy*, on the other hand, is freedom from intrusion into private matters. For example, external consultants working on a project within the organization might have access to private information (e.g., human resources records, customer databases), but they should not share this information with any other party as an expectation of maintaining confidentiality. At an individual level, privacy is guaranteed by the United Nations' Universal Declaration of Human Rights (Article 12): "No one shall be subjected to arbitrary interference with his privacy...," and "Everyone has the right to the protection of the law against such interference or attacks."[1] In today's world, companies act more or less with a notion of "corporate personhood," that is, they can own assets, including intellectual properties, and engage in contractual relationships. Therefore, the concept of privacy can be easily imagined to be extended to corporations as well.

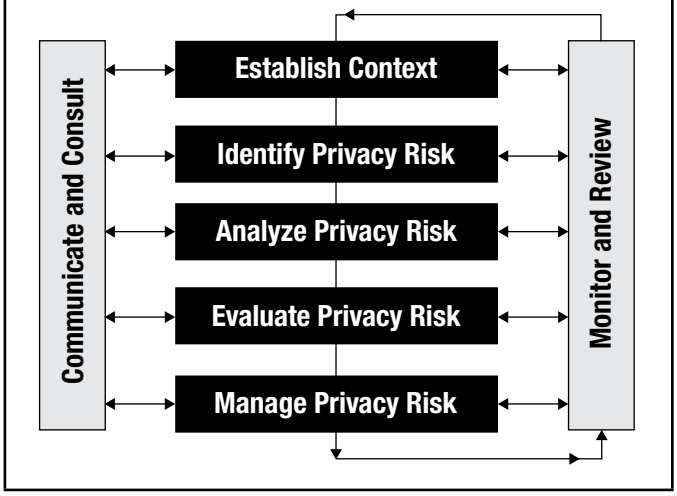
PRIVACY AUDIT METHODOLOGY

The high-level steps of the methodology that can be adopted to conduct a privacy audit are illustrated in **figure 1**.

The related considerations for each step are as follows:

- **Establish context**—A key challenge in any privacy-related discussion is that it is a very subjective phenomenon. A substantial amount of grey area always creeps in whenever attempts are made to define privacy, as there is no

Figure 1—Privacy Audit Methodology Based on ISO 31000:2009



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:

universally agreed-upon understanding. The interpretation may vary significantly by country, culture or organization. For instance, most organizations nowadays set up a banner notification on computer login screens about monitoring the activities of the user and deploy some sort of technical tools on their network for this task. However, it is debatable to what extent the organization can utilize these data. Some argue that monitoring data (e.g., search terms, web sites visited, products purchased) on an organization's resources (e.g., computer, Internet) during official working hours is not a violation of privacy, even if the company sells these data to an external party. Others term such actions as intrusion of privacy. The paramount question of who is the data owner (the company that collected the data or the individual[s] who produced the data) is given a fair amount of consideration. It is imperative for auditors to ensure that all stakeholders are aligned to the criteria used and the outcome of the proposed privacy audit.

- **Identify privacy risk**—The next step is to identify privacy-related risk by utilizing the usual risk identification tools, techniques and methods. Although listing all possible privacy risk is beyond the scope of this article and may not be practical, the following emerging risk areas should be part of this step:
  - Operating model—Hosted computer solutions (cloud computing[2]) are increasingly considered by corporations. Without a reasonable degree of research, judgments are swiftly promulgated about the perceived evils of the hosted solutions. Auditors should objectively review the associated risk and assign the risk rating accordingly, keeping in mind that the concept of hosted solutions is neither novel nor abstract. Furthermore, cloud computing is not inherently bad news for privacy concerns. Such concerns are based on the unfounded belief that data kept in-house are somehow more secure. As a matter of fact, the security of data is dependent upon the security measures utilized by the organization and not on location—in-house or in the cloud.
  - Social media—Social media has provided an excellent way for companies to communicate with their customers and stakeholders on a timely basis. However, as is possible for personal social media accounts where information from different sources can be aggregated to reveal sensitive information, it may be possible for companies to be publishing seemingly innocuous information, but when combined or correlated with other sources, the information disclosed is private.
  - Mobile devices—The skyrocketing ownership of smart mobile devices has given rise to security concerns related to bring your own device (BYOD). From a privacy perspective, the following points are worth extra consideration:
    - Location data—The integration of navigation systems in the inherent cell-tower triangulation position system has raised some genuine privacy concerns. Geolocation data from mobile devices are considered to be sensitive.[3] These data can be used for (unwanted) marketing to consumers based on location or for tracking the movement of users. Different guidelines are being developed to address the privacy of location-based data.[4]
    - Hardware identifiers—Mobile apps can access unique hardware identifiers for marketing and other communication purposes to the consumer. Permission for such tracking might not have been explicitly granted by the owner of the device.
    - Personal utilities or games—Some mobile apps can gain unwarranted access to the utilities on the phone, which are not required for the intended purpose of installing the application.
  - Big data—The rapid enhancements in data collection and analytics technologies are resulting inversely in privacy erosion. Sophisticated tools can correlate data from different sources to identify personal or private information. The data warehouse created to analyze and

provide business benefits can also result in unintended leakage of private information.
  – Conflict with other laws—Data privacy requirements can sometimes conflict with other laws, e.g., data retention laws.
- **Analyze privacy risk**—Risk analysis predominantly consists of performing two steps:
  1. Assign inherent risk rating.
  2. Evaluate implemented controls.

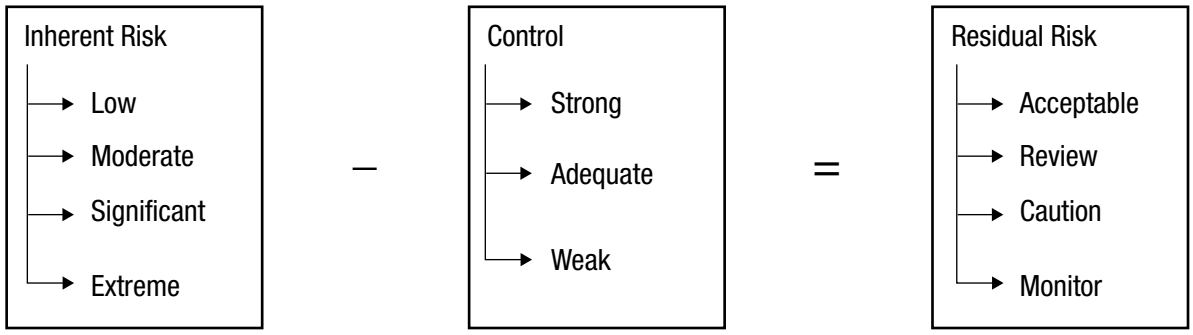
  Inherent risk rating can be assigned to each risk using an impact/consequence and probability matrix (see example in **figure 2**).

  The effectiveness and efficiency of implemented controls should be assessed to evaluate the degree of risk mitigation. Examples of privacy controls that an organization may have or may wish to implement include, but are not limited to:
  – Privacy policy—A policy should be documented, approved and communicated to all employees and stakeholders. In addition to taking any regulatory requirements into consideration, the policy should disclose management's intention on information collection and its subsequent usage.
  – Database privacy controls—Cell suppression, partitioning, noise and perturbation are some of the techniques that can be used to mitigate risk associated with inference and aggregation attacks. In these kinds of attacks, information from different sources (e.g., online voter registration records, phone records, social network sites) is linked to disclose private information. For instance, a privacy enthusiast and researcher revealed the private health records of a governor of a US state using publicly available databases in a quintessential reidentification attack.[5] Techniques such as privacy integrated queries (PINQ) could be used to provide privacy for underlying records.[6]
  – Cryptography—As required by several standards, including the Payment Card Industry Data Security Standard (PCI DSS), all personally identifiable information (PII) has to be stored in an encrypted format to prevent misuse or unauthorized access to such information.

Figure 2—Inherent Risk Rating Matrix

		Consequence/Impact				
		1—Notable	2—Minor	3—Moderate	4—Major	5—Severe
Probability	5—Definitely	Moderate risk	Significant risk	Significant risk	Extreme risk	Extreme risk
	4—Likely	Moderate risk	Significant risk	Significant risk	Extreme risk	Extreme risk
	3—Possible	Moderate risk	Moderate risk	Significant risk	Significant risk	Extreme risk
	2—Unlikely	Low risk	Moderate risk	Significant risk	Significant risk	Extreme risk
	1—Rare	Low risk	Low risk	Moderate risk	Moderate risk	Significant risk

Figure 3—Privacy Residual Risk Calculation



- **Evaluate privacy risk**—The residual risk is calculated based on inherent risk and control ratings. Residual risk is the level of risk that remains after taking into account all existing controls. **Figure 3** shows a suggested equation for residual risk calculation.
- **Manage privacy risk**—This step is primarily performed by management, and the auditor's role generally is to ascertain the adequacy of the steps taken to mitigate risk. Using residual risk rating as a basis, risk management initiatives can be identified. Such initiatives might include strengthening the current controls or implementing new controls to mitigate privacy-related risk. There are several forms of risk management, such as avoidance, transfer or reduction to an acceptable level, after taking into consideration the cost vs. benefit of the risk treatment.
- **Communicate and consult**—Periodic reports should be provided to management, the audit committee and any other stakeholder during each phase of the methodology. Any major areas of concern should be brought to management's attention immediately.
- **Monitor and review**—The performance of the privacy risk management system should be continuously monitored. Regulatory requirements, internal processes and business processes might change, which, in turn, could affect privacy risk management practices. Appropriate monitoring and review processes should be completed throughout the risk management process to ensure that all decisions are made based upon current and up-to-date information.

CONCLUSION

The notion and understanding of privacy will continue to evolve. Data collection and utilization have already been, and continue to be, even more pervasive, in some cases with the individual's consent, but in many cases without the individual's knowledge. Debates will continue about privacy on one hand and efficiency and convenience on the other. New or updated regulatory requirements are expected to emerge as well.

In this ever-changing scenario, auditors should establish and follow a comprehensive privacy audit methodology to ensure that their organizations are not inadvertently exposed to any undesired risk. Furthermore, steps should be taken to ensure that all privacy-related risk is minimized to an acceptable level. Auditors should also be wary of emerging technological trends and their impact on privacy. Consideration should be given to include privacy audit in the annual audit plan, and reports should be provided on a periodic basis to all stakeholders.

REFERENCES

Kernochan Tama, Julia; "Mobile Data Privacy: Snapshot of an Evolving Landscape," *Journal of Internet Law*, vol. 16, no. 5, November 2012

Enright, Keith P.; Privacy Audit Checklist, *http://cyber.law.harvard.edu/ecommerce/privacyaudit.html*

Determann, Lothar; "Data Privacy in the Cloud: A Dozen Myths and Facts," *The Computer and Internet Lawyer*, vol. 28, no. 11, November 2011

Ohm, Paul; "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, vol. 57, 13 August 2009, p. 1701

ENDNOTES

[1] United Nations, Universal Declaration of Human Rights (Article 12), *www.un.org/en/documents/udhr/index.shtml#a12*

[2] National Institute of Standards and Technology, "Cloud," USA, *www.nist.gov/itl/cloud/*

[3] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012, supra n. 36, p. 59, *www.ftc.gov/os/2012/03/120326privacyreport.pdf*

[4] CTIA—The Wireless Association, "Best Practices and Guidelines for Location Based Services," 23 March 2010

[5] Barth-Jones, Daniel C.; "*The 'Re-identification' of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now,*" 18 June 2012, *www.futureofprivacy.org/wp-content/uploads/The-Re-identification-of-Governor-Welds-Medical-Information-Daniel-Barth-Jones.pdf*

[6] Microsoft, "Privacy Integrated Queries," *http://research.microsoft.com/en-us/projects/pinq/*

Unlocking Hidden Value in ERP System Acquisitions Using Risk Management

Gregory Zoughbi, CISA, CISM, CGEIT, CRISC, COBIT 4.1 (F), ABCP, CISSP, ITIL Expert, PMP, TOGAF 9 (C), is an advisor to chief information officers (CIOs) and chief executive officers (CEOs) on the governance of enterprise IT (GEIT) and business administration. He advocates using business administration concepts in the governance and management of enterprise IT. Zoughbi previously worked at the headquarters of CAE Inc., General Dynamics Canada and BMW Financial Services. He is a recipient of the ISACA CGEIT Geographic Achievement Award.

A proper understanding of a potential enterprise resource planning (ERP) investment's benefits, costs and risk is essential for successfully creating its business case. In particular, the business case includes a net present value (NPV) calculation, but this requires quantifying the benefits, costs and risk.[1] Generally, the NPV increases as benefits increase and as risk and costs decrease. One way to make an ERP investment more attractive is to reduce its risk while ensuring that its benefits minus costs remain constant or increase. One way to achieve this is using risk management practices.[2]

A SIMPLIFIED RISK MANAGEMENT PROCESS

Various frameworks and standards for risk management exist, including ISACA's Risk IT,[3] ISO's 31000:2009 Risk Management,[4] Committee of Sponsoring Organizations of the Treadway Commission (COSO)'s *Enterprise Risk Management—Integrated Framework*[5] and the National Institute of Standards and Technology (NIST)'s Special Publication (SP) 800-30 *Guide for Conducting Risk Assessments*.[6] A simplified risk management process is illustrated in **figure 1**.

The process begins by defining the scope and context for risk management. This is then followed by a risk assessment step in which risk is identified and analyzed qualitatively and, as much as possible, quantitatively.

Once risk is understood, controls can be added to reduce the likelihood of the risk occurrence or its impact. Because risk is a function of its likelihood and impact, reducing either of those elements results in a reduced residual risk (the risk that remains after a control is implemented). In addition, a control may be added to transfer the risk, in full or in part, to third parties, e.g., by purchasing insurance. In this way, the impact of risk to the organization is reduced. Finally, risk can also be reduced by avoiding the activities or circumstances that create the risk scenario.

As a result, acceptable residual risk—the risk that remains after risk treatment—remains. Risk management is a cyclic process, so scope definition, or revision, follows. Risk must be continuously monitored so that appropriate responses are taken.

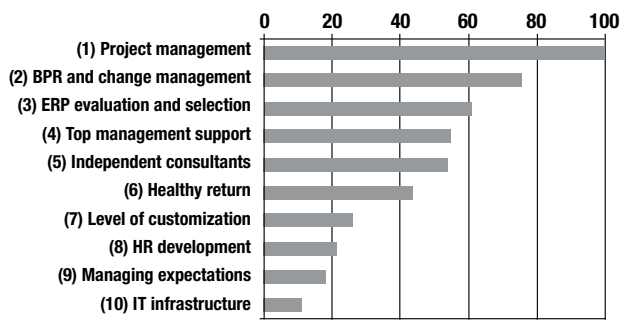
ERP RISK ASSESSMENT

An appropriate risk assessment requires identifying and understanding risk factors, which are "those factors that influence the frequency and/or business impact of risk scenarios."[7] Risk factors common across ERP system acquisitions are presented in **figures 2** and **3**.[8, 9]

Figure 1—A Simplified Risk Management Process

Figure 2—ERP Risk Factors and Corresponding Concerns		
#	Risk Factor	Corresponding Areas of Concern
1	Project management	Implementation plan. Budget estimates. Schedule estimates. Project manager's capability. Team size estimates. Team strength and composition. Team commitment. Testing quality. Software release management. Project monitoring and control. Project work environment. Empowering team members. Training team members.
2	Business process reengineering (BPR) and change management	Focus of requirements (make it business-driven, not technical-driven). Strategic alignment. Requirements-functionality mapping analysis. Balance of BPR vs. tool customization. User and project readiness for reengineered processes. Integration of ERP and other systems. Business process mapping (as-is and to-be). Business process standardization. Data robustness across processes. Data accuracy across processes. Fitness of the ERP system and its processes. Incremental implementation. Proper organizational change management. Proper job design. User involvement in BPR. User training on new processes.
3	ERP evaluation and selection	Business requirements definition. Vendor evaluations. ERP software's fitness for purpose. Performance measures for the system. Defining deadlines and milestones. Timely implementation. Detailed project plan.
4	Top management support	Involvement and commitment of business executives. Allocation of sufficient financial and human resources. Resolution of political problems. Communication with employees. Cooperation between IT and business managers.
5	Independent consultants	Involvement of external experts. Their involvement throughout the life cycle. Their ERP and BPR project experience. Their soft skills, e.g., communication, professionalism. Their value-added expertise, in relation to in-house experts. Their managerial support. Their technical support.
6	Healthy return (including cost control and postimplementation performance measurement)	Validating the business case throughout the ERP life cycle. Establishing key performance indicators (KPIs), including benefits realization KPIs. Calculation of return. Proper user awareness and training on ERP system. Close tracking of implementation costs. Consideration of all project risk factors. Early establishment of an ERP vision.
7	Level of customization	Limiting customization to must-have advantages. Leveraging best practices from standard processes in the ERP system.
8	Human resource development (IT staff and users)	User training and documentation on ERP system. IT staff training on ERP system maintenance and support. Including all employees in ERP implementation. Refraining from using the ERP system to reduce employee headcounts.
9	Managing expectations	Establishing realistic expectations. Managing stakeholders' expectations. Alerting top management on ERP system complexity, associated risk and possible complications.
10	IT infrastructure	Consideration of existing IT infrastructure. Proper IT infrastructure with an appropriate budget. Integrity of existing databases.

Figure 3—Relative Importance of Various ERP Risk Factors



ERP RISK TREATMENT AND ITS IMPACT ON THE BUSINESS CASE

In NPV calculations, risk is represented by the discount rate for future cash flows. Because organizations require higher returns on riskier investments, the discount rate changes in the same direction as the risk—an increase in risk results in a higher discount rate and *vice versa*, i.e., the higher the discount rate, the less the impact of future cash flows on the NPV. If one reduces risk, the discount rate for future cash flows decreases, thus leading to an increased impact of future cash flows on the NPV. Because net cash flows attributed to ERP systems are more likely to be positive in later years, reducing the risk and the discount rate generally results in a higher NPV. This makes the business case for an ERP system acquisition more attractive.

Figure 4 illustrates an NPV calculation example for an ERP system acquisition based on a nine-year life cycle. In this example, risk treatment resulted in reducing the discount rate from 15 percent to 10 percent, which resulted in increasing the NPV from a negative US $487,000 to a positive US $1,549,994. As a result, a previously unattractive investment became desirable with proper risk treatment. One way to estimate the discount rate is to compare the investment being evaluated to other investments with known risk and discount rates. These may be, for instance, past investments of this organization or similar investments of other organizations.

Figure 4—An NPV Calculation Example Before and After Risk Treatment

Year	Transaction	Cash Flow ($)		
		Future Value	Present Value Before Risk Treatment (discount rate = 15%)	Present Value After Risk Treatment (discount rate = 10%)
0	Investment	(8,000,000)	(8,000,000)	(8,000,000)
1	Savings	(1,500,000)	(1,304,348)	(1,363,636)
2	Savings	1,000,000	756,144	826,446
3	Savings	2,000,000	1,315,032	1,502,630
4	Savings	3,000,000	1,715,260	2,049,040
5	Savings	4,000,000	1,988,707	2,483,685
6	Savings	4,000,000	1,729,310	2,257,896
7	Savings	3,000,000	1,127,811	1,539,474
8	Savings	1,000,000	326,902	466,507
9	Savings	(500,000)	(142,131)	(212,049)
		NPV	(487,313)	1,549,994

Note: Negative values appear in parentheses.

As demonstrated, treating risk can significantly alter the business case. Risk related to these risk factors can be treated in various ways. One method is to add administrative controls—"the rules, procedures and practices dealing with operational effectiveness, efficiency and adherence to regulations and management policies."[10] The following are three examples of risk treatment techniques using administrative controls:

- Define IT principles.
- Require professional certifications.
- Enhance the IT governance framework.

DEFINE IT PRINCIPLES

IT principles are "general rules and guidelines, intended to be enduring and seldom amended, that…provide guidance on the use and deployment of all IT resources and assets across the enterprise. They are developed in order to make the information environment as productive and cost-effective as possible."[11]

An organization should define IT principles that are suitable to its context and strategic objectives. The life cycle of ERP systems is measured in years and can exceed a decade. Acquisition alone can take a few years because ERP systems impact the entire organization. For instance, ERP systems include several modules such as finance, human resources (HR), procurement and learning management. Furthermore, each module is often implemented in phases, prolonging the acquisition period. Therefore, it is appropriate to define IT principles to guide ERP system acquisitions.

Given the common ERP risk factors previously discussed, it is possible to define IT principles to mitigate related risk. In essence, IT principles serve as administrative controls to reduce the likelihood and/or impact of risk. **Figure 5** provides examples of IT principles for the ERP risk factors. For example, an IT principle to "involve top management in key decisions and obtain their support" can reduce risk related to top management support (risk factor number four in **figure 5**) by addressing areas of concern such as the allocation of sufficient financial and human resources, the resolution of political problems, and communication with employees. Because members of top management contributed to making the decisions, they are more likely to feel like owners of the initiative and, therefore, support it.

REQUIRE PROFESSIONAL CERTIFICATIONS

Organizations can reap benefits by requiring staff and consultants to hold appropriate professional certifications. Certifications provide an independent confirmation of credibility, enable job standardization and, most important, ensure that certification holders are skilled and motivated.[12] Requiring ERP project team members to hold relevant certifications can mitigate ERP system acquisition risk and, therefore, increase the likelihood of acquisition success and business benefit realization. Implementing this should ideally be achieved in collaboration with the HR department.

Figure 5—Examples of IT Principles for ERP Risk Factors		
#	Risk Factor	Sample IT Principles
1	Project management	• Estimate costs based on properly planned and scheduled work to be done. • Base monitoring and control priorities on the float of each path along the project network (lower float requires higher priority). • Use Herzberg's two-factor theory[13] to motivate employees and increase their commitment.
2	BPR and change management	• Involve business experts to define new business processes. • Focus on training and communication. • Consider change impact to individuals.
3	ERP evaluation and selection	• Ensure the ERP system's fitness for purpose. • Maintain a list of preferred vendors. • Maintain generic acquisition guidelines that are shared with vendors.
4	Top management support	• Involve top management in key decisions and obtain their support. • Use top management as change agents.
5	Independent consultants	• Involve independent consultants for projects with budgets above US $100,000. • Require consultants to hold appropriate vendor-independent and vendor-specific professional certifications.
6	Healthy return (including cost control and postimplementation performance measurement)	• Define and monitor benefits realization KPIs. • Validate the business case and project cash flows throughout the ERP system's life cycle. • Utilize activity-based costing (ABC) rather than traditional costing.
7	Level of customization	• Prefer BPR over customization. • Justify each customization based on how it provides a competitive advantage higher than that provided by adopting the ERP system's standard configuration.
8	Human resource development (IT staff and users)	• Never forget training for business users and IT staff. • Ensure that each team in the acquisition life cycle includes company staff and external vendor staff to facilitate knowledge sharing.
9	Managing expectations	• Be careful of vendor-painted images. • Use a stakeholder management model to classify and manage stakeholders.
10	IT infrastructure	• Always revise IT infrastructure's capacity with the expected ERP system's requirements. • Maintain an information architectural model.

Obtaining a professional certification typically requires demonstrating competency by successfully passing an examination and completing a minimum number of relevant years of work experience. For example, ISACA defines task statements and knowledge statements for each of its professional certifications. Task statements are used to demonstrate relevant work experience, whereas examinations are based on knowledge statements. Of special relevance to ERP risk factors are ISACA's Certified in Risk and Information Systems Control™ (CRISC™),[14] Certified in the Governance of Enterprise IT® (CGEIT®)[15] and Certified Information Systems Auditor® (CISA®).[16] CRISC is concerned with risk management and, therefore, is generally relevant to all risk factors. CGEIT and CISA are also relevant to all risk factors, but are likely to be more useful for some risk factors over others. For instance, CGEIT is more relevant for obtaining top management support (risk factor number four) than for project management (risk factor number one) because of governance's focus on executive/top management and boards of directors. Similarly, CISA is more relevant for auditing ERP evaluation and selection (risk factor number three) than for managing expectations (risk factor number nine).

In addition, the Project Management Institute (PMI) defines the Project Management Body of Knowledge (PMBOK)[17] for the Project Management Professional (PMP®)[18] certification. A PMP certification is especially relevant for the ERP project manager and project management team because it requires practicing proper project management (risk factor number one), including ERP evaluation and selection (risk factor number three), obtaining top management support (risk factor number four), and managing expectations (risk factor number nine).

Another relevant certification is The Open Group's TOGAF® 9.[19] TOGAF is an enterprise architecture framework that includes business, information systems and technology architectures in its scope. Therefore, it is relevant to all risk factors but, given the architectural complexity of ERP systems, TOGAF 9 is especially relevant for BPR and change management (risk factor number two) and ERP evaluation and selection (risk factor number three) because they are directly impacted by the architecture.

Furthermore, some non-IT certifications are also relevant. For example, the Institute of Management Consultants USA (IMC USA) defines a common body of knowledge[20] for its Certified Management Consultant (CMC)[21] certification. One may ensure that independent consultants (risk factor number five) hold this certification to ensure that they follow proper consulting practices and utilize CMC competencies for BPR and change management (risk factor number two) and managing expectations (risk factor number nine). Furthermore, various HR certifications are also helpful for human resource development (risk factor number eight).

Other certifications can also be helpful and include the APMG Sourcing Governance Foundation[22] because its scope includes acquisitions and outsourcing. Furthermore, vendor-specific IT certifications, such as those of SAP, Oracle, Microsoft and IBM, are especially important for ensuring technical competency of the ERP product being implemented and its supporting IT infrastructure (risk factor number 10).

Figure 6 summarizes the relationships between these certifications and ERP risk factors.

ENHANCE THE IT GOVERNANCE FRAMEWORK

Establishing and maintaining an IT governance framework is key to effective governance of enterprise IT. Leadership, organizational structures and processes are the key components of an IT governance framework.[23] An effective IT governance framework supports the objective of governance, which is value creation through benefits realization, risk optimization and resource optimization.[24]

Figure 6—Examples of Professional Certifications and Suggested Relevance to the ERP Risk Factors

#	Risk Factor	CRISC	CGEIT	CISA	PMP	TOGAF	CMC	HR-related
1	Project management	■	▒	▒	■	▒	▒	▒
2	BPR and change management	■	■	■	▒	■	■	▒
3	ERP evaluation and selection	■	■	■	■	■	▒	□
4	Top management support	■	■	▒	■	▒	▒	▒
5	Independent consultants	■	■	▒	▒	■	■	□
6	Healthy return (including cost control and postimplementation performance measurement)	■	■	■	▒	▒	□	□
7	Level of customization	■	■	■	□	■	□	□
8	Human resource development (IT staff and users)	■	▒	■	▒	▒	□	■
9	Managing expectations	■	▒	▒	■	■	■	□
10	IT infrastructure	■	■	■	□	■	□	□

Legend:
Black: Relevant
Grey: Partly relevant
White: Not relevant

Every organization should have its own specific IT governance and IT management frameworks.[25, 26, 27] However, they can benefit from established IT governance and management frameworks to reduce the ERP risk factors. For instance, COBIT® 5 and its previous versions introduced processes common to effective IT organizations. Each process is described in detail by identifying, for example, its inputs, practices, outputs, measures and goals. By considering these, an organization can enhance its IT governance and management frameworks by considering lessons learned by other organizations.

Figure 7 illustrates how COBIT 5 can be used to treat risk resulting from top management support (risk factor number four). First, the risk factor's areas of concern are analyzed separately. Next, COBIT 5 processes that can treat risk related to the area of concern are identified. Finally, COBIT 5 processes for all areas of concern for that risk factor are grouped together to form control drivers. As a result, the control drivers become best practice guidance for reducing risk related to the risk factor.

Repeating this process for the top five risk factors identifies the control drivers (**figure 8**). Of these control drivers, eight COBIT 5 processes address approximately 70 percent of the risk related to these five risk factors.

Figure 7—Example Using COBIT 5 Processes to Address Risk Factors

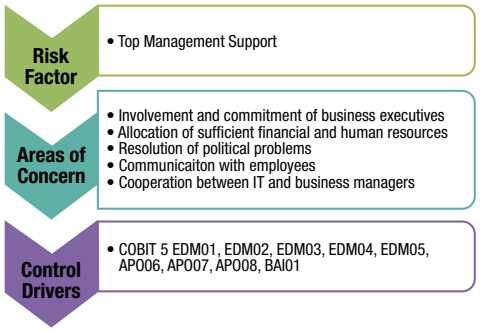
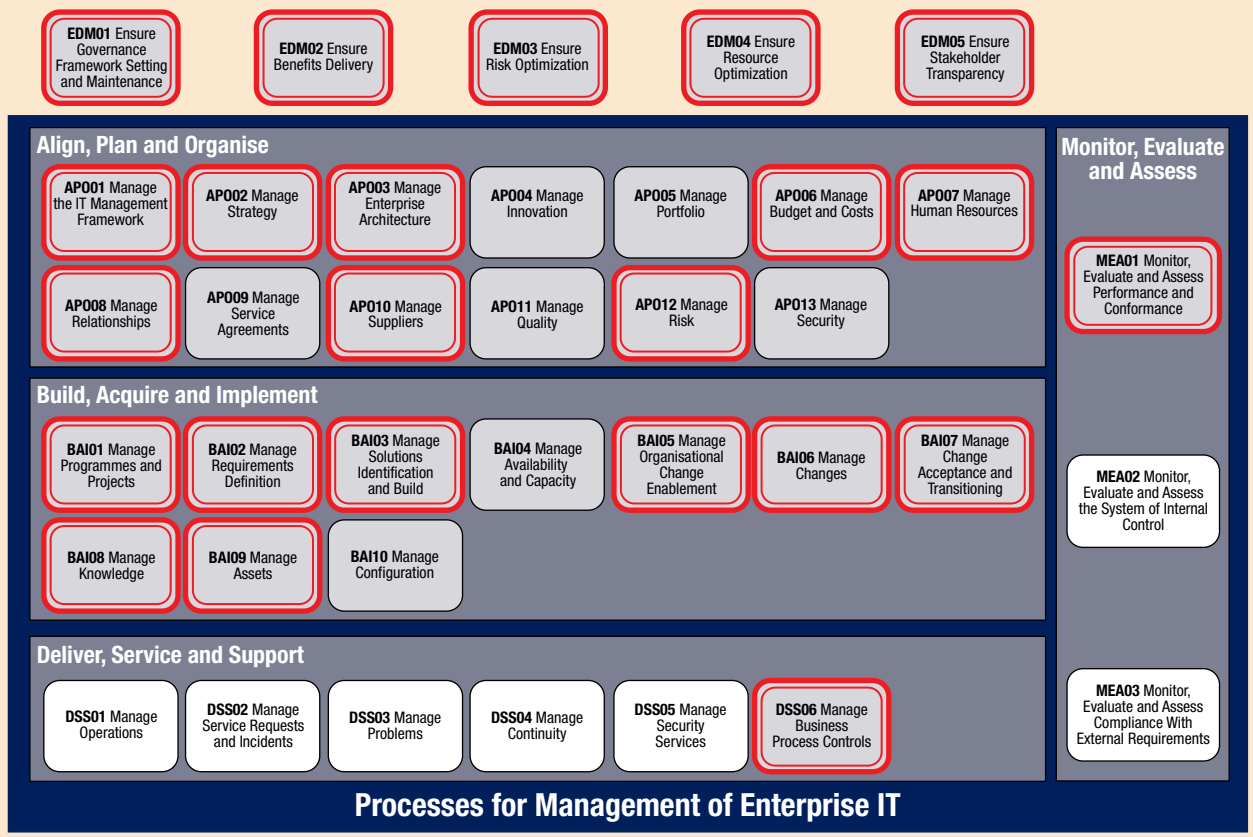


Figure 8—COBIT 5 Processes Used as Control Drivers for Top Five Risk Factors



Adapted from: ISACA, COBIT 5, USA, 2012, *www.isaca.org/cobit*
Based on the results of: Zoughbi, G. *et al.*, "Using Governance and Risk Management Practices to Improve Outcomes of Enterprise Resource Planning (ERP) System Acquisitions," BCS International IT Conference, 2013

This accounts for the difference in risk factor importance and assumes that areas of concern within a single risk factor have equal importance. These control drivers are COBIT 5 EDM01, EDM02, EDM03, EDM04, EDM05, APO07, APO08 and BAI01.

Additionally, other frameworks can also assist with governance-related issues (see, for example, the related guidance section at the end of each COBIT 5 process). For instance, the Information Technology Infrastructure Library (ITIL®)[28] covers IT service management and, therefore, it assists in improving the delivery of IT services including ERP information services. Furthermore, PMBOK is relevant for managing IT projects, and so is *Capability Maturity Model Integration* (CMMI)[29] because it focuses on product development and acquisitions. TOGAF also includes an architecture development method (ADM) that addresses business, information systems and technology architectures. Finally, the APMG sourcing governance[30] is also relevant because it focuses on outsourcing and acquisitions.

Figure 9 identifies the control drivers for the top five risk factors.

Figure 9—Control Drivers for Top Five ERP Investment Risk Factors

#	Risk Factor	Control Drivers
1	Project management	• COBIT 5 APO06, APO07, BAI01 and BAI07 • PMBOK • CMMI process category Project Management (PM) and process areas Verification (VER), Configuration Management (CM), Process and Product Quality Assurance (PPQA)
2	BPR and change management	• COBIT 5 EDM02, APO01, APO02, APO03, APO06, APO07, APO12, BAI01, BAI02, BAI05, BAI06, BAI09 and DSS06 • TOGAF ADM phases A, B and C • CMMI process area Validation (VAL)
3	ERP evaluation and selection	• COBIT 5 APO10, BAI01, BAI02, BAI03, BAI09 and MEA01 • APMG sourcing governance • CMMI process areas Decision Analysis and Resolution (DAR) and VAL, and process category PM • PMBOK
4	Top management support	• COBIT 5 EDM01, EDM02, EDM03, EDM04, EDM05, APO06, APO07, APO08, BAI01
5	Independent consultants	• COBIT 5 EDM01 and EDM04 • APMG sourcing governance • CMMI process area Supplier Agreement Management (SAM)

CONCLUSION

Risk is an important element of an ERP system acquisition business case; its role and impact are tremendous and can completely alter the investment decision. A business case creator must understand risk management practices and make sure appropriate risk management is conducted before a decision is made on the business case. In this way, an organization can avoid rejecting an ERP investment that can produce business benefits if appropriate risk management is performed. Therefore, risk treatment can unlock hidden value and business benefits in potential ERP investments.

Risk treatment can be done in various ways and may be simple to achieve. Given the common ERP risk factors, this article has presented three risk treatment techniques that are based on defining IT principles, requiring professional certifications and enhancing the IT governance framework. A risk management practitioner is well positioned to use these risk treatment techniques and can do so with the assistance of numerous widely accepted IT certifications and IT governance and management frameworks. The wheel need not be reinvented, but rather intelligently utilized to unlock hidden value in investments through early risk treatment and appropriately preparing more favorable business cases.

ENDNOTES

[1] Zoughbi, G.; "Creating the Business Case for ERP System Acquisitions Using GEIT," *ISACA Journal*, vol. 1, 2013

[2] Zoughbi, G.; G. Kattnig; S. Parkinson; "Using Governance and Risk Management Practices to Improve Outcomes of Enterprise Resource Planning (ERP) System Acquisitions," BCS International IT Conference, 2013

[3] With the release of COBIT 5 in 2012, key elements of Risk IT have been incorporated in COBIT. *COBIT for Risk* was released in August 2013 and can be found at *www.isaca.org/cobit.*

[4] International Organization for Standardization (ISO), ISO 31000:2009, *Risk management—Principles and guidelines*, 2009

[5] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management—Integrated Framework*, 2004

[6] National Institute of Standards and Technology (NIST), Special Publication 800-30, *Guide for Conducting Risk Assessments*, 2012

[7] ISACA, Risk IT, USA, 2009, *www.isaca.org/riskit*

[8] *Op cit*, Zoughbi, Kattnig and Parkinson, 2013

[9] *Op cit*, Zoughbi, 2013

[10] ISACA, Glossary, 2013, *www.isaca.org/glossary*

[11] The Open Group, The Open Group Architecture Framework (TOGAF), 2011

[12] Smart, B.; "Why Should Organizations Care About Professional Certifications?," *ISACA Journal*, vol. 2, 2013

[13] Herzberg, F.; "One More Time: How Do You Motivate Employees?" *Harvard Business Review*, September-October 1987, p. 5-16

[14] ISACA, CRISC Certification Job Practice, 2013, *www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Prepare-for-the-Exam/Pages/Job-Practice-Areas.aspx*

[15] ISACA, CGEIT Certification Job Practice, 2013, *www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Job-Practice-Areas/Pages/default.aspx*

[16] ISACA, CISA Certification Job Practice, 2013, *www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Prepare-for-the-Exam/Job-Practice-Areas/Pages/2011-CISA-Job-Practice-Areas.aspx*

[17] Project Management Institute (PMI), *A Guide to the Project Management Body of Knowledge (PMBOK Guide), 4th Edition*, 2008

[18] Project Management Institute (PMI), PMI PMP Credential, 2013, *www.pmi.org/Certification/Project-Management-Professional-PMP.aspx*

[19] The Open Group, TOGAF 9 Certification Program, *www.opengroup.org/certifications/togaf9-program*, 2011

[20] Institute of Management Consultants USA, *IMC USA's Competency Framework and Certification Scheme for Certified Management Consultants (CMC)*, 2010, *https://www.imcusa.org/store/view_product.asp?id=1793052*

[21] Institute of Management Consultants USA, "What Is the CMC?," 2013, *www.imcusa.org/?page=CERTWHATCMC*

[22] APMG-International, *Sourcing Governance Foundation Certification*, 2013, *www.apmg-international.com/en/qualifications/sourcing/*

[23] ISACA, *Board Briefing on IT Governance, 3rd Edition*, 2003

[24] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, 2012, *www.isaca.org/cobit*

[25] Burns, T.; G. M. Stalker; *The Management of Innovation*, London, 1961

[26] Lawrence, P. R.; J. W. Lorsch; *Organization and Environment: Managing Differentiation and Integration*, Harvard University, USA, 1967

[27] Chandler Jr., A. D.; *Strategy and Structure: Chapters in the History of the American Industrial Enterprise*, MIT Press, USA, 1962

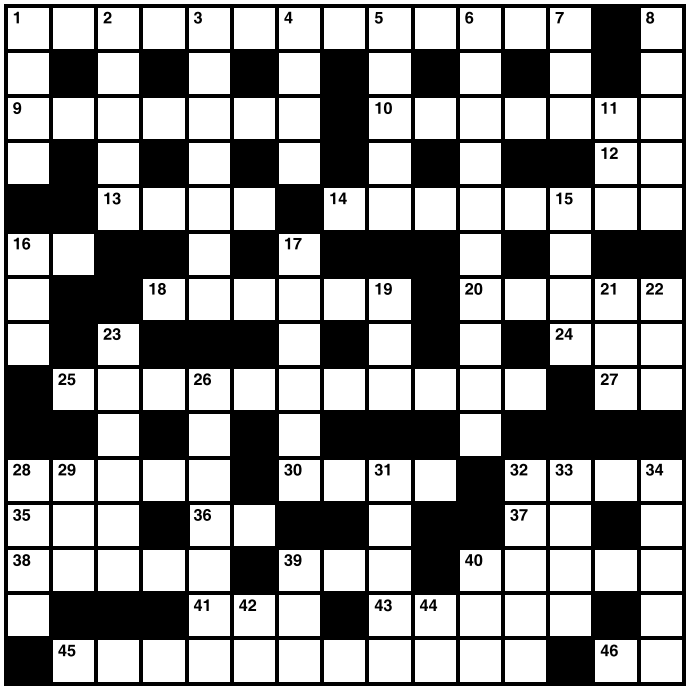
[28] The APM Group Ltd., ITIL, version 3, UK, 2007

[29] Software Engineering Institute (SEI), *Capability Maturity Model Integration*, version 1.3, 2010

[30] APMG-International, The Demand Supply Governance Framework, 2012

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1. Protection against Internet assaults
9. Task or program that is or was executing
10. Offensive actions designed to harm a company or individual
12. Institutional investor, for short
13. Big ____
14. Fundamental facts or principles
16. Decibel (abbr.)
18. Virus used by cybercriminals to encrypt an organization's data and then demand payment for the key (goes with 23 down)
20. ___ *incognita*
24. PC alternative
25. Statistical relation between two or more variables
27. Acidity measurement
28. Copied with intent to deceive
30. Instance of execution of a program
32. Deceive, in slang
35. Copy
36. Distance measurement (abbr.)
37. "The" in French
38. Capable of copying itself to other computers
39. Amount charged
40. These institutions are a favorite target of cybercriminals
41. Computer pioneer Lovelace
43. _____ acids
45. Technology coming into use as part of computer access ID verification
46. That is (abbr.)

DOWN

1. System ___, may be needed when changing an operating system
2. Wide-reaching
3. Add to the database again
4. Estimation words
5. Commonly used medium for cyberattacks
6. A major benefit of cloud computing, enabling better control of repeatable business activities
7. "You know the rest," for short
8. Cornerstone
11. Root___, stealthy type of software
15. Expected standard
16. Often highly costly form of attack on a web site
17. Java application
19. Choose, with "for"
21. Criticize
22. Online financial transaction, abbr.
23. See 18 across
26. Warning signal (2 words)
28. Top pick, informally
29. It specifies how some software components should interact with each other (abbr.)
31. _____ phishing
32. Apply spin to
33. Word form for "billionth"
34. Use inefficiently
39. Outlying
40. Recycling ___
42. Reverse prefix
44. "My" in Spanish

(Answers on page 58)

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

Ganapathi Subramaniam, CISA, CISM, has recently joined Microsoft (India) as chief security officer. Prior to this, he was with Accenture (India), as part of the global information security function. He relocated to India to join Accenture in 2007 from the UK, where he had spent nine years with PricewaterhouseCoopers and Ernst & Young. An avid reader, he is a regular columnist for the *Journal*, writes for other industry publications and is an international conference speaker.

Q How does one audit the cyberresilience of any organization? What kind of baseline security controls would we expect to see to ensure resilience?

A Cybersecurity has become a key area of focus for organizations across the world. A number of governments are in the process of or have recently created and deployed policies governing cybersecurity. Protection of key critical infrastructure remains one of the top priorities of government. Even in the private sector, given the frequent occurrence of attacks around the globe, organizations have stepped up measures to recover operations should an attack ever occur.

Let us consider an example of a typical attack: The attacker sends emails with embedded malicious code. When the recipient opens the email, the embedded malicious code gets downloaded into the recipient's system. Using the malicious code and capturing access credentials, the attacker is able to spread the attack to other systems within the same organization. Thus, the impact is multiplied. The attacker then removes or modifies key data from/within the system where he/she has gained illegal entry.

How do attacks differ? There are different players with different motives. Traditionally, the players used to be simple script kiddies engaging in attacks for the sake of fun. Today, cyberattacks are an industry of their own. It can be possible for a novice to gain access to malicious code and tools with little effort. They are available free or at affordable prices. They are not bound by any geographical limits. Sitting in one part of the world, the attack can be carried out on the other end of the world. Attackers are typically shrewd enough not to leave traces so it is next to impossible to identify them.

Thus, cyberresilience is essential for any organization today. How cyberresilience differs from a traditional disaster recovery plan should also be considered.

Cyberresilience must be built around the following key principles:

- It must protect from all possible attacks.
- Should an attack occur despite protective controls, it must be possible to detect it.
- Should an attack take place, it must be possible to recover the operations and bring the systems and processes back to "run" state.

The auditing of cyberresilience must be based on similar principles. The following is a very high-level indicative checklist for IS auditors when completing an audit on the adequacy and appropriateness of cyberresilience measures:

- All systems must be adequately patched, especially those that face or connect to the Internet. It is essential for the auditor to ensure that the systems and processes surrounding patch management are sufficient enough to mitigate potential risk.
- The most current and updated versions of all software, particularly operating systems, must be running. It is not appropriate to run a system that is no longer vendor-supported. Running systems unsupported by the vendor is a risk.
- It is essential to have a defined data classification system in place. Data classification systems will help to bucket the data under different categories and determine the quantum controls required to protect such systems and applications against attacks. Not all systems and applications require an equal level of controls and protection.
- Monitoring systems must be in place to detect any potential attacks. These systems must be effective enough to raise appropriate alerts and alarms to the individuals responsible for protecting such systems.
- The protection accorded must be at the lowest element level so that any containment in the event of an attack can be localized and restricted. By according element-level protection, it is possible to limit the impact of the attack if it were to occur.
- Any untrusted system must be isolated.

Enjoying this article?

- Learn more about and discuss cybersecurity in the Knowledge Center.

www.isaca.org/topic-cybersecurity

There are numerous resources on this topic that may be helpful as well. Microsoft has published a number of white papers on this subject, e.g., one by James Kavanagh, chief security advisor, Microsoft Australia, titled "Building Cyber Resilience" is apt for your question.[1] Also, the Australian Signals Directorate has published a set of baseline controls that are adopted by many countries.[2]

ENDNOTES

[1] Kavanagh James, "Building Cyber Resilience," Microsoft Australia

[2] Department of Defense, Australian Signals Directorate, Australian Government, *www.asd.gov.au/infosec/top35mitigationstrategies.htm*

Q&A

CPE Quiz

Prepared by Sally Chan,
CGEIT, CMA, ACIS

Take the quiz online:

QUIZ #152

Based on Volume 5, 2013—Integrated Business Solutions

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

TRUE OR FALSE

RAVAL ARTICLE

1. It is impractical to divide the world into good people and bad people and use it to develop tactics to generate appropriate behavior. In practice, group norms of governance invariably focus on helping members of the group to be aware of, and control, their self-interest.
2. Moral commitment should be motivated by strong ethical leadership, include constant communication of the convention and relevant examples related to the convention, and comprise leadership's willingness to provide help.

DE HAES, DEBRECENY AND VAN GREMBERGEN ARTICLE

3. The enhanced role of IT for enterprise value creation and risk management has been accompanied by an increased emphasis on GEIT.
4. To assist organizations with enhancing strategic alignment, the COBIT 5 development team undertook providing guidance to understand why enterprise goals do not drive IT-related goals and *vice versa*.
5. COBIT 5 uses the term "enterprise goals" (as opposed to "business goals" in COBIT 4) to signal explicitly that the framework includes profit-oriented, not-for-profit and governmental enterprises.
6. A focus on covering the enterprise end-to-end comprises a move from managing IT as a cost to managing IT as an asset. This shift is an essential element of business value creation.
7. One example of the balanced scorecard metric for an enterprise goal of optimization of service delivery costs is the percent of business stakeholders satisfied that IT service delivery meets agreed-upon service levels.
8. COBIT 5 identifies a set of governance and management enablers that includes 37 processes.

NICHO AND FAKHRY ARTICLE

9. The top 10 data breaches in 2012, according to the Identity Theft Resource Center (ITRC) database, were analyzed to determine the nature of the attacks and evaluate the role of technical and nontechnical IT mechanisms in these breaches. The nature of most attacks is technical.
10. Information security is often not addressed in a holistic and comprehensive way. When all of its dimensions are taken into account, real risk exists to prevent a really secure environment. In response, 12 dimensions of IS security are proposed.
11. COBIT 5 consolidates and integrates COBIT 4.1, Val IT 2.0, Risk IT and the Business Model for Information Security (BMIS) and aligns with other frameworks and standards such as ITIL, International Organization for Standardization (ISO) standards, Project Management Body of Knowledge (PMBOK), PRINCE2 and The Open Group Architecture Framework (TOGAF).

LUELLIG AND FRAZIER ARTICLE

12. When it comes to information governance practices related to regulatory issues, legal compliance, records retention and disposal policies, COBIT principles are often being leveraged as broadly and as effectively as possible.
13. COBIT 4.1 is based on five key principles for the governance and management of enterprise IT: meeting stakeholder needs; covering the enterprise end-to-end; applying a single, integrated framework; enabling a holistic approach; and separating governance from management.

YU ARTICLE

14. Horizontal scaling involves increasing the internal capacity of a system so it can handle more transactions. This is normally the fastest way to increase capacity without substantially changing the operating environment or the system architecture.
15. The first step in determining the need for in-memory computing is to determine if the application requires a lot of data access and manipulation.
16. IMDBs do not support database triggers and would not have the same level of granularity for field constraints.

VOLCHKOV ARTICLE

17. The strategy of investment in security has to target the mitigation of high-risk areas and the improvement of less adequate or immature processes. An executive management report should, therefore, contain at minimum the following three sections: explanation of a strategy and security program, operational efficiency of a security organization, and cost of security deliveries.
18. Risk assessment and maturity model are two dimensions of the corporate security posture. Any initiative can be viable only if it targets mitigation of risk and/or improvement of one or more immature security processes.

ISACA Journal
CPE Quiz
Based on Volume 5—Integrated Business Solutions

Quiz #152 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC # _____

Quiz #152

True or False

RAVAL ARTICLE

1. _____
2. _____

DE HAES, DEBRECENY AND VAN GREMBERGEN ARTICLE

3. _____
4. _____
5. _____
6. _____
7. _____
8. _____

NICHO AND FAKHRY ARTICLE

9. _____
10. _____
11. _____

LUELLIG AND FRAZIER ARTICLE

12. _____
13. _____

YU ARTICLE

14. _____
15. _____
16. _____

VOLCHKOV ARTICLE

17. _____
18. _____

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 54 for the puzzle.

1 C	Y	2 B	E	3 R	C	4 O	V	5 E	R	6 A	G	7 E	■	8 B
O	■	R	■	E	■	R	■	M	■	U	■	T	■	A
9 P	R	O	C	E	S	S	■	10 A	T	T	A	C	11 K	S
Y	■	A	■	N	■	O	■	I	■	O	■	■	12 I	I
■	■	13 D	A	T	A	■	14 E	L	E	M	E	15 N	T	S
16 D	B	■	■	E	■	17 A	■	■	■	A	■	O	■	■
O	■	■	18 C	R	Y	P	T	19 O	■	20 T	E	R	21 R	22 A
S	■	23 L	■	■	■	P	■	P	■	I	■	24 M	A	C
■	25 C	O	R	26 R	E	L	A	T	I	O	N	■	27 P	H
■	■	C	■	E	■	E	■	■	■	N	■	■	■	■
28 F	29 A	K	E	D	■	30 T	A	31 S	K	■	32 S	33 N	O	34 W
35 A	P	E	■	36 F	T	■	■	P	■	■	37 L	A	■	A
38 V	I	R	A	L	■	39 F	E	E	■	40 B	A	N	K	S
E	■	■	■	41 A	42 D	A	■	43 A	44 M	I	N	O	■	T
■	45 F	I	N	G	E	R	P	R	I	N	T	■	46 I	E

ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

The specialised nature of information systems (IS) audit and assurance and the skills necessary to perform such engagements require standards that apply specifically to IS audit and assurance. The development and dissemination of the IS audit and assurance standards are a cornerstone of the ISACA® professional contribution to the audit community.

IS audit and assurance standards define mandatory requirements for IS auditing. They report and inform:

- IS 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 committee and, ultimately, in disciplinary action.

ITAF™, 2nd Edition (www.isaca.org/itaf) provides a framework for multiple levels of guidance:

- **IS Audit and Assurance Standards**
  - The standards are divided into three categories:
  - General standards (1000 series)—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments, and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
  - Performance standards (1200 series)—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care
  - Reporting standards (1400 series)—Address the types of reports, means of communication and the information communicated
- **IS Audit and Assurance**
  The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorisation as the standards (also divided into three categories):
  - General guidelines (2000 series)
  - Performance guidelines (2200 series)
  - Reporting guidelines (2400 series)
- **IS Audit and Assurance Tools and Techniques**
  - These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programmes, reference books, and the COBIT® 5 family of products. Tools and techniques are listed under *www.isaca.org/itaf*

An online glossary of terms used in ITAF is provided at *www.isaca.org/glossary*.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the control professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or IS environment.

IS Audit and Assurance Standards

The titles of issued standards documents are listed as follows:

General
1001 Audit Charter
1002 Organisational Independence
1003 Professional Independence
1004 Reasonable Expectation
1005 Due Professional Care
1006 Proficiency
1007 Assertions
1008 Criteria

Performance
1201 Engagement Planning
1202 Risk Assessment in Planning
1203 Performance and Supervision
1204 Materiality
1205 Evidence
1206 Using the Work of Other Experts
1207 Irregularity and Illegal Acts

Reporting
1401 Reporting
1402 Follow-up Activities

IS Audit and Assurance Guidelines

Please note that the guidelines are being revised and comments from public exposure are being addressed. The new guidelines are scheduled to be issued in the third quarter of 2014.

General
2001 Audit Charter (G5)
2002 Organisational Independence (G12)
2003 Professional Independence (G17 and G34)
2004 Reasonable Expectation
2005 Due Professional Care (G7)
2006 Proficiency (G30)
2007 Assertions
2008 Criteria

Performance
2201 Engagement Planning (G15)
2202 Risk Assessment in Planning (G13)
2203 Performance and Supervision (G8)
2204 Materiality (G6)
2205 Evidence (G2)
2206 Using the Work of other Experts (G1)
2207 Irregularity and Illegal Acts (G9)
2208 Sampling (G10)

Reporting
2401 Reporting (G20)
2402 Follow-up Activities (G35)

The ISACA Professional Standards and Career Management Committee (PSCMC) is dedicated to ensuring wide consultation in the preparation of ITAF standards and guidelines. Prior to issuing any document, an exposure draft is issued internationally for general public comment.

Comments may also be submitted to the attention of the Director of Professional Standards Development via email (*standards@isaca.org*); fax (+1.847. 253.1443) or postal mail (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

Links to current and exposed ISACA Standards, Guidelines, and Tools and Techniques are posted at *www.isaca.org/standards.*

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

Advanced Persistent Threats: How to Manage the Risk to Your Business
132 pages—**APT**

Member $35.00 | NonMember $60.00

eBook—**WAPT**

Member FREE | NonMember $60.00

Big Data—A Revolution That Will Transform How We Live, Work, and Think
270 pages—**1HMBD**

Member $16.00 | NonMember $26.00

COBIT® 5 for Risk
213 pages—**CB5RK**

Member $35.00 | NonMember $175.00

eBook—**WCB5RK**

Member $35.00 | NonMember $175.00

IT Governance for CEOs & Members of the Board
108 pages—**1CSITG**

Member $13.00 | NonMember $23.00

COBIT 5 Enabling Information
270 pages—**CB5EI**

Member $35.00 | NonMember $135.00

eBook—**WCB5EI**

Member FREE | NonMember $135.00

Featured...
www.isaca.org/featuredbooks

Cyber Forensics from Data to Digital Evidence
342 Pages—100**WCF**

Member $80.00 | Nonmember $90.00

Configuration Management: Using COBIT 5
60 Pages—**CB5CM**

Member $30.00 | Nonmember $55.00

eBook—**WCB5CM**

Member FREE | Nonmember $55.00

Transforming Cybersecurity: Using COBIT®5
190 Pages—**CB5TC**

Member $35.00 | Nonmember $60.00

eBook—**WCB5TC**

Member FREE | Nonmember $60.00

Reverse Deception: Organized Cyber Threat Counter-Exploitation
464 pages— **31-MRDO**

Member $40.00 | Nonmember $50.00

Responding to Targeted Cyberattacks
90 pages—**RTC**

Member $35.00 | Nonmember $59.00

eBook Format—WRTC

Member Free | Nonmember $59.00

* 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

We are constantly expanding. Check out our new books and eBooks!
https://www.isaca.org/bookstore/Pages/New-Arrivals.aspx

SUPPLEMENT

NEW/FEATURED BOOKS www.isaca.org/newbooks

Advanced Persistent Threats: How to Manage the Risk to Your Business

by ISACA

This book explains the nature of the security phenomenon known as the advanced persistent threat (APT). It also provides helpful advice on how to assess the risk of an APT to the organization and recommends practical measures that can be taken to prevent, detect and respond to such an attack. In addition, it highlights key differences between the controls needed to counter the risk of an APT attack and those commonly used to mitigate everyday information security risk. 132 pages, 2013

NEW

Print Format—**APT** Member $35.00 Nonmember $60.00

eBook—**WAPT** Member FREE Nonmember $60.00

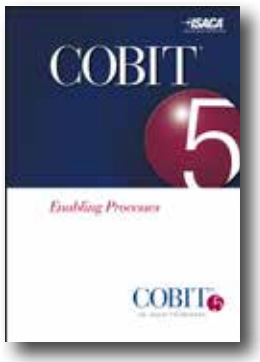
Big Data—A Revolution That Will Transform How We Live, Work, and Think

by Viktor Mayer-Schonberger, Kenneth Cukier

A revelatory exploration of the hottest trend in technology and the dramatic impact it will have on the economy, science, and society at large. "Big data" refers to our burgeoning ability to crunch vast collections of information, analyze it instantly, and draw sometimes profoundly surprising conclusions from it. This emerging science can translate myriad phenomena—from the price of airline tickets to the text of millions of books—into searchable form, and uses our increasing computing power to unearth epiphanies that we never could have seen before. A revolution on par with the Internet or perhaps even the printing press, big data will change the way we think about business, health, politics, education, and innovation in the years to come. It also poses fresh threats, from the inevitable end of privacy as we know it to the prospect of being penalized for things we haven't even done yet, based on big data's ability to predict our future behavior. 270 pages, 2013

NEW

Print Format—**1HMBD** Member $16.00 Nonmember $26.00



COBIT 5 Enabling Information

by ISACA

Enterprises are experiencing increasing difficulty in maintaining control of their data to comply with legal and regulatory requirements. *COBIT 5: Enabling Information* is a reference guide that provides a structured way of thinking about information governance and management issues in any type of organization. This structure can be applied throughout the life cycle of information, from conception and design, through building information systems, securing information, using and providing assurance over information, and to the disposal of information. 270 pages, 2013

NEW

Print Format—**CB5EI** Member $35.00 Nonmember $135.00

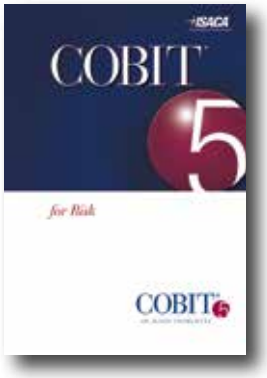
eBook—**WCB5EI** Member FREE Nonmember $135.00

COBIT 5 for Risk

by ISACA

Effectively managing IT risk helps drive better business performance by linking information and technology risk to the achievement of strategic enterprise objectives. Risk is generally defined as the combination of the probability of an event and its consequence. *COBIT 5 for Risk* defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise. 213 pages, 2013

NEW



Print Format—**CB5RK** Member $35.00 Nonmember $175.00

eBook—**WCB5RK** Member $35.00 Nonmember $175.00

Configuration Management: Using COBIT 5

by ISACA

Enterprises continuously experience changes; driven by both external and internal forces. When changes occur in one part of the enterprise without proper communication and coordination, signs of malfunction are likely to manifest as business disruptions, inefficiencies and potential financial losses. Configuration management (CM) reduces the risk of these malfunctions as part of a strategy to manage internal enterprise changes and minimize unforeseen impacts. 190 pages, 2013

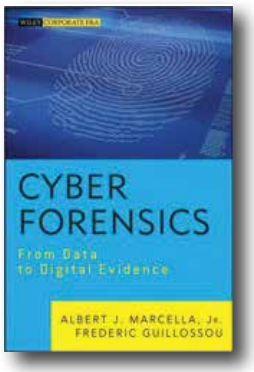
Print Format—**CB5CM** Member $30.00 Nonmember $55.00

eBook—**WCB5CM** Member FREE Nonmember $55.00

Cyber Forensics from Data to Digital Evidence

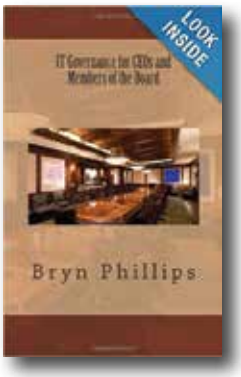
by Albert J. Marcella, Jr., Frederic Guillossou

This book explains the basic principles of data as building blocks of electronic evidential matter, which are used in cyber forensics investigations. The entire text is written with no reference to a particular operation system or environment, thus it is applicable to all work environments, cyber investigation scenarios, and technologies. The text is written in a step-by-step manner, beginning with the elementary building blocks of data progressing upwards to the representation and storage of information. It includes practical examples and illustrations throughout to guide the reader. 342 pages, 2013



Print Format—100**WCF** Member $80.00 Nonmember $90.00

NEW/FEATURED BOOKS www.isaca.org/newbooks



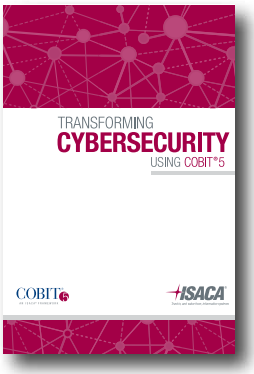
IT Governance for CEOs & Members of the Board

NEW

by Bryn Phillips

This book gives a concise overview of Information Technology Governance and is geared towards those who need to understand it the most, but usually have the least time to do so; CEO's and members of the Board! It provides a summary of the reasons IT Governance is required, a brief description of the elements of IT Governance, and, most importantly, gives guidance with regards to the responsibilities of the Board. This book also gives guidance as to what is required of the Board and CEO, and what should be delegated to the CIO and others. 108 pages, 2013

Print Format—**1CSITG** Member $13.00 Nonmember $23.00



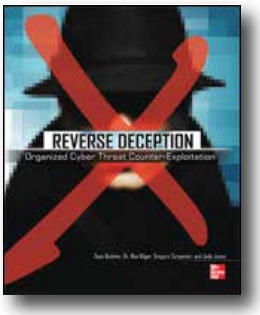
Transforming Cybersecurity: Using COBIT 5

by ISACA

The cost and frequency of cybersecurity incidents are on the rise, is your enterprise keeping pace? The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cybersecurity has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with cybersecurity will be essential to organizational survival and profitability. 190 pages, 2013

Print Format—**CB5TC** Member $35.00 Nonmember $60.00

eBook—**WCB5TC** Member FREE Nonmember $60.00

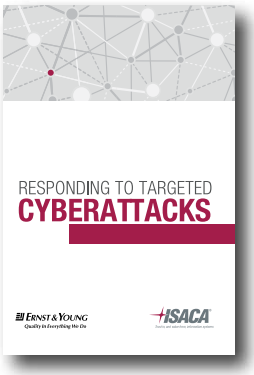


Reverse Deception: Organized Cyber Threat Counter Exploitation

by Sean Bodmer, Dr. Mak Kilger, Gregory Carpenter, Jade Jones, Jeff Jones

Expose, pursue, and prosecute the perpetrators of advanced persistent threats (APTs) using the tested security techniques and real-world case studies featured in this one-of-a-kind guide. Reverse Deception: Organized Cyber Threat Counter-Exploitation shows how to assess your network's vulnerabilities, zero in on targets, and effectively block intruders. Discover how to set up digital traps, misdirect and divert attackers, configure honeypots, mitigate encrypted crimeware, and identify malicious software groups. The expert authors provide full coverage of legal and ethical issues, operational vetting, and security team management. 464 pages, 2013

Print Format—**31-MRDO** Member $40.00 Nonmember $50.00



Responding to Targeted Cyberattacks

By ISACA

The threat environment had radically changed over the last decade. Most enterprises have not kept pace and lack the necessary fundamentals required to prepare and plan against cyberattacks. To successfully expel attackers, the enterprise must be able to:

- Conduct an investigation
- Feed threat intelligence into a detailed remediation/eradication plan
- Execute the remediation/eradication plan

This publication covers a few of the basic concepts that will help answer the key questions posed by a new outlook that a breach WILL eventually occur. *Responding to Targeted Cyberattacks* is available for purchase in ebook and as print format. ISACA members have complimentary download access to the ebook. Nonmembers of ISACA may choose to purchase the ebook. 90 pages, 2013

Print Format—**RTC.** Member $35.00 Nonmember $59.00

Ebook—**WRTC.** Member FREE Nonmember $59.00

YOU HAVE THE **PASSION**. NOW **SHARE IT**.

BE PART OF THE INNOVATIVE THINKING THAT HELPS SHAPE THE IT PROFESSION. DISCOVER ISACA® VOLUNTEER OPPORTUNITIES.

INFLUENCE MORE

ISACA VOLUNTEER BODIES

Contribute to the imaginative thinking and leading-edge resources of the IT industry by sharing your knowledge and skills. ISACA volunteer and their respective volunteer bodies help shape valuable content worldwide.

ISACA volunteers help advance the dynamic IT profession by influencing:

> Certification programs
> Professional conferences
> Education programs
> Insightful research
> Professional standards

READY TO MAKE YOUR MARK?

Learn about ISACA International volunteer body opportunities and criteria ***www.isaca.org/participate***.

2014-2015 INTERNATIONAL VOLUNTEER BODY OPPORTUNITIES

1 November 2013 - Application period opens

13 February 2014 - Application period closes

Learn more at ***www.isaca.org/volunteer***

ISACA®
Trust in, and value from, information systems

Europe's biggest information security event!

29 April to 01 May 2014 | Earl's Court, London UK

What is in it for you?

- Meet with 325+ industry-leading vendors and suppliers.
- Earn CPD and CPE credits from attending the free education programme sessions!
- Exclusive access to industry experts, keynote speakers and thought leaders.
- Network with peers, share knowledge, collaborate and build relationships.

infosecurity EUROPE

Register free now at: www.infosec.co.uk

Secure your stand now and meet 13,000 potential customers!

For Europe, Africa, Asia, Australia and Oceania sales:

Malcolm Wells
Tel: +44 (0)20 8910 7718 | malcolm.wells@reedexpo.co.uk

Ben Race
Tel: +44 (0)20 8910 7991 | ben.race@reedexpo.co.uk

David Price
Tel: +44 (0)20 8910 7047 | david.price@reedexpo.co.uk

Greg Fleming
Tel: +44 (0) 208 910 7081 | greg.fleming@reedexpo.co.uk

For US and Canadian sales:

Raymond Filbert
Tel: +1203 840 5821 | rfilbert@reedexpo.com

follow Infosecurity Europe on Twitter: @infosecurity