Volume 6, 2014

ISACA® Journal

Cybersecurity

Featured articles:

How Zero-trust Network Security Can Enable Recovery From Cyberattacks

Leveraging Industry Standards to Address Industrial Cybersecurity Risk

Bridging the Gap Between Access and Security in Big Data

And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG

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 volunteers and their respective volunteer bodies help shape valuable content worldwide.

ISACA volunteers help advance the dynamic IT profession by influencing:

> Certification programs

> Insightful research

> Professional standards, white papers guidance and publications

> COBIT and CSX deliverables

> Education Programs and Conferences

READY TO MAKE YOUR MARK?

Learn about ISACA International volunteer body opportunities and criteria.

Now accepting applications for 2015-2016 International Volunteer Body Opportunities.

Apply now at

www.isaca.org/participate15

2015-2016 INTERNATIONAL VOLUNTEER BODY OPPORTUNITIES

November 2014 - Application period opens

ISACA®

Trust in, and value from, information systems

VoIPshield Systems, Inc.

COBIT 5® includes VoIP
We've Got You Covered

VoIPaudit is an essential tool for all **COBIT®** and **PCI** professionals.
No other product comes close.

Former EVP Fraud & Risk Management, Visa

"Without proper security, and controls around VoIP, organizations risk breaches that can incur financial losses, lose competitive advantage, not to mention brand impact."

Bashir Fancy

Don't wait for the auditor to highlight your issues, identify and fix them now:

- **VoIPaudit** only takes **5 minutes to set up.** The rest is automated.
- Our report identifies your trouble spots by standard or framework, and explains the steps needed to become compliant. Our coverage includes all current industry assurance standards and frameworks:
  - **COBIT 4.1®** and **COBIT 5®**
  - **PCI DSS 2.0** and **PCI DSS 3.0**
  - **ISO / IEC 27001:2013** and **ISO / IEC 27002:2013**

NEW
TEST YOUR SYSTEM
FOR FREE

download **VoIPaudit lite** at **www.voipshield.com.** Or contact us at **+1 613-591-6589**

VOLUME 6, 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 in December.

Seven Mistakes Being Made in SIEM and How to Fix Them
Flint Brenton

Book Review: 100 Things You Should Know About Authorizations in SAP
Reviewed by Horst Karin, Ph.D., CISA, CRISC, CISSP, ITIL

Book Review: Cyberethics: Morality and Law in Cyberspace, 5th Edition
Reviewed by Maria Patricia Prandini, CISA, CRISC

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

The **projected growth rate** for the information security analyst profession between 2012 and 2020

SOURCE: BUREAU OF LABOR STATISTICS, 2014

Do you have what it takes to answer the call?

Elevate your information security career with one of Capella's new MS in Information Assurance and Security options: **Digital Forensics** | **Network Defense**

Your future is waiting. Start now. CAPELLA.EDU/ISACA OR 1.866.670.8737

See graduation rates, median student debt, and other information at www.capellaresults.com/outcomes.asp.

ACCREDITATION: Capella University is accredited by the Higher Learning Commission.
CAPELLA UNIVERSITY: Capella Tower, 225 South Sixth Street, Ninth Floor, Minneapolis, MN 55402, 1.888.CAPELLA (227.3552), www.capella.edu. ©Copyright 2014. Capella University. 14-7778

Capella University

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

Whiz Bang 2000

Facts: Cyberattacks are a known threat to the information systems of organizations around the world. There are many products on the market that purport to detect and/or prevent cyberattacks. Cyberattacks are happening anyway.

Why is this so?

- Maybe the companies that make cybersecurity products do not have good salespeople? *No, that is not the reason.*
- Maybe chief information security officers (CISOs) are not interested in products that detect and/or prevent cyberattacks? *No, that is not the reason either.*
- Maybe the products are not very good? *That is a possibility, but there is no comprehensive evidence to that effect.*
- Maybe cyberattacks are not a problem that lends itself to packaged solutions? *Hmmm…*

CYBERSECURITY PRODUCT FEATURES

There are many cybersecurity software products on the market. They come from large companies better known for computer hardware, small firms that have gained a reputation for after-the-fact repair of cyberattack-related damage and start-ups about which little is known beyond their web sites. Some of these products promise to stop advanced persistent threats (APTs) used by cybercriminals. Others merely say they will detect zero-day attacks, malicious communications, and anomalous attacker indicators.[1] Rather than pick on any one vendor, or even several at a time, I have invented a totally fictitious product that I call Whiz Bang 2000 (WB2K) (trademark, copyright, patent pending, marca registrada, etc., etc.). WB2K is intended to be a compendium of the features claimed by many, if not all, of the products I have seen in the marketplace. It will:

- Maintain awareness of all changes to an organization's infrastructure configuration
- Enforce access control and change management policies to monitor, detect, contain and prevent malicious activities across end points, including servers, laptops and desktops
- Aggregate risk factors to automatically elevate alerts and containment controls including the trigger of forensic actions
- Monitor and block known bad applications and unknown applications, preventing the rapid spread of cyberattacks
- Detect, prevent and contain malicious software effectively on and off the network
- Use a signature-less approach to detect new or unknown malware with automated behavioral analysis of code in physical memory
- Manage scans based on schedule or policy violation and facilitate the retrieval of memory forensics to support incident response
- Determine the characteristics of an attack and which resources—software and data—have been affected
- Monitor all software coming through the Internet gateway for viruses and other malware

So, aside from the fact that the product does not exist, why is my phone not ringing off the hook with orders for WB2K?

OTHER TOOLS

Many of the features of WB2K are available in products that already are in use in many data centers. For example, configuration management databases (CMDBs), and their related software, generally have knowledge of configuration changes. These are often fairly expensive tools. While they are often found in large enterprises, they may be beyond the budgets of small to medium-sized businesses.

> "No organization that is serious about cybersecurity should operate without an IDPS."

For those that do have a CMDB and the aligned ITIL-supported change and configuration management processes that go with it, a cybersecurity product may, in many cases, be redundant.

Intrusion detection and prevention systems (IDPSs) are aware of malicious activities on

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:

networks and information systems (IS) infrastructures. They can trigger alerts and prevent the spread of malicious software across an organization's systems. In my opinion, no organization that is serious about cybersecurity should operate without an IDPS, and, in my experience, few do. But they do not always apply them everywhere and on every endpoint, so there may be gaps in many organizations' defenses. There is no reason to believe, however, that the detective properties of a cybersecurity product, such as the mighty Whiz Bang 2000, would be any more effective than long-used IDPS tools.

Enjoying this article?

- Read *Cybersecurity: What the Board of Directors Needs to Ask*.

  www.isaca.org/iia-isaca-report

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

  www.isaca.org/topic-cybersecurity

MARKET DOMINANCE

Across the IT field, there are certain products that have achieved such dominance that they are the *de facto* standards, attracting the vast bulk of customers and antitrust lawsuits. No product has attained that status in the area of cybersecurity. Considering how long information security products have been in the marketplace, it is a bit surprising that no company has captured the imagination, if not the money, of those who buy such products for large organizations.

It may well be that buyers are waiting for the market to shake out the lesser products and let a clear winner (or at least a few) emerge. If this is just a matter of an immature marketplace, it is time for it to grow up quickly; the threats are getting worse, not slackening. But there is a circularity to this argument: Buyers are not buying because vendors are not selling. In the bazaar that is software sales, we should expect the imprimatur of purchases of certain leading organizations to spur further deals with similar companies. I do not see that happening, at least not yet.

PURCHASE INHIBITORS

I think there is a psychological inhibitor working against the large-scale acquisition of cybersecurity products. *The New York Times* pointed out recently that CISOs have thankless jobs. Their positions are only as secure as the next successful cyberattack. Andrew Casperson, a former CISO, is quoted as saying "In the old days, there was a saying, 'Nobody ever got fired for buying IBM,' because you could trust IBM. But security firms have never been able to establish that level of credibility."[2]

To go to management with a request for budget for a cybersecurity product is an implicit endorsement not only of a specific vendor's product, but of the concept that *any* product is capable of solving the problem of cyberattacks, without any clarity as to what a solution might be. The community of information security professionals has labored for decades to protect information systems from abusers, misusers, fraudsters and thieves. And, the professionals have not always succeeded. In most cases, their strategy has been to make the difficulty and cost of undermining security so high that attempts, much less *successful* attacks, were rendered unlikely. The world is now contending with highly skilled, well-financed attackers with sufficient resources and incentives to undermine or overwhelm the barriers that have been erected in the past.

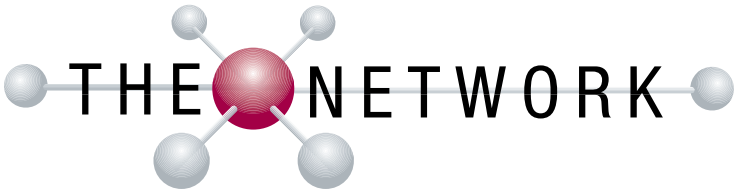
For many CISOs, buying and implementing a cybersecurity product is taking a gamble with their careers. Unless and until there is a demonstrably superior product, I suspect that products in this area of IT will be slow to take command in data centers around the world. And, until the information systems that live in those data centers are demonstrably securable, it may make no sense to buy protective products that do not, cannot, protect.

But if anyone is interested, I would be glad to offer the next release of Whiz Bang 2000.

ENDNOTES

[1] Software advertising tends to be of the "leaps over tall buildings" school of panegyrics. Throughout this article, I use paraphrases of vendor text, but do not identify them.

[2] Perlroth, Nicole; "A Tough Corporate Job Asks One Question: Can You Hack It?," *The New York Times*, 20 July 2014



Kathleen M. Stetz, CISA, CISM, CRISC, PMP

Kathleen M. Stetz, is a technical risk and compliance analyst for a Fortune 500 company in the Chicago, Illinois, USA, area. Stetz has spent more than 20 years in the IT security, risk management, compliance and project management sectors. Before taking on her current role, she worked as an outside consultant providing IT direction to audit projects. Prior to this, she was the operational IT risk officer for a major mortgage lending bank in Chicago, where she was responsible for developing policies and providing risk management strategies. Stetz is also an instructor for the local ISACA chapter, teaching and preparing candidates who are working to achieve their professional certifications.

Q: *What do you see as the biggest risk factors being addressed by IT security professionals?*

A: The biggest risk factor has and will always be protecting the organization's systems and data from harm and adverse conditions by focusing on the security attributes for information integrity, confidentiality or privacy, and availability. This is more difficult to achieve today because systems have integrated mobile technologies and applications causing the operating environment to constantly change and, in turn, increasing the level of complexity. Seeing how these new technologies will impact day-to-day operations throughout the organization is not always apparent.

Security professionals need to take an integrated approach by looking at processes end to end, involving knowledgeable stakeholders from the IT and business sides, and having an eye on the key risk influencers for understanding the emerging threats to the people, processes, technology and possible external events—the operational risk factors.

Q: *How can businesses protect themselves?*

A: Businesses must take a holistic approach to risk management to see how the fast-changing environment will impact their goal attainment. IT controls no longer belong just to the IT areas, but there is cross-over to the business side, thus involving the right stakeholders from both sides is paramount. It is also important to understand how all of the pieces fit together and identify potential points of failure proactively.

Q: *What do you see as the biggest compliance challenges on the horizon?*

A: I believe that the biggest emerging compliance challenge is addressing change for new technologies or integration projects while protecting existing information. It is often difficult to separate the data with an understanding of the data classification among diverse test environments and conditions while protecting this information from unauthorized resources. The control environment now spans multiple areas with an increased complexity and perhaps several control owners handling different parts of the processes that at one time existed within one area.

Q: *How do you believe the certifications you have attained have advanced or enhanced your career?*

A: My certifications have offered me opportunities that have helped me to advance my career. I have several certifications and those offered by ISACA® are especially important because each discipline follows a risk-based methodology that can be universally applied to any industry or market. This approach has helped me develop a strategic view of effective risk management to break down the traditional boundaries and barriers between IT and the business to work more collaboratively.

When making recommendations for staffing, I always ask to see if a candidate has any certifications. Those individuals who have achieved professional certifications seem to be more serious with a demonstrated commitment to the profession. They have worked hard to achieve their success and have a level of confidence that sets them apart.

Q: *You have moved up the ranks in IT audit and transitioned into risk and compliance. For someone new in their professional career or someone looking to make a similar transition, please describe how you have made these changes and adjusted to new roles.*

A: Moving into the risk and compliance area is a separate function from the traditional IT auditing process. To make this transition, you need to have the desire to transform the auditing role by partnering and consulting with the various IT areas to help them understand key areas of risk. This entails looking beyond the controls to understand the processes of what is being delivered. As an auditor, you are looking to find the exceptions around the control failures to issue a report; whereas, by taking on the role of a compliance analyst or consultant, you are working as partner and change agent helping these areas make process improvements to enhance control effectiveness.

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:

WHAT IS YOUR FAVORITE BLOG?
I really do not read blogs. However, I access the ISACA site very regularly—*www.isaca.org*.

WHAT IS ON YOUR DESK RIGHT NOW?
My computer, white papers, books, and risk and control models

AS 2014 COMES TO AN END, WHAT ARE YOUR FINAL GOALS FOR THE YEAR?
1. Ensure that all 2014 issues are brought to a successful resolution and are closed—all major risk factors mitigated.
2. Roll out my control issue trend analysis of potential threats/risk.
3. Mentor and get feedback from the students of the CISA exam preparation course that I teach through ISACA's Chicago Chapter.

WHAT IS YOUR NUMBER ONE PIECE OF ADVICE FOR OTHER RISK AND COMPLIANCE PROFESSIONALS?
Respect individuals and before taking any action, follow the quality adage: Think, plan and do.

WHAT ARE YOUR FAVORITE BENEFITS OF YOUR ISACA MEMBERSHIP?
1. Networking opportunities
2. eLibrary, *www.isaca.org/elibrary*
3. ISACA Knowledge Center, *www.isaca.org.knowledgecenter*

WHAT DO YOU DO WHEN YOU ARE NOT AT WORK?
I volunteer to teach the ISACA CISA review course offered by the Chicago Chapter; I enjoy helping those who are striving to obtain this certification. When I'm not teaching, I love to listen to music and play the piano.

An Alchemy of C3: Character, College and Computers

Vasant Raval, DBA, CISA, ACMA, is a professor of accountancy at Creighton University (Omaha, Nebraska, USA). The coauthor of two books on information systems and security, his areas of teaching and research interest include information security and corporate governance. Opinions expressed in this column are his own and not those of Creighton University. He can be reached at *vraval@creighton.edu.*

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:

Over the past two decades, the demand for information systems (IS) knowledge workers has outpaced the supply. During the 1990s, under pressure to meet Y2K date needs, organizations needed programmers. The currency of most application software then was COBOL, so there was a rush to produce competent COBOL programmers. The situation today is no different, only the coding needs have shifted to other areas, such as SQL, Java, Perl or Ruby. If anything, the gap between the demand and supply of code writers has increased vastly worldwide. The US Bureau of Labor Statistics projection indicates that by the year 2020, 1,000,000 programming jobs in the US will go unfilled.[1]

This, of course, is an opportunity for some. To meet the shortage in supply of competent software developers, many universities offer certificate programs, focused exclusively on a specific skill set and little else, all delivered in a rather short span of time, generally no more than one year. Such moves to feed the careerist mind are not limited to established colleges and universities. A whole new cadre of fast-track coding schools has cropped up. Career starters as well as midlife career switchers are welcome at most of these schools. If accepted into the program, all they need to do is go through a rather rigorous training.

Now and in the future, the need to understand how to use computers has gained permanence. Quality of life depends heavily on the ability to use information efficiently and effectively. The ubiquity of technology application has created an advocacy for introducing computer learning from early childhood, as in the case of other universal subjects, such as basic sciences.[2] With properly designed curriculum and its delivery, high schools and colleges can help students become more sensitive about ethical dilemmas in the use of technology and how to resolve them.

As noted previously, the other push to introduce more and more specific computer instruction comes from the near-term demand-supply gap in various IT jobs. Noticing the gap, employers pitch to lawmakers that the pipeline for skilled coders, for example, is nearly dry; the lawmakers in turn introduce various legal measures that may help solve the problem. Some demand for skilled coders may be met by offshoring the requirements; however, this is a politically sensitive option. Meanwhile, realizing the potential for economic gains, coding schools are born at home.

But where does all this lead in our dialog on information ethics? My intention is to establish links among three interacting forces of transmutation in this space—character, college education and computers—and suggest certain caveats in terms of information ethics. We first look at the most important element, character, then discuss college—and other institutions of learning—where character should be refined, and finally address computers, where the impact of character and college would be evident.[3]

CHARACTER

To quote former British Prime Minister Gordon Brown, "The problem of unbridled free markets…is that they can reduce all relationships to transactions, all motivations to self-interest, all sense of value to consumer choice and all sense of worth to a price tag."[4]

In a rapid response to today's pressing needs, we may get blindsided. We miss the understanding that in the long run, what makes a vibrant workforce is not the particular skill, but rather the character of the person. The foundation of optimal life-long development, character strengths are linked to important aspects of individual and social well-being.[5] Wisdom and knowledge, courage, humanity, justice, temperance, and transcendence represent just one classification of character strengths.[6]

Our moral development, which expresses itself in every volitional choice we make, has to do with our integrity—our *will* to do right and resist wrong. This can be at any level—physical,

mental, moral or spiritual—and in any role, as a family member, employee at work, or leader in business and society. Our disposition defines the bent, or proneness, to make certain choices and walk away from others. Without character strength, despite all the skills and competencies to deliver desired economic outcomes, one may lack the motivation to do the right thing. Character matters; it colors everything for which we live. As a society and individually, it is our duty to avail ourselves of every opportunity to hone our character, often seen as a silent, but relatively stable and dominant, partner in our behavior.

COLLEGE

Character gets molded throughout one's life. However, there are two windows where our character is most influenced. First is one's family. The environment in which the family lives, unwritten rules, rituals and protocols, and the system of punishment and rewards unique to the family forge the child's character, mostly through vicarious learning. The family leaves a lasting impact on one's quality of life.

Outside of the family and friends, the other most significant source that hones our character is schools and colleges attended for education. Maturity, judgment, purpose in life and courage, for example, are sharpened in the educational environment through interaction with other students and the faculty or mentors. The practice of character development is consciously embedded in traditional liberal arts colleges. For example, Creighton University, where I teach, believes in development of the whole person, and, in the spirit of living this mission, the campus life and learning fully integrate personal development of the students, not just delivery of skills needed to make a living.

However, many colleges and universities have drifted toward programs for skills development with a view to attract enrollment, often an important source of cash flow for the institution. Business, engineering, law and computer science are among many academic areas where well-paid jobs are more easily found. When more attention is paid to skills development, there is less room to reflect on life's purpose, justice and service. In other words, the development of the whole person is sacrificed to a degree.

While some colleges and universities are aligning toward feeding the careerist mind, code schools are even more disappointingly positioned. Even if they desire to integrate ethics into their curriculum, there is often little room to do so. Most of these institutions do not have a code of ethics or mission and core value statements. Although detailed curricula are not accessible for these programs, on the surface, it seems they do not have any part of their curriculum devoted to information ethics, for example. After all, to them, what matters is the development of competencies to code—a laser focus on this very specific need.

Now, at the receiving end, people seek careerist development of all kinds. Automakers such as BMW run their own schools to train workers for their factories, and Facebook has its own program to orient new recruits into its specific work life. These are perfectly legitimate options to fill the void between what you know and what it will take to do the job and do it right. On the ethics front, the concern is this: If the schools and colleges that one has attended did not wire the person for ethical awareness and judgment, the job-specific training programs most likely will not offset the need for character development. Besides, ethical awareness is in part affected by the specific context within which ethical dilemmas take shape. A person who learned about, say, Kantian precepts of ethical conduct at a college may not be able to see the ethical dilemma in a programming role, for example. Thus, it is important for the vocational training to weave in context-dependent awareness-building exercises in ethics. If these sensitivities are not developed here, the next best hope is in the employer's orientation of vocationally qualified recruits. The real risk lies in the possibility that across this value chain, none of the organizations involved has addressed this developmental need.

COMPUTERS

Computers, of course, are enablers of almost everything. This includes possibilities of doing good or bad, sometimes even without being aware that you are participating in the deed. As the CBS *60 Minutes* episode, "Is the U.S. Stock Market Rigged?,"[7] reveals, programming skills were used to create speed advantage (high frequency trades [HFTs]) that extracts millions of dollars of potential gain from the security trades queued to arrive at the exchange. HFT firms used sophisticated computer programs to capitalize on price imbalances (make the market) and, thus, profit at the expense of other market participants who had already queued their transaction on slower networks. If I were a member of

the project team that delivered HFT programs, would I be aware of this motive? Or would I just put my head down and code the requirements so that millions of investors can be marginally cheated out of their gains?

Coders are not just coders anymore. Their role is richer than the traditional task of designing and maintaining financial transaction processing programs.[8] Whether they are aware or not, they wield great influence. Every bit of automation can be powerful in terms of speed and scale, and the impact of the code could be vast. Therefore, training in coding—and just downright coding only—may not be a good thing. Yes, it makes people viable in finding careers and paychecks, but the potential lack of ethical awareness in the long run could impose significant costs on society as a whole. The coding schools, employers recruiting at such schools and firms that run their own vocation-specific schools with similar objectives should recognize this anomaly and introduce their own requirements to bridge the ethical awareness gap.

AN ALCHEMY OF C[3]

Computers have truly become the lifeline of today's economies and societies. To prevent ethical lapses with vast impact across the globe, it behooves us to demand accountability from those who wield influence through their skills, including coders. IT knowledge workers should ideally have some college education as a context for personal development and maturity. In its absence, blind following of the rules without exercising professional skepticism could occur. Given the size of potential impact, even one instance of moral compromise is one too many.

Coding schools should consider seriously some minimal requirements on information ethics. It is clear that their curriculum would be "dense" in technical content and challenging deliverables; yet, it is equally clear that some orientation to ethical awareness is not only warranted, but also a responsible thing for the coding schools to do. At the receiving end, talented coders without any prior opportunity for self-development outside of the family environment will benefit from their employer's program designed to increase awareness of the context within which ethical issues arise on the job. And this goes for not just the career starters, but also for the midlife career switchers. For them, even if they have some college degree, chances are, the context of this new job domain is quite different. Consequently, their awareness may be blunted. They too need help in understanding the context of their work and nuances of consequences they build into applications they write.

The IT profession shoulders heavy responsibility to do the right thing—and even more so in the future as the world gets surrounded by computers. It is critical that we do not reduce all relationships to transactions, all motivations to self-interest, all sense of value to consumer choice and all sense of worth to a price tag.

ENDNOTES

[1] Mims, Christopher; "Programming Is a Trade; Let's Act Like It," *The Wall Street Journal*, 4 August 2014, p. B1, B6

[2] "Coding in Schools: A is for Algorithm," *The Economist*, 26 April 2014, *www.economist.com/node/21601250/print*

[3] I caution that this discussion may appear disjointed, however, in the end a unified picture emerges.

[4] Burns, John F.; Landon Thomas Jr.; "Anglo-American Capitalism on Trial," *The New York Times*, 28 March 2009, *www.nytimes.com/2009/03/29/weekinreview/29burns.html?pagewanted=all&_r=0*

[5] Park, N.; C. Peterson; "Character Strengths: Research and Practice," *Journal of College and Character*, 10(4), April 2009, p. 1-10

[6] *Op cit*, p. 2-3

[7] CBS, "Is the U.S. Stock Market Rigged?," *60 Minutes, www.cbsnews.com/videos/is-the-u-s-stock-market-rigged-2/*

[8] Even in this rather straightforward traditional task, it is likely that ethical dilemmas are involved. For example, management asks a programmer to modify the payroll program to include a specific amount as mileage reimbursement and the rest as gross pay where employees are not required to keep any records of their business travel, and the mileage varies across pay periods. What should the programmer do?

The Core of IT Auditing

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 who 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. After nine years writing the *Journal*'s IS Audit Basics column, Singleton will make this volume 6, 2014, column his last.

With the advent of the latest wave of information technologies such as big data, social media, technologies as a service and the cloud in general, it is worth taking the time to revisit the basics of IT audit. Usually, when such new technologies arise, the issues are the same as something in the past, and the way to address the emerging technology is to do what IT auditors always do when faced with challenges of new technologies. We go back to the core of IT auditing and what IT auditing is all about. It is about identifying risk and the appropriate controls to mitigate risk to an acceptable level.

THREE THINGS AN IT AUDIT IS NOT

But first, especially for those new to the profession and for those outside our profession, it should be noted what IT auditing is not. It is *not* about ordinary accounting controls or traditional financial auditing. That knowledge and skill set served the audit profession well from the beginning of auditing in the middle ages (with exchequers and other forms of auditing) until the introduction of computing systems in the 1950s. In fact, before 1954, it was possible for an auditor to use a very similar audit program from day one of his/her career until he/she retired. To put it simply, the use of computers in accounting systems introduced a new source of risk associated with accounting processes and information (i.e., data). And, it introduced the need for those who understand this new "thing" to identify and mitigate the risk.

IT auditing is also *not* compliance testing. Some believe IT auditors are about making sure people conform to some set of rules—implicit or explicit—and that what we do is report on exceptions to the rules. Actually, that is management's job. It is not the compliance with rules that is of interest to IT auditors. IT auditors are examining whether the entity's relevant systems or business processes for achieving and monitoring compliance are effective. IT auditors also assess the design effectiveness of the rules—whether they are suitably designed or sufficient in scope to properly mitigate the target risk or meet the intended objective.

Compliance failures are important to IT auditors, but for reasons beyond the keeping of rules. A compliance failure can be, and often is, the symptom of a bigger problem related to some risk factor and/or control, such as a defective system or business process, that can or does adversely affect the entity. Thus, to the IT auditor, compliance failures are much more about risk (ultimately) than the rules themselves.

It is also passé to automatically or casually consider IT considerations of an audit to be out of scope because it is not explicitly related to some stated requirement, or to consider an audit to be a waste of time. The fact is IT can and does adversely affect business processes or financial data in ways of which management may not be adequately aware.

UNIQUE INHERENT RISK

IT presents risk factors that are unique to accounting, auditing and systems. That is, IT itself brings risk to the entity regarding its systems, business processes and financial/accounting processing. That risk is unique to IT and without IT being present, that risk would not exist—at least not to the same level. It takes a professional, such as an IT auditor, to identify and assess the inherent risk associated with IT.

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:

ISACA thanks Tommie for his years of service to the Journal *and the association. Your words have influenced many professionals and will continue to do so. Wishing you the very best as you end this chapter and begin the next!*

Those risk factors include systems-related issues, such as systems development, change management and vulnerabilities, and other technology-specific factors. Apart from the IT professional, such risk can go unnoticed, to the detriment of the entity. For example, a university had the following experience related to its financial aid systems.

The university's IT department wrote its own code for financial aid. The university had a great deal of financial aid available as a private institution, leading to the majority of students receiving some form of aid. The experienced IT auditor, seeing these facts, identified certain inherent risk associated with financial aid including the accuracy of the code, the possibility of a bug in the code, and the possibility of fraudulent code that needed to be addressed, examined and mitigated. However, management of the university did not recognize any risk and assumed the IT department had done its due diligence and everything about the financial aid code was acceptable. A few years later, the university accidentally discovered a bug in the code that was causing calculations of financial aid to be overstated. Millions of dollars of financial aid had been awarded over those years in error, and the institution had some financial problems causing it to abandon some of its programs. This case is offered to illustrate the need to identify and assess the inherent risk associated with IT to the entity.

Given that almost all entities employ some level of IT, the day has come when these entities truly need an IT auditor to evaluate their inherent risk of IT. IT auditors are particularly trained and skilled at doing that task. IT auditors are capable of identifying the nature and risk of IT technologies and systems.

> "The day has come when almost all entities truly need an IT auditor to evaluate their inherent risk of IT."

Back to the emerging technologies issues, the place to start with them is to properly assess the nature, specificity and assessed level of risk. Once this process is thought through diligently, the IT auditor and others can begin to put together adequate controls to satisfactorily mitigate risk.

THE ROLE OF CONTROLS

One of the main reasons for a control is to mitigate some identified risk. The way to deal with an inherent risk that is at a level higher than what is acceptable is to implement an effectual control to mitigate that risk to an acceptable level.

Enjoying this article?

- Refer to *Information Systems Auditing: Tools and Techniques*.

www.isaca.org/audit_tools_techniques

That being said, there are some points to remember about controls and the role they play in IT auditing, or auditing in general. First, IT auditors need to be wary of false security by a control that is effective enough to mitigate the risk to an acceptable level. While experienced IT auditors are generally good at this exercise, management and others may not be as adept at understanding the reality of a control.

On the other hand, IT auditors should remember and keep in mind that controls introduce a cost and a benefit. The cost is almost always in real dollars—cost of identifying, designing, implementing and managing the control. The cost can also be an impact cost of inconvenience or operational efficiency in slowing down a process. Some of the latter is not so much a concrete observation as it is an understanding of, and taking into account, the impact of a control. A key for IT auditors has been seeking a balance between these costs (real/concrete and impact) and benefits. Benefits can also be real and concrete—understanding the relative difference in having the control operate effectively and doing without it. That balance is easier to describe than to discern effectually.

For instance, an organization wants to implement an effective password policy for the length of life for passwords. The common wisdom is that the life should be inversely correlated with the amount of risk associated with unauthorized access. That is, if there is a high risk associated with unauthorized access, the life should be short (e.g., 90 days for an online bank account). However, once that policy is implemented, there could be an unintended cost associated with forgotten passwords due to the frequency of changes in them. The result could be users frequently forgetting passwords and having to use entity resources for assistance in obtaining access—a cost that includes delays and frustration, among other results. Thus, the key is due diligence in assessing the real net benefit of a control.

Another consideration is that an entity has a business or purpose for which it is in operation. That purpose needs to be part of the consideration. It is easy to lose sight of the unintended impact on operations.

Generally speaking, the higher the inherent risk, the higher the interest should be in a control to mitigate that risk. IT auditors need to, therefore, consider the level of inherent and residual risk when conveying recommendations for controls.

Last, controls are often embedded in technologies or systems. That fact alone suggests that IT auditors need to be involved in assisting with the design where independence allows it. It also suggests a high importance for using IT auditors to assess the effectiveness of the internal control system. How can the control embedded in IT be properly assessed without an IT subject-matter expert providing assistance in understanding how effectively the control operates?

UNDERSTANDING THE REAL RESIDUAL RISK

One of the issues with analyzing risk is that it is usually relative and subject to judgment. All constituents want controls to be "good enough" so that things will be "okay." But, what is "good enough" and what is "okay"? Risk is not usually subject to an absolute measurement.

Bad managers have a tendency to misjudge or misapply controls and risk. Concerned with surviving and making a profit, they sometimes do not see the reality of residual risk and rush ahead only to encounter a bad result. Or, they get paranoid and avoid a perfectly acceptable risk and take no action to their detriment. Good managers, however, understand the reality of residual risk, and usually make the right decisions and often have a contingency plan should the risk come to the forefront. One of the challenges for IT auditors is to help managers be good or great managers by understanding the real residual risk and taking the appropriate action related to it.

One challenge in understanding the reality of residual risk is to properly assess risk and controls holistically. First, some controls are not IT and there is a tendency by some to overlook a manual control that has the potential to mitigate an IT-related risk. For instance, review and reconciliation by a controller may adequately reduce/mitigate the risk of unauthorized access to data and databases. That is, if someone were able to compromise the access controls, or lack thereof, and compromise data in a financial/accounting database, any error or fraud created would be caught promptly and corrected. Thus, the residual risk may be relatively low considering the manual control.

Second, a residual risk that exists in one area may be addressed by an effective control in another area. For instance, it may be that a firewall has inadequate protection against an outsider coming through the perimeter and hacking into the system. It would be easy to jump to conclusions about the high-level residual risk related to financial data and financial reporting, for example; however, if the entity has strong access controls at the network layer (e.g., a strong Active Directory control matrix and logical segregation of duties), at the application layer, and over the operating system and database access, what are intruders going to do once they gain access through the perimeter? Therefore, it is crucial to do a mental walk-through of how the perceived residual risk will play out if it becomes reality, to determine if it is a real residual risk. This example assumes the audit objective was related to financial reporting. Obviously, if this situation were one where the audit objectives were related to systems in general (internal audit) or the firewall in particular, the residual risk would be real and need attention. Either way, the firewall is broken and probably needs to be fixed.

Scoping the residual risk means the IT auditor also needs to have a mental map of all the broken things in the IT space and which ones are real/relevant and which ones are broken; but out of scope. (The truth is, all IT audits will likely unveil several things, but they may not all be in scope.)

It is also crucial that the IT auditor develop a rational argument for why something found in the IT audit needs to be addressed and remediated, and ensure that it makes sense from a business perspective. The tendency of IT auditors is to find broken things and want them all fixed because they are broken. However, IT auditors need to examine from a business perspective what really needs to be fixed. The rationale should be a reasonable, realistic, business-oriented scenario of a relatively high risk that would come to fruition.

These issues illustrate the need for IT auditors to be effective communicators.[1]

CONCLUSION

What IT auditors do is usually contained in risk and control arenas. Therefore, it is critical that IT auditors be adept at understanding, analyzing and communicating results related to risk and controls and what we do.

ENDNOTE

[1] Singleton, Tommie; "Beyond the IT in IT Audit," *Information Systems Control Journal*, vol. 3, 2008, *www.isaca.org/archives*

How Zero-trust Network Security Can Enable Recovery From Cyberattacks

Eric A. Beck is a cofounder and Principal of Risk Masters Inc., a consulting firm specializing in risk management services. Beck has more than 25 years of business continuity and IT disaster recovery consulting experience across a wide range of clients and industries. Prior to cofounding Risk Masters, Beck led Protiviti's Northeast US business continuity management (BCM) practice as an associate director. Beck is also a former member of the Deloitte & Touche's enterprise risk services BCM practice and global BCM leadership team. He can be reached at *erbeck@riskmastersinc.com.*

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:

Corporate risk managers and security professionals understand that risk is not a problem that can be solved, but rather a process that must be managed. As such, they are constantly searching for new risk mitigation methods and tools in a "cat-and-mouse" game to stay ahead of evolving threats that overtake their ability to manage the threats. Today, within the realm of cybersecurity, a cyberattack from malware is one of those threats.

Late last year, reports surfaced of data breaches at Target, Neiman Marcus and other organizations, making cybersecurity a hot-button issue for most corporate boards, senior executives and government agencies. Incidents like these, targeting retail point-of-sale systems, are believed to be the result of advanced persistent threat (APT) attacks. APT attacks are typically planned and executed by patient hackers over extended periods of time with the intention of stealing or destroying specific data (e.g., customer credit card numbers). Such attacks can remain latent and unidentified as they spread their infection, often surfacing weeks or months after the initial network breach. APTs often start with a brute-force attack designed to steal a privileged user ID and password, or with attempts to trick an employee with privileged system access into opening an email with a viral payload. Once the payload is opened, the infection can then capture the employee's user ID and password or otherwise access an organization's information systems to retrieve confidential data or damage computer systems.

Cyberthreats are not unique to the US. In August 2012, Saudi Aramco and Qatari firm RasGas announced that they had been hacked by what would later become known as the Shamoon virus. Ultimately, the Shamoon attack exfiltrated confidential data and then destroyed thousands of user workstations within each firm. It is believed by many experts that the Shamoon virus was introduced onto the corporate networks of these firms by a disgruntled employee or other insider using a thumb drive that was inserted into a computer server from within each company's data center.

También disponible en español
www.isaca.org/currentissue

Regardless of the method by which a malware infection is introduced, the consequences of a cyberattack can be significant, both financially and in terms of its impact on the company's reputation. Given that the number of similar events is expected to grow in the coming years, it is important to revisit the fundamental elements of risk management and ask whether the organization recognizes and responds effectively to the threat of cyberattacks.

HOLISTIC MANAGEMENT OF CYBERRISK

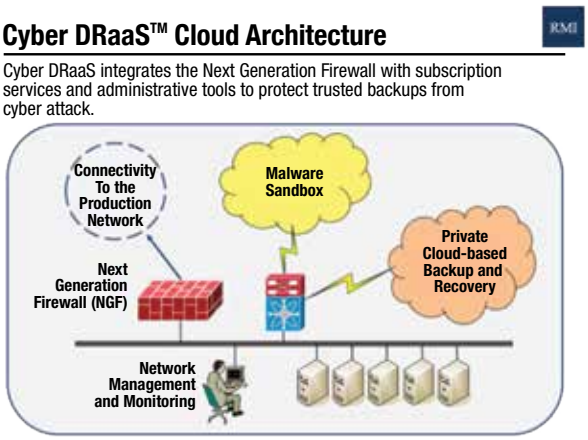
The three major elements of risk management, at their most fundamental level, remain constant as they apply to all potential threats, including cyberattacks. These elements include threat avoidance, operational recovery and risk transfer. How management chooses to balance its investment of limited risk capital across these three elements depends on a number of factors. Most certainly, one of these factors is whether there exists a viable and cost-effective control to mitigate a particular component of risk. For example, as of yet, no one has devised a cost-effective avoidance control for mitigating the aftereffects of an exploding dirty bomb. However, investment in operational recovery can relocate critical business and IT resources to another geography that is sufficiently distant from a bombing site in order to enable continuity of business.

As it pertains to cyberattacks, most organizations have allocated their risk capital to preventive threat avoidance controls. Point solutions such as legacy firewalls, intrusion protection devices, virtual private networks (VPNs) and antivirus scanning reflect some of the controls that companies have relied on to fend off cyberattacks. Additionally, an August 2013 study released by Experian showed that 31 percent of companies have purchased some form of cybersecurity insurance, the most

common form of risk transfer.[1] However, when reviewing current literature pertaining to operational recovery from cyberattacks, one finds very little has been written on the subject. A major reason for this is because there are few controls or countermeasures currently on the market that have been designed specifically for cyberrecovery. This is particularly true for cyberthreats that can remain latent and undetected on a network while they have the ability to compromise the integrity of traditional disaster recovery backups.

Therefore, how does one ensure that a company is properly prepared to rebuild and recover its critical information systems and data in the aftermath of a successful cyberattack? One answer is Cyber DRaaS™ (see **figure 1**), a publicly available IT reference architecture for cyber Disaster Recovery as a Service (DRaaS) that organizations may implement as an investment in cyberrecovery.

Figure 1—Cloud Architecture



© Risk Masters Inc. 2014. All rights reserved.

CYBER DRAAS—A REFERENCE ARCHITECTURE FOR CYBERRECOVERY

Cyber DRaaS has two components that are combined to enable cyberrecovery in an organization:

- **Cyber DRaaS cloud infrastructure**—Cyber DRaaS integrates the Next Generation Firewall (NGF) technology with cloud-based data backup services to create, retain and protect trusted image backups. Trusted images represent base-level backups that will be used to recover critical servers and data in the aftermath of a successful cyberattack. The integrity of trusted images is assured using a combination of end-to-end encryption during data backup, advanced high-performance malware scanning, network-based behavioral analytics that detect malware and data integrity checks within the storage cloud.
- **Cyber DRaaS computer event response planning**—Cyber DRaaS requires careful planning to enable a competent response to a cyberattack. Effective contingency planning for cyberattacks complement Cyber DRaaS infrastructure investment by delivering computer event response team (CERT)-compliant organizational readiness. This includes a customized set of tactical processes and procedures for identifying and responding to cyberattacks.

The two components of Cyber DRaaS combine to deliver a viable and workable capability to recover from the damage inflicted to critical information systems by cyberattacks. The benefits of Cyber DRaaS are significant when compared to those of traditional disaster recovery strategies. Such benefits include:

- Cyber DRaaS incorporates NGF, a disruptive network security technology that blocks unsecure port-level access while delivering enhanced authentication and authorization security at the application and user-ID levels.
- Cyber DRaaS architecture carries with it flexible deployment options that include phased implementation within an existing fortress/moat network or as part of a fully deployed zero-trust network.
- Cyber DRaaS's improved security protections enable an organization to establish real-time connectivity between the production network and the Cyber DRaaS backup cloud. As such, Cyber DRaaS represents an alternative to traditional air-gap solutions that many organizations establish to physically separate a production network from off-line trusted images backups.
- Cyber DRaaS reduces the amount of time that will be required to recover from a cyberattack by simplifying the process of recovery and enabling early recognition that an attack has occurred.

Enjoying this article?

- Refer to other cybersecurity resources.
  www.isaca.org/cyber
- Discuss and collaborate on cybersecurity and network security in the Knowledge Center.
  www.isaca.org/knowledgecenter

- Cyber DRaaS offers a highly secure alternative to traditional data backup architectures that may become the next-generation solution model for production disaster recovery backup.
- For corporate officers and directors, investment in Cyber DRaaS clearly demonstrates due diligence in mitigating the growing threat from cyberattacks, thereby limiting potential liability from shareholder derivative suits.

The NGF is one of several critical components of Cyber DRaaS (see **figure 2**) because it represents a disruptive technology in network architecture, one that has been described as a firewall on steroids. That is because the NGF integrates common network security point solutions, such as remote access, intrusion protection, token authentication and deep-packet scanning, into a single high-performance device (see **figure 3**). The NGF also offers stronger access-control capabilities than the current generation of port-based firewalls because authorization occurs at the application and user levels while simultaneously blocking all port-level access. By

Figure 2—Cyber DRaaS Critical Technology Components

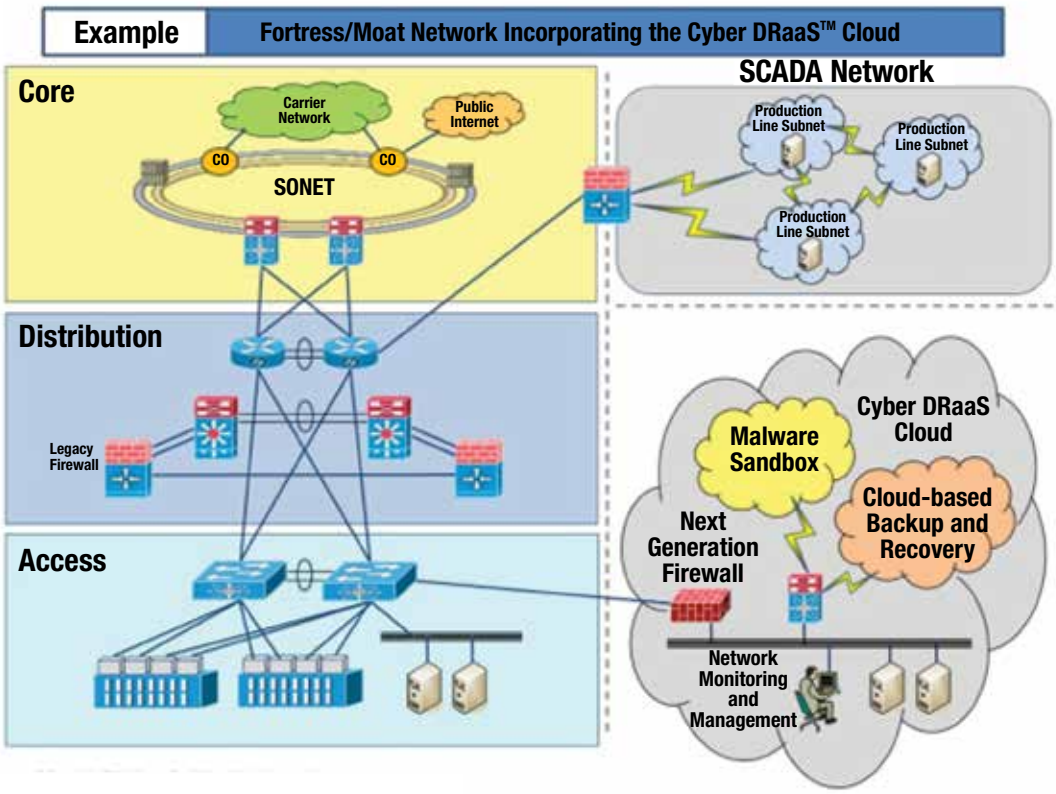
Cyber DRaaS™—Critical Technology Components

Cyber DRaaS incorporates the following enabling technologies.

Cloud Backup and Recovery	• Manages data backup and restore processes for trusted images • Routine integrity checking of trusted image backups • Optimal performance with data compression and duplication
Next Generation Firewall	• Network policy enforcement at application/user level, not port • Content scanning for known and unknown malware signatures • Predictable high-performance single-pass software engine
Network Management	• Policy-driven security management across deployed firewalls • Visibility into network traffic, deployed applications and policies • Graphical tools enabling immediate investigation of malware
Malware Sandbox	• Malicious content/malware redirected to virtualized sandbox • Monitoring of known signatures and malicious network behaviors • New malware discoveries generate new dataase signatures

© Risk Masters Inc. 2014. All rights reserved.

Figure 3—Incorporating Cyber DRaaS Into Fortress/Moat Security Models



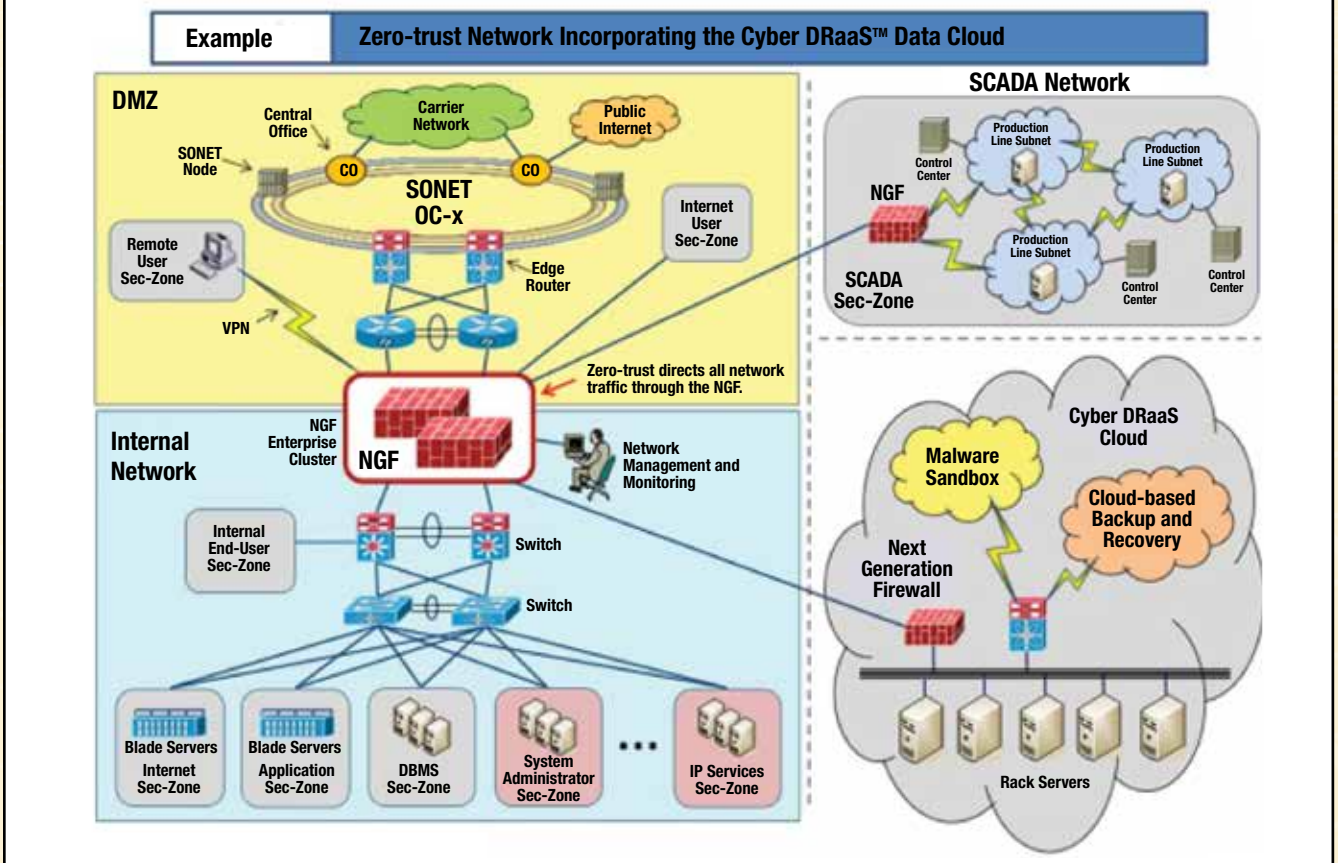
© Risk Masters Inc. 2014. All rights reserved.

combining both authentication and authorization, neither one of which offers sufficient protection in and of itself, the NGF virtually eliminates the likelihood of unauthorized intrusion into the Cyber DRaaS cloud to corrupt trusted image backups.

Cyber DRaaS also incorporates two vendor-provided cloud services. The first cloud service includes automated backup and restore functions, offering end-to-end encryption of data from the source server to the destination storage cloud. Backup data are scanned for malware signatures as they pass through the NGF by first decrypting the data to validate their content and then reencrypting the data before transmission into the cloud. The integrity of data stored in the cloud is also periodically checked using hash totaling or other algorithms. Organizations should check with their chosen cloud service provider to understand what service options it provides in terms of frequency of integrity checks, specific hashing algorithms used and encryption alternatives.

The second cloud service includes behavioral heuristics used by the NGF against all data traffic to identify suspect and unknown malware that is then redirected and isolated into a cloud-based sandbox. Once isolated, the malware can be further analyzed to define its signature. Each newly identified signature is then automatically redistributed back to the NGF's malware signature database, thereby ensuring that scanning profiles remain current as each new threat is identified.

Figure 4—Zero-trust Network Incorporating Cyber DRaaS Data Cloud



© Risk Masters Inc. 2014. All rights reserved.

CYBER DRAAS IN A ZERO-TRUST NETWORK

Organizations looking for a more advanced architecture for cyberresiliency should consider deploying Cyber DRaaS under what John Kindervag of Forrester Research has termed a zero-trust network (see **figure 4**). Zero-trust network architecture replaces the fortress/moat model comprised of core, distribution and access layers with an alternative architecture reflecting a hub-and-spoke design. Zero trust places a high-performance NGF cluster at the center of the network to act as a data traffic distribution hub, segmenting the network into isolated work groups. Zero trust also assumes that all data traffic on the network is untrusted. Therefore, all traffic must be scanned for malware and then authorized by the NGF according to a predetermined rule set before being allowed to traverse the network within a work group. As such, Cyber DRaaS can be easily deployed under its own security zone within the zero-trust network architecture to enable secure recovery from any potential cyberattack.

Adoption of the NGF and deployment of a zero-trust network architecture are still in their infancy today as many enterprises remain committed to their existing investments in fortress/moat network defenses and point security solutions. Most enterprises that have deployed the NGF have done so on a limited basis around highly critical applications, such as Payment Card Industry Data Security Standard (PCI DSS) compliance or to protect critical customer databases. This type of limited deployment is precisely how Cyber DRaaS can be implemented under a fortress/moat network to protect trusted images. However, as the frequency and sophistication of cyberattacks continue to increase, organizations may come to see the benefits of enterprise deployment of a zero-trust network model and expand its use to build a more cyberresilient data network.

CONCLUSION

Cyber DRaaS does not reflect a future theoretical architecture for cyberrecovery, but rather one that can be implemented today with existing technology and proper planning. Therefore, managers who are looking for a strategy to comply with the US National Institute of Standards and Technology (NIST) Cybersecurity Framework requirements for response and recovery, or who are more generally concerned about how they can mitigate cyberrisk, should give due consideration to Cyber DRaaS. By deploying Cyber DRaaS, management will have the tools it needs to proactively respond to cyberthreats before they happen and to recover critical data and information systems from cyberattacks after they occur.

ENDNOTES

[1] "Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age," Ponemon Institute, August 2013, sponsored by Experian® Data Breach Resolution, *www.experian.com/innovation/business-resources/ponemon-study-managing-cyber-security-as-business-risk.jsp?ecd_dbres_cyber_insurance_study_ponemon_referral*

COBIT® Focus
is where global professionals share their practical tips for using and implementing ISACA's frameworks.

Free subscriptions.
Subscribe Now!

For more information, contact the editors at *publication@isaca.org.*

This weekly digital publication accepts articles for review on an ongoing basis.
Learn more at *www.isaca.org/cobitsubmit.*

Leveraging Industry Standards to Address Industrial Cybersecurity Risk

Ivan Alcoforado, CISSP, PMP, is a senior manager in KPMG's risk consulting and IT advisory practice with more than 18 years of experience helping design and deliver projects for large organizations in information risk; security; program and project management; identity and access management; business continuity and disaster recovery; and governance, risk and compliance (GRC). He also holds an ISA 99/IEC 62443 Cybersecurity Fundamentals Specialist certificate from the International Society of Automation (ISA) and can be reached at *ialcoforado@kpmg.ca.*

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:

Industrial automation control systems (IACS) technologies have increasingly converged with those used by regular IT systems, including the use of Internet Protocol (IP) interconnections and Windows-based computers, with consequent growth in their technology and cybersecurity risk profile.

Incidents involving IACS are often the result of outdated security control practices, aging IT technologies, and knowledgeable internal and external attackers. Some incidents have low profiles, causing odd behaviors and small disruptions that go unexplained, and others have bigger consequences with major operational and safety impacts. The US Industrial Control Systems Computer Emergency Response Team (ICS-CERT) responded to 256 incidents in 2013 (85 percent more than in 2012).[1] This might not seem like much when compared with the 47,000 computer incidents reported in 2013 by Verizon in its data breach report,[2] but the consequences of a cybersecurity incident involving IACS can be disastrous. The 2012 cyberattack on Saudi Aramco, for instance, damaged 30,000 computers and was aimed at disrupting production.[3] Luckily, it failed to affect oil and gas assets. A nonattack-related problem with a supervisory control and data acquisition (SCADA) system in the US, for instance, led to the spill of more than 1,000,000 gallons of crude oil in 2010.[4]

Breach-disclosure regulations are usually concerned with consumer privacy and frequently do not apply to IACS because they do not normally include personally identifiable information (PII). However, in 2011, the US Securities and Exchange Commission (SEC) Corporate Finance (CF) Disclosure Guidance: Topic No. 2[5] broadened the understanding of disclosure obligations of public companies. Considering cyberincidents as the result of both attacks and unintentional actions, the SEC's Division of Corporation Finance understands that companies should disclose cyberincidents "that are individually, or in the aggregate, material, including a description of the costs and other consequences." Additionally, it requires discussion about the aspects of the "business or operations that give rise to material cybersecurity risks" and risk of incidents "that may remain undetected for an extended period."[6] This means that, depending on the nature of the business and its operations, cybersecurity IACS-related risk and incidents may need to be disclosed.

In a similar way, Canadian Securities Administration (CSA) Staff Notice 11-326 asks registrants to consider whether risk, incidents and controls "are matters they need to disclose in a prospectus or a continuous disclosure filing."[7] The CSA specifically addresses cybercrime, thus leaving out some unintentional actions, but it should consider cyberattacks involving IACS, depending on the nature of the company's business.

Given the potential safety, environmental and operational impacts a major IACS incident may cause, management should be concerned with enhancing resiliency and response capabilities to these threats while keeping key stakeholders well informed.

DEFINING IACS

IACS is the term adopted by The International Society of Automation (ISA) to broadly refer to several types of components and systems in all industries. This includes, but is not limited to:

- **SCADA systems**—Used on geographically dispersed field assets where central monitoring and control are needed; frequently found in railway transportation systems and oil and natural gas pipelines
- **Distributed control systems (DCS)**—Architecture composed of subsystems responsible for controlling localized processes; often found in electrical power generation and distribution, water management, traffic management, and process-based industries such as chemicals, oil refineries, metallurgical and pharmaceutical

- **Programmable logic controllers (PLC)**—Computerized devices equipped with nonvolatile memory used to control equipment and processes; used extensively in several industries, including manufacturing, transportation and mining
- **Safety instrumented systems (SIS)**—Hardware and software controls used on hazardous processes to prevent or mitigate consequences; found in several industries and require special attention when protecting against cybersecurity risk

TYPICAL CYBERSECURITY THREATS TO IACS

Cybersecurity incidents impacting IACS may result from the following threat agents:

- **Insider action**—Typically employee or contractor unintentional misuse or intentional abuse resulting in disruption or circumvention of existing controls
- **Industrial spies/competitive intelligence**—Usually working on behalf of competitors and trying to gather information such as production capacity, technologies involved and plant architecture
- **Botnet operators/spammers/phishers**—People who operate schemes for hire and obtain monetary gain by executing or enabling attacks for others, usually involving, for example, denial of service (DoS) or malware distribution
- **Hacktivists**—Individuals motivated by political, environmental or ideological causes
- **Organized crime**—Groups motivated by financial gain. The threat of disruption may be used to blackmail an organization.
- **Foreign governments**—System attacks by foreign agents or state-sponsored groups to steal industrial secrets, disrupt production and, potentially, exploit safety hazards
- **Natural**—Physical events caused by nature, e.g., tornados, floods, earthquakes

These elements typically exploit IACS environments by taking advantage of control weaknesses. **Figure 1** indicates potential impacts of exploiting IACS control weaknesses.

WHAT SHOULD AN IACS CYBERSECURITY PROGRAM LOOK LIKE?

All IACS programs need to take into consideration their dissimilarities from traditional IT. There are several differences, but three types are key:

1. **Focus on safety and availability**—In an environment where failure can result in operational disruption and loss of life, outages and variances from performance specifications are unacceptable.
2. **Specialized and proprietary technologies**—While IT focuses on interoperability and standardization to gain efficiencies, IACS were developed independently by multiple vendors with a focus on the challenges of individual plants or industries.

Figure 1—Potential Impacts From Common IACS Control Weaknesses

		Threats					
		Unauthorized Commands	Unauthorized Configuration Change	Information Gathering	Unauthorized System Access	Disruption/ Destruction	Detection Evasion
Control Weaknesses	Poor physical security		X		X	X	
	Low security awareness			X	X		
	Weak protocol security	X		X	X		
	Inadequate network segregation				X	X	
	Lenient access controls	X			X		X
	Component remote access/backdoors	X			X		
	Malware (including advanced persistent threats [APTs])	X	X	X	X	X	
	Weak audit logs						X

Source: Ivan Alcoforado. Reprinted with permission.

3. **Equipment lifetime**—It is not unusual to find plants with commercial lifetimes of 20, 30 or 40 years. This is particularly challenging when using IP or Windows-based components, which usually follow the typical three-to-five-year lifetime expectancy of technology.

Taking these differences into account, a robust IACS cybersecurity program should identify priorities and controls, paying special attention to critical operations and safety hazards and their associated controls. It should:

- Take a risk-based approach when assessing capabilities, identifying priorities and applicable requirements to prepare the organization. Bear in mind that, as a result of this assessment, some IACS might be identified as so critical and/or hazardous that a high-protection approach is needed, zeroing vulnerabilities and isolating components.
- Set up an IACS cybersecurity framework, leveraging broad standards such as International Electrotechnical Commission's IEC 62443/ISA 99 and/or industry-focused standards such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), to establish objectives and then define processes, controls, technologies and teams to protect the IACS environment
- Establish metrics and goals together with testing, monitoring, response and auditing processes to detect and respond to deficiencies and incidents
- Integrate the organization, engaging operations personnel; automation engineers; health, safety and environment (HSE) teams; continuity management areas; and security teams through cross-functional synergies and joint processes
- Enable the organization, raising awareness of staff on the importance of security and building the skills needed to assess, protect, detect and respond to cybersecurity incidents
- Build a threat intelligence model and ecosystem that allow the organization to follow evolving threats and issues in the IACS world that are relevant to its operation. New threats are discovered daily and attackers need to find only one flaw to successfully execute an attack.
- Collaborate with industry organizations, component manufacturers, service providers, incident response teams and law enforcement. Industry organizations can help improve standards and learn from known incidents. Manufacturers and service providers should help organizations deal with vulnerabilities and improve the environment. Response teams and law enforcement should help organizations deal with more serious incidents. Especially when dealing with attacks perpetrated by organized crime and foreign governments, external help is needed to defend from such resourceful groups.

Enjoying this article?

- Read *Implementing the NIST Cybersecurity Framework*.

http://www.isaca.org/us-cyber-implementation

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

www.isaca.org/topic-cybersecurity

UNDERSTANDING IACS SECURITY STANDARDS

One of the challenges when establishing an IACS cybersecurity framework is the lack of relevant, broad, universally accepted standards or frameworks, such as the International Organization for Standardization's ISO 27000 series and COBIT®. Such sources can help define the components of an organization's framework by providing a comprehensive list of activities and controls that can be tailored to a company's particular context. As certain industry initiatives evolve, this situation should be resolved for IACS.

For example, in February 2014, the US National Institute of Standards and Technology (NIST) published the first version of its *Framework for Improving Critical Infrastructure Cybersecurity*. This framework is composed of three basic parts:

- **Core**—With a set of activities and expected outcomes that are common to critical infrastructure and IACS, this section includes useful mapping to other standards and frameworks, such as the latest version of ISO 27001 published in 2013, COBIT® 5 and ISA 62443.
- **Tiers**—Describe the degree of cybersecurity risk management practices in an organization. While not a full-fledged maturity model, the approach establishes four tiers from "partial" to "adaptive," with the latter being the most complete level.

- **Profile**—Used to represent the current as-is state and the target to-be state to allow planning, prioritization and monitoring of progress metrics. The profile can also be used for self-assessments and communications.

Another key initiative, led by the ISA, is a set of standards, ISA/IEC 62443 (formerly ISA99, and now in collaboration with the International Electrotechnical Commission), aimed at protecting industrial automation and control systems. These standards establish good security practices for designing, building and implementing components and complete IACS and, in their operation, establish an IACS security management system.

The standards are divided into four parts and are evolving, with some documents still under development:

- **General**—Establishes the context for all standards in the series, defining concepts and terminology, as well as life cycle and compliance metrics
- **Policies and procedures**—Provides guidance for developing an IACS security management system and, in the future, certification of supplier policies and practices
- **System**—Identifies security technologies, requirements and assurance levels for IACS networks
- **Component**—Describes product development and technical security requirements for IACS equipment

As a recent and evolving standard, ISA/IEC 62443 is fairly updated with regard to current security challenges in IACS environments, and even its draft documents provide some insight into good practices and solutions. Alignment with these standards represents an important step toward compliance with industry practices and protection of critical infrastructure assets.

A number of industry-specific standards exist, such as the American Petroleum Institute (API) 1164 "Pipeline SCADA Security," the US Transportation Security Authority (TSA) "Pipeline Security Guidelines," and the American Gas Association Report No. 12 "Cryptographic Protection of SCADA Communications," to address specific challenges of each vertical. One of the most complete standard sets is the NERC CIP, established in 2006. It can be viewed as covering three main aspects:

- **Management**—Establishing a risk-based approach and security policies, together with personnel security measures, from training to background checks (CIP 002 "Critical Asset Identification," CIP 003 "Security Management Controls" and CIP 004 "Cyber Security Personnel and Training")
- **Asset protection**—Defining logical and physical security measures to protect critical assets, including hardening, configuration management, technical assessments and monitoring (CIP 005 "Electronic Security Perimeter" and CIP 006 "Physical Security")
- **Operations**—Identifying processes to secure critical assets and incident response and recovery procedures to handle issues (CIP 007 "System Security Management," CIP 008 "Incident Reporting and Response Planning" and CIP 009 "Recovery Plan for Critical Cyber Assets")

Although focused on and mandatory only for the electric sector, NERC CIP provides valuable guidance in the protection of critical assets that may be transferable to other industries.

SETTING UP AN IACS CYBERSECURITY FRAMEWORK

Figure 2 provides an example of an organization's IACS cybersecurity framework, designed using standards, but tailored for the environment. For each item in the program scope there is a process, an action plan, and standard and/or control documentation. Governance and policies use existing enterprisewide structures and processes. Monitoring uses already-established areas and processes, but defines adjustments needed on each one to support the IACS cybersecurity program and perform proper reporting.

When establishing this framework, the structure of the COSO *Internal Control—Integrated Framework* was used as a foundation with provisions sought from other standards. Whenever a provision is not available or is considered incomplete in an IACS standard or framework, COBIT elements are used to address the gap. A summary of the standards used can be found in **figure 3**.

CONCLUSION

As more and more organizations start reporting cybersecurity risk and incidents, security professionals, internal auditors and IT auditors need to pay as much attention to IACS controls as they do to controls for traditional IT. IACS technologies are increasingly using standard IT components, and, as a consequence, the threat landscape to these environments has grown. However, IT standards and controls are not immediately applicable to IACS due to specific business and operational requirements.

Figure 2—Example of IACS Cybersecurity Framework

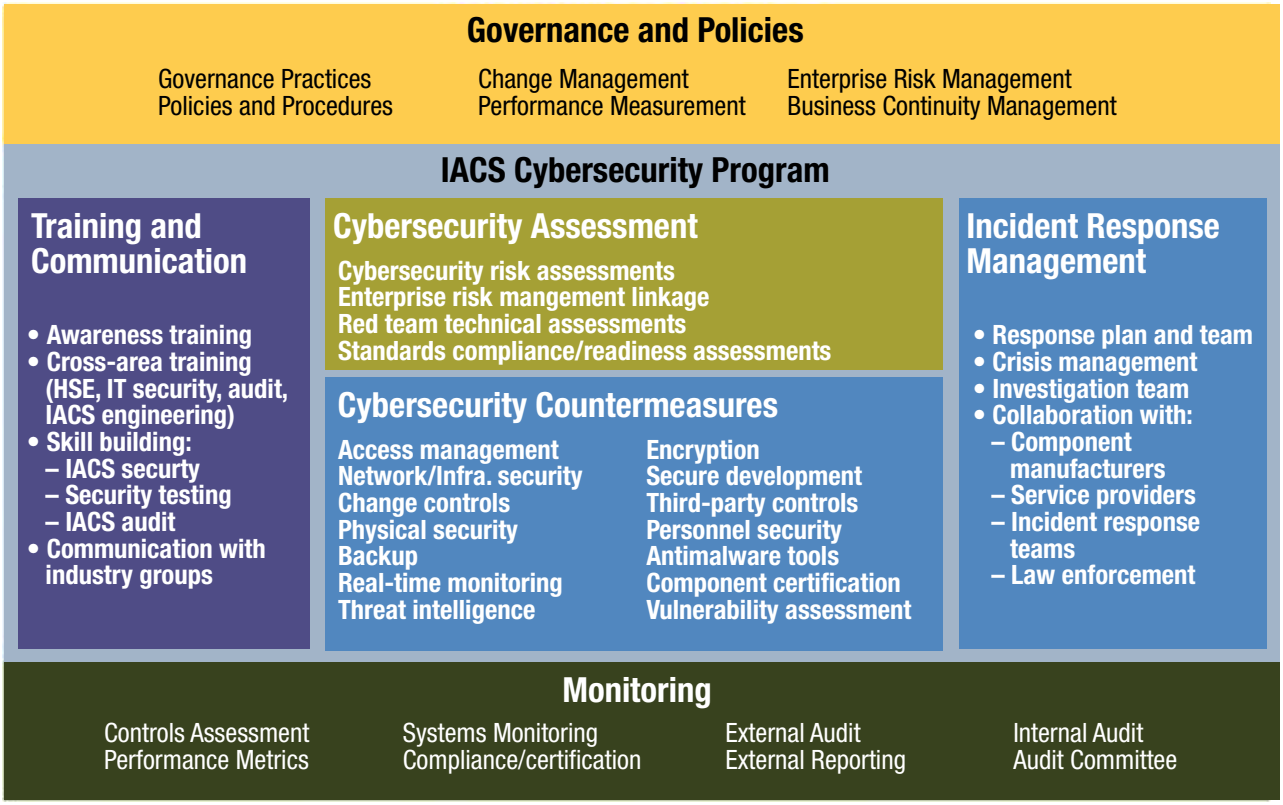


Figure 3—Standards Leveraged for IACS Cybersecurity Framework Example

	NIST Framework	ISA/IEC 62443	NERC CIP	COBIT 5
Governance and policies	ID.BE, ID.GV	2-1		EDM01, 03 AP007
Cybersecurity assessment	ID.AM, ID.RA, ID.RM	1-1, 2-1, 3-3	CIP-002	AP001, 02, 08, 12, 13
Cybersecurity countermeasures	PR.AC, PR.DS, PR.IP, PR.MA, PR.PT, DE.AE, DE.CM, DE.DP	2-1, TR 3-1, 3-3	CIP-003 CIP-005 CIP-006	BAI02, 03, 06, 07, 09, 10 DSS04, 05
Incident response management	RS.RP, RS.CO, RS.AN, RS.MI, RS.IM, RC.RP, RC.IM	2-1, 3-3	CIP-008 CIP-009	DSS02, 04
Training and communication	PR.AT, RS.CO, RC.CO	2-1	CIP-004	BAI05, 08 DSS04
Monitoring		1-3 (draft 5) 2-1	CIP-003	EDM05, MEA01, 02, 03

Source: Ivan Alcoforado. Reprinted with permission.

Several IACS security standards and framework initiatives, as noted previously, have been published in recent years and can be valuable tools when establishing a company's IACS cybersecurity framework. They constitute good references for IACS security, but might not fit directly in an organization's control environment and need to be tailored. In a field evolving as rapidly as security, tight integration with a company's controls and dynamic processes to keep up with threats are essential to success.

REFERENCES

Robinson, M.; "The SCADA Threat Landscape," 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013), BCS The Chartered Institute for IT, UK, 16-17 September 2013

National Institute of Standards and Technology, "NIST Cybersecurity Framework—ISA 99 Response to Request for Information," The International Society of Automation (ISA), USA, 5 April 2013

Department of Homeland Security, "Roadmap to Secure Control Systems in the Transportation Sector," USA, August 2012

National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," USA, 12 February 2014

ISA99 Committee, *http://isa99.isa.org/*

Transportation Security Authority, "Pipeline Security Guidelines," US Department of Homeland Security (DHS), USA, April 2011

ENDNOTES

[1] Industrial Control Systems Computer Emergency Response Team, *ICS-CERT Monitor*, October-December 2013, *https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf*

[2] Verizon, *2013 Data Breach Investigation Report*, *www.verizonenterprise.com/DBIR/2013/*

[3] Industrial Control Systems Computer Emergency Response Team, *ICS-CERT Monitor*, January-March 2013, *https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Jan-Mar2013.pdf*

[4] Walsh, D.; "Cyberstalkers Threaten Pipeline Security," *The New York Times* Green blog, 10 January 2013, *http://green.blogs.nytimes.com/2013/01/10/cyberstalkers-threaten-pipeline-security/?_php=true&_type=blogs&_r=0* and "EPA Response to Enbridge Spill in Michigan," *http://epa.gov/enbridgespill*

[5] US Securities and Exchange Commission, Division of Corporation Finance, "CF Disclosure Guidance: Topic No. 2—Cybersecurity," USA, 13 October 2011, *www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm*

[6] *Ibid*.

[7] Canadian Securities Administrators, "CSA Staff Notice 11-326—Cyber Security," October 2013, *www.albertasecurities.com/Regulatory%20Instruments/4642797-v2-CSA_Staff_Notice_11-326_Cyber_Security.pdf*

Bridging the Gap Between Access and Security in Big Data

Ulf T. Mattsson is the chief technology officer (CTO) of Protegrity. He created the initial architecture of Protegrity's database security technology, for which the company owns several key patents. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's research and development organization in the areas of IT architecture and IT security.

Organizations are failing to truly secure their sensitive data in big data environments. Data analysts require access to the data to efficiently perform meaningful analysis and gain a return on investment (ROI), and traditional data security has served to limit that access. The result is skyrocketing data breaches and diminishing privacy, accompanied by huge fines and disintegrating public trust. It is critical to ensure individuals' privacy and proper security while retaining data usability and enabling organizations to responsibly utilize sensitive information for gain.

También disponible en español
www.isaca.org/currentissue

(BIG) DATA ACCESS

The Hadoop platform for big data is used here to illustrate the common security issues and solutions. Hadoop is the dominant big data platform, used by a global community, and it lacks needed data security. The platform provides a massively parallel processing platform[1] designed for access to extremely large amounts of data and experimentation to find new insights by analyzing and comparing more information than was previously practical or possible.

Data flow in faster, in greater variety, volume and levels of veracity, and can be processed efficiently by simultaneously accessing data split across up to hundreds or thousands of data nodes in a cluster. Data are also kept for much longer periods of time than would be in databases or relational database management systems (RDBMS), as the storage is more cost-effective and historical context is part of the draw.

A FALSE SENSE OF SECURITY

If the primary goal of Hadoop is data access, data security is traditionally viewed as its antithesis. There has always been a tug of war between the two based on risk, balancing operational performance and privacy, but the issue is magnified exponentially in Hadoop (**figure 1**).

For example, millions of personal records may be used for analysis and data insights, but the privacy of all of those people can be severely compromised from one data breach. The risk involved is far too high to afford weak security, but obstructing performance or hindering data insights will bring the platform to its knees.

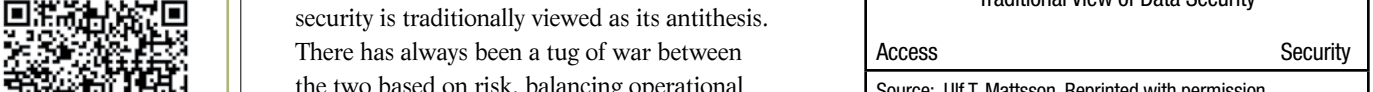
Despite the perception of sensitive data as obstacles to data access, sensitive data in big data platforms still require security according to various regulations and laws,[2] much the same as any other data platform. Therefore, data security in Hadoop is most often approached from the perspective of regulatory compliance.

One may assume that this helps to ensure maximum security of data and minimal risk, and, indeed, it does bind organizations to secure their data to some extent. However, as security is viewed as obstructive to data access and, therefore, operational performance, the regulations actually serve as a guide to the least-possible amount of security necessary to comply. Compliance does not guarantee security.

> "Compliance does not guarantee security."

Obviously, organizations do want to protect their data and the privacy of their customers, but access, insights and performance are paramount. To achieve maximum data access and security, the gap between them must be bridged. So how can this balance best be achieved?

Figure 1—Traditional View of Data Security



Source: Ulf T. Mattsson. Reprinted with permission.

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:

DATA SECURITY TOOLS

Hadoop, as of this writing, has no native data security, although many vendors both of Hadoop and data security provide add-on solutions.[3] These solutions are typically based on access control and/or authentication, as they provide a baseline level of security with relatively high levels of access.

Access Control and Authentication

The most common implementation of authentication in Hadoop is Kerberos.[4] In access control and authentication, sensitive data are displayed in the clear during job functions—in transit and at rest. In addition, neither access control nor authentication provides much protection from privileged users, such as developers or system administrators, who can easily bypass them to abuse the data. For these reasons, many regulations, such as the Payment Card Industry Data Security Standard (PCI DSS)[5] and the US Health Insurance Portability and Accountability Act (HIPAA),[6] require security beyond them to be compliant.

Coarse-grained Encryption

Starting from a base of access controls and/or authentication, adding coarse-grained volume or disk encryption is the first choice typically for actual data security in Hadoop. This method requires the least amount of difficulty in implementation while still offering regulatory compliance. Data are secure at rest (for archive or disposal), and encryption is typically transparent to authorized users and processes. The result is still relatively high levels of access, but data in transit, in use or in analysis are always in the clear and privileged users can still access sensitive data. This method protects only from physical theft.

Fine-grained Encryption

Adding strong encryption for columns or fields provides further security, protecting data at rest, in transit and from privileged users, but it requires data to be revealed in the clear (decrypted) to perform job functions, including analysis, as encrypted data are unreadable to users and processes.

Format-preserving encryption preserves the ability of users and applications to read the protected data, but is one of the slowest performing encryption processes.

Implementing either of these methods can significantly impact performance, even with the fastest encryption/decryption processes available, such that it negates many of the advantages of the Hadoop platform. As access is paramount, these methods tip the balance too far in the direction of security to be viable.

Some vendors offer a virtual file system above the Hadoop Distributed File System (HDFS), with role-based dynamic data encryption. While this provides some data security in use, it does nothing to protect data in analysis or from privileged users, who can access the operating system (OS) and layers under the virtual layer and get at the data in the clear.

Data Masking

Masking preserves the type and length of structured data, replacing it with an inert, worthless value. Because the masked data look and act like the original, they can be read by users and processes.

Static data masking (SDM) permanently replaces sensitive values with inert data. SDM is often used to perform job functions by preserving enough of the original data or de-identifying the data. It protects data at rest, in use, in transit, in analysis and from privileged users. However, should the cleartext data ever be needed again (i.e., to carry out marketing operations or in health care scenarios), they are irretrievable. Therefore, SDM is utilized in test/development environments in which data that look and act like real data are needed for testing, but sensitive data are not exposed to developers or systems administrators. It is not typically used for data access in a production Hadoop environment. Depending on the masking algorithms used and what data are replaced, SDM data may be subject to data inference and be de-identified when combined with other data sources.

Dynamic data masking (DDM) performs masking "on the fly." As sensitive data are requested, policy is referenced and masked data are retrieved for the data the user or process is unauthorized to see in the clear, based on the user's/process's role. Much like dynamic data encryption and access control, DDM provides no security to data at rest or in transit and

Enjoying this article?

- Read *Big Data: Impacts and Benefits*.
  www.isaca.org/Big-Data-WP
- Discuss and collaborate on big data in the Knowledge Center.
  www.isaca.org/topic-big-data

little from privileged users. Dynamically masked values can also be problematic to work with in production analytic scenarios, depending on the algorithm/method used.[7]

Tokenization

Tokenization also replaces cleartext with a random, inert value of the same data type and length, but the process can be reversible. This is accomplished through the use of token tables, rather than a cryptographic algorithm. In vaultless tokenization, small blocks of the original data are replaced with paired random values from the token tables overlapping between blocks. Once the entire value has been tokenized, the process is run through again to remove any pattern in the transformation.

However, because the exit value is still dependent upon the entering value, a one-to-one relationship with the original data can still be maintained and, therefore, the tokenized data can be used in analytics as a replacement for the cleartext. Additionally, parts of the cleartext data can be preserved or "bled through" to the token, which is especially useful in cases where only part of the original data is required to perform a job.

Tokenization also allows for flexibility in the levels of data security privileges, as authority can be granted on a field-by-field or partial field basis. Data are secured in all states: at rest, in use, in transit and in analytics.

BRIDGING THE GAP

In comparing the methods of fine-grained data security (**figure 2**), it becomes apparent that tokenization offers the greatest levels of accessibility and security. The randomized token values are worthless to a potential thief, as only those with authorization to access the token table and process can ever expect to return the data to their original value. The ability to use tokenized values in analysis presents added security and efficiency, as the data remain secure and do not require additional processing to unprotect or detokenize them.

This ability to securely extract value from de-identified sensitive data is the key to bridging the gap between privacy and access. Protected data remain useable to most users and processes, and only those with privileges granted through the data security policy can access the sensitive data in the clear.

DATA SECURITY METHODOLOGY

Data security technology on its own is not enough to ensure an optimized balance of access and security. After all, any system is only as strong as its weakest link and, in data security, that link is often a human one. As such, a clear, concise methodology can be utilized to help optimize data security processes and minimize impact on business operations (**figure 3**).

Figure 2—Comparison of Fine-grained Data Security Methods

Data Security Methods	Performance	Storage	Security	Transparency
System without data protection	●	●	○	●
Monitoring + blocking + obfuscation	◔	●	◔	◔
Data type preservation encryption	◒	●	◒	◔
Strong encryption	◔	◔	●	◔
Vaultless tokenization	●	●	●	◔
Hashing	●	◔	●	○
Anonymization	●	●	●	○

Worst ○ ◔ ◒ ◔ ● Best

Source: Ulf T. Mattsson. Reprinted with permission.

Figure 3—Data Security Methodology	
Classification	Determine what data are sensitive to the organization, either for regulatory compliance and/or internally.
Discovery	Find out where the sensitive data are located, how they flow, who can access them, performance and other requirements for security.
Security	Apply the data security method(s) that best achieve the requirements from discovery, and protect the data according to the sensitivity determined in classification.
Enforcement	Design and implement data security policy to disclose sensitive data only to authorized users, according to the least possible amount of information required to perform job functions (least-privilege principle).
Monitoring	Ensure ongoing, highly granular monitoring of any attempts to access sensitive data. Monitoring is the only defense against authorized user data abuse.
Source: Ulf T. Mattsson. Reprinted with permission	

Classification

The first consideration of data security implementation should be a clear classification of which data are considered sensitive, according to outside regulations and/or internal security mandates. This can include anything from personal information to internal operations analysis results.

Discovery

Determining where sensitive data are located, their sources and where they are used are the next steps in a basic data security methodology. A specific data type may also need different levels of protection in different parts of the system. Understanding the data flow is vital to protecting it.

Also, Hadoop should not be considered a silo outside of the enterprise. The analytical processing in Hadoop is typically only part of the overall process—from data sources to Hadoop, up to databases, and on to finer analysis platforms. Implementing enterprisewide data security can more consistently secure data across platforms, minimizing gaps and leakage points.

Security

Next, selecting the security method(s) that best fit the risk, data type and use case of each classification of sensitive data, or data element, ensures that the most effective solution across all sensitive data is employed. For example, while vaultless tokenization offers unparalleled access and security for structured data, such as credit card numbers or names, encryption may be employed for unstructured, nonanalytical data, such as images or other media files.

It is also important to secure data as early as possible, both in Hadoop implementation and in data acquisition/creation. This helps limit the possible exposure of sensitive data in the clear.

Enforcement

Design a data security policy based on the principle of least privilege (i.e., revealing the least possible amount of sensitive data in the clear in order to perform job functions). This may be achieved by creating policy roles that determine who has access or who does not have access, depending on which number of members is least. A modern approach to access control can allow a user to see different views of a particular data field, thereby exposing more or less of the sensitive content of that data field.

Assigning the responsibility of data security policy administration and enforcement to the security team is very important. The blurring of lines between security and data management in many organizations leads to potentially severe abuses of sensitive data by privileged users. This separation of duties prevents most abuses by creating strong automated control and accountability for access to data in the clear.

Monitoring

As with any data security solution, extensive sensitive data monitoring should be employed in Hadoop. Even with proper data security in place, intelligent monitoring can add a context-based data access control layer to ensure that data are not abused by authorized users.

What separates an authorized user and a privileged user? Privileged users are typically members of IT who have privileged access to the data platform. These users may include system administrators or analysts who have relatively unfettered access to systems for the purposes of maintenance and development. Authorized users are those who have been granted access to view sensitive data by the security team.

Highly granular monitoring of sensitive data is vital to ensure that both external and internal threats are caught early.

CONCLUSION

Following these best practices would enable organizations to securely extract sensitive data value and confidently adopt big data platforms with much lower risk of data breach. In addition, protecting and respecting the privacy of customers and individuals helps to protect the organization's brand and reputation.

The goal of deep data insights, together with true data security, is achievable. With time and knowledge, more and more organizations will reach it.

ENDNOTES

[1] The Apache Software Foundation, *http://hadoop.apache.org*. The Apache Hadoop software library is a framework that allows for distributed processing of large data sets across clusters of computers using simple programming models. It is designed to scale up from single servers to thousands of machines, each offering local computation and storage. Rather than relying on hardware to deliver high availability, the library itself is designed to detect and handle failures at the application layer, thus delivering a highly available service on top of a cluster of computers, each of which may be prone to failures.

[2] Commonly applicable regulations include US Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS), US Sarbanes-Oxley, and state or national privacy laws.

[3] These solution providers include Cloudera, Gazzang, IBM, Intel (open source), MIT (open source), Protegrity and Zettaset, each of which provide one or more of the following solutions: access control, authentication, volume encryption, field/column encryption, masking, tokenization and/or monitoring.

[4] Massachusetts Institute of Technology (MIT), USA, *http://web.mit.edu/kerberos/*. Kerberos, originally developed for MIT's Project Athena, is a widely adopted network authentication protocol. It is designed to provide strong authentication for client-server applications by using secret-key cryptography.

[5] PCI Security Standards Council, *www.pcisecuritystandards.org*. PCI DSS provides guidance and regulates the protection of payment card data, including the primary account number (PAN), names, personal identification number (PIN) and other components involved in payment card processing.

[6] US Department of Health and Human Services, *www.hhs.gov/ocr/privacy*. HIPAA Security Rule specifies a series of administrative, physical and technical safeguards for covered entities and their business associates to use to ensure the confidentiality, integrity and availability of electronic protected health information.

[7] Dynamically masked values are often independently shuffled, which can dramatically decrease the utility of the data in relationship analytics, as the reference fields no longer line up. In addition, values may end up cross-matching or false matching, if they are truncated or partially replaced with nonrandom data (such as hashes). The issue lies in the fact that masked values are not usually generated dynamically, but referenced dynamically, as a separate masked subset of the original data.

Data Owners' Responsibilities When Migrating to the Cloud

Ed Gelbstein, Ph.D., has worked in IT for more than 40 years and is the former director of the United Nations (UN) International Computing Centre. Since leaving the UN, Gelbstein has been an advisor on IT matters to the UN Board of Auditors and the French National Audit Office (Cour des Comptes) and is a faculty member of Webster University (Geneva, Switzerland). He can be contacted at *ed.gelbstein@gmail.com.*

Viktor Polic, Ph.D., CISA, CRISC, CISSP, has been an information and communication technology professional with the United Nations and several specialized agencies since 1993. He is chief of the information security office at the International Labour Organization and an adjunct faculty member at Webster University. He can be contacted at *polic@webster.ch.*

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:

Understanding who owns data is not as simple as it appears at first. It is easy to say that all data belong to the organization. This is correct, but it does not identify accountability for such ownership. The IT function may process data, store data, back data up and perform other services, but it does not own the data. Outsourcing service providers do not own data any more than an internal IT function does.[1]

Data management, data quality and other aspects of data governance tend to get little attention from the IT community, and best practices in these domains rely on the work of other professional bodies such as DAMA International, publishers of the Data Management Body of Knowledge (DMBOK).[2]

The cloud, in its many variants, has the potential to offer many advantages to clients. Senior management is attracted by the possibility of achieving cost reductions and simplifying the enterprise IT environment. Time will tell if these materialize to the expected degree, but it is right to explore the cloud option in detail.

Twenty-five years ago, the client-server architecture seemed to spell the end of the mainframe (it did not). Thin clients did not make it to the market until the emergence of smartphones and tablets that, in turn, brought the challenges of bring your own device (BYOD) and mobile information security risk.[3]

Outsourcing was also expected to deliver significant cost reductions and, in many cases, it did. The main lessons learned from outsourcing were that:

- The contracts are complex and biased toward the provider
- The benefits from well-managed outsourcing extend beyond financials
- It is difficult to separate from an outsourcer

Before discussing the role and responsibilities of data owners, it may be good to recall that there was a form of cloud many years ago: the time-sharing computer bureaus (1950s-70s).[4] These bureaus provided an Infrastructure as a Service (IaaS) capability and sometimes Software as a Service (SaaS), as well.

Only then, things were simpler:

- The number of end users was relatively small (in the 1950s, anyone who could do anything with a computer was considered a mathematical genius).
- The technology was simpler—usually one mainframe, leased lines or dial-up connections (2-4 kilobit per second [Kbps]), and a dumb terminal.
- While initially the computer bureaus handled batch processing, transaction processing became a possibility (which later developed into outsourcing).
- There were no issues of data ownership and the same was true for the location of the data (at the enterprise, at the bureau or in transit).
- Security was not as significant an issue as it is now.
- Vendor lock-in was not an issue—the data were owned by the organization and it could have them processed elsewhere; contracts were simpler, too.
- The applicable jurisdiction was clear. Data rarely crossed borders
- There was little or no legislation on data processing, security or data protection.

DATA OWNERS AND THEIR DATA

The data owner should be a business user who understands the business impact of a security incident resulting in loss of availability, confidentiality or integrity.

This understanding enables the data owner to make informed decisions on the actions to be taken to mitigate the impact of such security incidents, including:

- The definition of data management requirements and the specification and/or acquisition of systems and services (including cloud computing)
- Information classification—together with the definition of criteria and procedures

- Requirements specification of specific data life-cycle activities, such as retention and disposal

There are several ways to approach information classification. A short and well-written guide to such classifications can be found in the freely available US Federal Information Processing Standards Publication (FIPS PUB) 199.

Every information system and its associated databases are supported by a number of data professionals that may include, for example, a data modeller, a data architect, a data steward and a database administrator. One of them should be designated to be the data custodian.

Data owners and data custodians should have a shared view of the appropriateness of the various mitigating actions. These, in turn, should be reviewed with officers responsible for risk and privacy. Consultations may also be appropriate with those working on data management and related business processes.

Data can exist in various states and each state has special requirements to ensure data confidentiality and integrity are not compromised: Data can be at rest (stored) and either unencrypted or encrypted.

Other responsibilities of the data owner include defining the retention period for data (often defined by regulations or laws) and authorizing their disposal and the method through which it will be carried out. The data owner is accountable for ensuring data disposal is carried out according to good practices. The more sensitive the data, the more important this becomes.

Whatever the data being disposed of, organizations must comply with regulatory acts (e.g., US Health Insurance Portability and Accountability Act [HIPAA], US Sarbanes-Oxley Act of 2002, the European Union [EU] Data Protection Directive). Participation of the compliance officer and validation by the internal audit function are also essential.

Granting access and privileges to data, the IT function or service provider may provide and operate an identity and access management (IAM) system, which is essentially an empty box. Data owners are responsible for defining who may access various systems functionalities and datasets and what they can do with the data.

Beyond this, the end user is allowed to perform one or more of the following functions on the data: read only, update, create and delete. Role-based access controls (RBAC) can be used to maintain defined individual roles. Exceptions are managed and access and privileges are terminated when the employee moves to another job or leaves the company. Failure to do this can have serious consequences.

Enjoying this article?

- Read *Security Considerations for Cloud Computing*.

www.isaca.org/cloud-security

- Learn more about, discuss and collaborate on cloud computing and mobile computing in the Knowledge Center.

www.isaca.org/knowledgecenter

Next, come things such as ensuring appropriate data quality; developing, maintaining and enforcing relevant data-related policies; and liaising with other data owners. All of these activities are required regardless of whether the data are processed in-house, by an outsourcing service provider or in the cloud. Having discussed data issues and conducted audits over many years, the authors believe that reality is often different. The main issues encountered include:

- **Unclear ownership**—Usually, the accountabilities of ownership are divided among the many data players mentioned previously without appropriate governance.
- **Unknown data meaning**—This relates to a lack of semantic definitions and incomplete or nonexistent data dictionaries, and carries the risk that data captured for one specific purpose may be used for another unrelated and inappropriate processing when converting data to load into a data warehouse.
- **Inflexible data structures and legacy systems**—These are still around and delivering good service. Some may still use flat files in which records may have variable lengths. These are still in use, primarily for large data transfers.
- **More and more data**—As the cost of storage continues to decrease, it becomes easy to create and store more data. This may also lead to metadata-related risk. For example, data collected from different departments of the same company may be correlated to provide confidential information on individual work assignments, business practices or external partnerships. The risk may also be potentially damaging to corporate identity, as well as individual identities of employees, customers and partners.

- **Large volumes of data**—Volume brings the challenge of scale as this alone ensures that some data will be incomplete or invalid, some will have inconsistencies, and some may be untraceable to their source.
- **Access controls not always being as good as they should be**—People can gradually acquire additional privileges when functional management looks at access control as a chore and simply signs a change control or equivalent document. When computer systems were designed in-house to meet specific business requirements, good programmers created (but did not document) workarounds to allow for bug-fixing, bypassing change controls, or even granting full access and privileges to production data.

> "Scale works against enterprises and the number of privileged users may be greater than anyone would guess."

- **Privileged users**—System administrators, database administrators and network administrators all have privileged access to hardware and software, and they require this to ensure that business needs are met. Others can acquire superuser privileges and keep them when their role (e.g., project manager) comes to an end. In a medium-sized organization, such privileged users are known and trusted, but it is rare to find a documented trail of what privileges they have, when their roles or privileges have last changed, and who approved them. Scale works against enterprises and the number of privileged users may be greater than anyone would guess. In the absence of records, monitoring and reviews, any one of these persons could cause significant damage to data, systems and the business.

MIGRATION TO THE CLOUD FOR DATA OWNERS

Nontechnical matters that must be addressed prior to transferring any data to a cloud service provider include those that have legal and regulatory implications, contractual matters, and domains of risk and uncertainty to recognize and, if appropriate, accept.

Legal and Regulatory

These issues are perhaps the best known and need not be repeated at length here. As legislation continues to develop, from the new version of the EU Data Protection Directive[5] to the US Patriot Act,[6] proper analysis requires the collaboration of, at a minimum, the data owner, the procurement function and legal affairs, and, ideally, someone accountable for data governance and IT governance.

The effectiveness of compliance with such legislation is defined by the fines for failure to comply. If these are small as a percentage of the cloud operators' turnover, this creates little incentive to improve the extent of compliance.

Contractual

As stated earlier, those who have entered into an outsourcing agreement have gained insights into how service providers structure and word these contracts. The providers have signed many such contracts and have access to knowledgeable and experienced legal advice, whereas the entity outsourcing for the first time has much less knowledge of the ins and outs of its procurement and legal services, which may put it at a disadvantage. The same applies to cloud contracts. Such contracts should include the usual service level agreements (SLAs) and guarantees, appropriate penalty clauses, and several other things that may not be necessary in a traditional outsourcing situation, such as:

- Clear and unambiguous definition of data ownership and what this implies in terms of access, copy, distribution, nondisclosure, deletion and destruction, throughout the data life cycle—up to and including exit from the cloud service provider (CSP)
- Data residence details, as well as procedures for data residence changes (server and/or location); contractual measures to ensure traceability of changes
- Classification of security incidents and their associated reporting needs
- Mechanisms for reporting data breaches to the data owner and details of what such reports should contain
- Control requirements, metrics and audits
- Contractual guarantees that data are segregated from the data of other clients
- Description of the exit process, including its associated retrieval of assets and their subsequent usability
- Contractual guarantees that all copies of data made by the virtualization replication process are destroyed upon exit from the contract

From a data owner's perspective, other topics that a well-designed contract should include are:

- Data access by CSP users, including under what circumstances, for what purpose and how this is reported to the data owner (regardless of whether the data are encrypted). A recent article in the *ISACA Journal* highlights new risk associated with limited understanding of the consequences of using encryption.[7]
- Monitoring the activities of CSP privileged users and being notified of personnel changes in these roles

Risk and Uncertainty Domains

It is often said that "prediction is difficult, particularly about the future." Going forward with any initiative or activity involves risk and uncertainties.

Risk is, in principle, measurable and involves making assumptions about threats, vulnerabilities and impacts. In information security, many threats are not random; thus, assumptions become guesses.

In the absence of numbers, practitioners revert to risk matrices with impact on one axis and likelihood on the other, and different colors (e.g., green, yellow and red) indicating degrees of risk. Although subjective, it is better than nothing.

Uncertainty applies not only to the future, but particularly to individual entities. Here statistics are less useful.

At least three driving forces can create risk, uncertainty and even conflict in an organization before migrating to the cloud:

1. **Organizational politics**—This is unrelated to governance and reflects the real organizational distribution of power (the ability to change the *status quo*) and influence (getting others to embrace decisions made by an individual). Politics can make governance ineffective and lead to bad decisions. When this happens, it is usually ego driven (or driven by an expectation of promotion and/or a bonus).
2. **Cost containment**—This is also known as saving money regardless of cost without taking into account unintended consequences and side effects, which are unpredictable at the time of deciding to migrate to the cloud.
3. **Pseudo leadership**—There are many in the IT industry who are more interested in being among the first to have the latest gadget, technology, software or service; or to be listed in some chief information officer (CIO) top 100 listing; or otherwise impress management and peers. Sometimes it works. Often, it ends badly.

Among the domains that could cause pain after migrating to the cloud are:

- Disputed/disputable definitions of data ownership ending in an expensive and lengthy legal process
- Compliance with cross-border data flow legislation and regulations, which vary from country to country (the EU Data Protection Directive has been implemented into national legislation throughout the EU in different ways), i.e., data may be stored in a compliant domain and processed in a noncompliant one
- Compliance with the Wassenaar Arrangement[8] on cryptography technologies
- Government access to data and seizures of servers
- Use of undeclared subcontractors, e.g., the CSP outsources some of its processes to another company without reporting this to its clients

DATA OWNER CONTROLS

Clearly, the data owner must be satisfied that the contractual relationship with the CSP is supported by appropriate controls that provide evidence that what was supposed to happen did and that the result met the conditions of the contract. The data owner should exercise appropriate diligence in assessing the proposed CSP's history of data breaches and related reports.

However, each control requires independent monitoring, tracking and reporting—all of which requires resources and time and is reflected in the price paid for the service. Too few controls do not provide adequate assurance, and too many controls may reduce the benefits gained from the service.

Data owners and the IT function should agree on the extent of controls to be required and this should match the criticality of the data and services to be provided. Some of these controls may require infrequent reporting, such as certification of compliance to a set of standards or accreditation by an independent body.

Other controls may include regular Statements on Standards for Attestation Engagements (SSAE) 16 (formerly Statement on Auditing Standards [SAS] 70),[9] or the European equivalent International Standard on Assurance Engagements (ISAE) 3402,audit reports carried out on the CSP by an independent and credible third party. For critical applications and data, it may be appropriate to consider having the right to audit the CSP and/or engage ethical hackers to conduct an assessment of their security arrangements. The Cloud Security Alliance (CSA) has launched the Security, Trust & Assurance Registry (STAR), which provides information on security controls and practices of CSPs.[10] This publicly available register can assist data owners in the CSP selection process.

Other suggested controls may include:

- Validation/testing of the exit process by taking selected data back and running it elsewhere

- Frequency, completeness and quality of backups
- Business continuity—demonstrable capacity including significant Internet outages (i.e., if required, involving the presence of a client representative)
- Data disposal processes
- Effectiveness of data isolation mechanisms and procedures
- Actions by CSP privileged users (with or without misuse or abuse)
- Confirmation that there are no data remaining at the CSP after exit

CRYPTOGRAPHY AND ENCRYPTION

Cryptography is a science focusing on secret communications. The security of the system should be ensured by the secret key and not by the secrecy of the algorithm. Therefore, the data owner should own the encryption key. This is important in situations when data custodians offer encryption services to data owners. The benefits of applying encryption to data in the cloud include:

- Simpler data residence issues as the data are readable by only a limited number of parties
- Reduced breach notification requirements
- No or reduced need to shred data at the time of disposal

The disadvantages of encryption are:

- The complexity of key management
- Export restrictions (weapons and dual-use technologies) of some encryption methods.[11] These are described in the Wassenaar Arrangement.

PREPARING FOR DIVORCE

The precautionary principle ("better safe than sorry") should be considered before signing a contract to migrate any applications or data considered to be mission-critical and/or sensitive to the cloud.

Some of the potential triggers that could drive the termination of a contract with a CSP include:

- Failure to comply with legal and regulatory issues
- Failure to meet SLAs and other terms of contract
- Significant audit observations and recommendations
- Data breaches, unauthorized data destruction or modification
- Use of nonapproved privileged users or subcontractors
- Unilateral changes to contract terms and conditions

External unpredictable triggers include:

- The CSP/client relationship turns poor and/or a loss of trust in the CSP develops.
- Other clients leave the CSP and, as a result, the CSP goes out of business.
- The CSP is the target in a mergers and acquisitions initiative. The new company imposes changes to terms and conditions.

PRENUPTIAL PREPARATIONS

The concept of "fail to plan" being equivalent to "plan to fail" applies to migrating data to the cloud. Data owners must give due care and attention to several issues, in particular:

- Prepare, maintain and test disaster recovery, business continuity and crisis management plans to be invoked in the event of a major disruption at the CSP or Internet service provider (ISP). Several major cloud operators suffered unexplained service interruptions in the last couple of years.[12]
- Prepare, maintain and test mechanisms to report data breaches to the appropriate bodies.
- Conduct regular exit simulation tests. These may involve taking a data extract from the CSP and running it in another environment to prove that the data are actually usable elsewhere.
- Develop and maintain a comprehensive exit strategy and associated plans to move the data and data processing to another CSP, an outsourcer or in house.
- Expect, and look for, side effects and unintended consequences of the migration, and be prepared to address them as they arise.

CONCLUSION

The cloud and its associated services represent a major step forward in information processing and promise to deliver many benefits, both operational and financial. Some cloud services, such as Gmail, have been adopted by many—mostly small and medium-sized organizations—and have operated successfully for years.

Like all new developments, the benefits of cloud services have been seen in the context of potential downsides, side effects, unintended consequences and other unknown unknowns. Organizations whose culture and requirements drive them to be early adopters should consider migrating in stages, beginning with noncritical applications or those where a standard package (SaaS) would meet their needs.

Mission-critical applications based on custom code should be carefully reviewed for suitability to migrate to a cloud environment. Migrating noncritical applications should release resources to focus on higher-value IT and data.

Laggards and those who are not convinced of the potential benefits of migrating to the cloud may be missing a valuable opportunity. Unfortunately, there is no right answer to any of these dilemmas.

ENDNOTES

1 This article is intended as a complement to Wlosinski, L.; "IT Security Responsibilities Change When Moving to The Cloud," *ISACA Journal*, vol. 3, 2013, bringing in the role of another major player: the data owner.

2 DAMA International, *The Data Management Body of Knowledge*, 2009

3 Projects/OWASP Mobile Security Project, "Top Ten Mobile Risks," *https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks*

4 IEEE Computer Society, "Compatible Time Sharing System (1961-1973)," 2011, *www.computer.org/portal/web/cshc*

5 European Parliament, Council of the European Union, European Union Data Protection Directive, *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT*

6 Congress, The US Patriot Act, *www.justice.gov/archive/ll/highlights.htm*

7 Ross, Steven J.; "A Tide in the Affairs," *ISACA Journal*, vol. 6, 2013

8 Wassenaar Arrangement, *www.wassenaar.org*

9 SSAE 16, *http://ssae16.com/SSAE16_overview.html*

10 Cloud Security Alliance, CSA Security, Trust & Assurance Registry (STAR), *https://cloudsecurityalliance.org/star/*

11 A useful survey of current legislation on cryptography and encryption is available at *www.cryptolaw.org.*

12 Google, "Today's Outage for Several Google Services," 24 January 2014, *http://googleblog.blogspot.ch/2014/01/todays-outage-for-several-google.html*

2015 ISACA® CONFERENCES

ENHANCE YOUR PROFESSIONAL EDGE AND GROW YOUR PROFESSIONAL NETWORK.

ISACA is dedicated to offering the most dynamic and inclusive conferences to keep you abreast of the latest advances in the IT profession. In addition, not only will you have the opportunity to earn CPE hours, you will also:

- Be provided with tools and resources immediately applicable to your position
- Hear from leading experts on emerging trends
- Network with the world's most-respected IT and IS professionals
- Enhance your knowledge and sharpen your skills

ACCOMPLISH MORE

ISACA®
Trust in, and value from, information systems

Upcoming ISACA conferences include:

› **2015 North America CACS**
16 – 18 March 2015 | Orlando, Florida, USA

› **2015 Asia Pacific CACS**
23 – 24 March 2015 | Hong Kong

› **2015 Governance, Risk, and Control Conference**
(an IIA & ISACA collaboration)
17 – 19 August 2015 | Phoenix, Arizona, USA

› **2015 Latin CACS/ISRM**
Dates to be announced soon | Mexico City, Mexico

› **2015 North America ISRM**
19 – 21 October | Washington D.C., USA

› **2015 EuroCACS/ISRM**
Dates and location coming soon, please visit ***www.isaca.org/conferencesjv-6*** for the most up-to-date information

Learn more at ***www.isaca.org/conferencesjv-6***

Feature

From Here to Maturity—Managing the Information Security Life Cycle

Kerry A. Anderson, CISA, CISM, CGEIT, CRISC, CCSK, CFE, CISSP, CSSLP, ISSAP, ISSMP, is an information security professional with more than 16 years of experience in information security and compliance. She is an adjunct professor of cybersecurity at Clark University (Massachusetts) and the author of numerous articles in professional journals and the book *The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture*. She can be reached at *kerry.ann.anderson@verizon.net*.

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:

All living things have a life cycle, from creation to their eventual conclusion. This is true of microorganisms, animals, individuals and organizations. The life cycle paradigm holds true for teams and the programs they manage, including information security programs, each of which has its own unique life cycle. However, information security programs move through a series of stages that tend to be remarkably alike, with similar milestones and indicators. A number of factors, such as organizational culture, leadership, business sector, competitive environment, external events and regulatory environment, may affect the maturation progress.

During the 1970s, Richard L. Nolan, Ph.D., developed one of the early models for evaluating the maturity of information technology functions: the Stages of Growth Model for IT Systems.[1] While this model has undergone some modifications, it is still in use today. The basis of the Nolan model is a qualitative assessment of maturity. While the Nolan Stages Model was specific to the maturity life cycle of IT organizations as a whole, its structure and stages can be adapted to various technology-related functions performed by the organization. This model can be adapted for information security and enhanced by identifying a set of benchmarks for each of the maturation stages. The information security model, while not scientifically vetted, can help the information security practitioner quickly estimate the maturation stage of an information security program.

WHY THE MATURITY STAGE IS IMPORTANT

Assessing the relative maturation stage of an information security program is important to determining if a security technology or best practice is appropriate for implementation. Information security programs at lower maturity levels may find it difficult to deploy or integrate complex technologies and operational practices. Maturation cannot be rushed. Just as with people, information security programs progress along the maturation life cycle at their own unique pace.

An information security program's maturity stage must be factored into all planning regarding people, process and technology. If a disparity occurs in the alignment of these elements and the information security program's maturity, the security posture may be less effective in fulfilling its objectives or fail to reap the benefits of its security investments. This situation may occur when a security executive from a highly mature information security program takes over a less mature program and tries to force the practices of his/her prior program into the new environment.

ORGANIZATIONAL MATURITY VS. INFORMATION SECURITY PROGRAM MATURITY

It is possible for no correlation to exist between the overall maturity of the organization and its information security program. For example, an Internet service company might be very mature in terms of its business model, financial operations and technology infrastructure. However, it may not have formally addressed information security to any extent beyond basic technical security functions, such as firewall administration. A good example is high-tech start-up companies. These companies may achieve maturity in the majority of their operational functions, but fail to establish a formal information security program. Initially, these companies may have limited assets and little to lose, so they can be cavalier in their approach to information security risk. However, as these companies grow and become successful, the financial and reputational risk associated with an information security incident increases.

Experiencing a security incident can also stimulate the creation of an information security program. A good example of this situation is LinkedIn. LinkedIn, which initially had no chief information security officer (CISO),[2, 3] is a successful social networking web site with more than 150 million users. In 2012, LinkedIn confirmed that a network breach had exposed hashed passwords associated with nearly 6.5 million accounts.[4] This situation is not limited to

Internet companies either. Both Sony and Target corporations experienced significant data breaches, and it was reported that neither corporation had designated a CISO role to drive their respective information security programs.[5, 6]

WHAT STIMULATES MATURITY PROGRESS

While it is possible for momentum for information security program progression to emanate from within an organization, such as from the hiring of strong, experienced leadership, more often it results from an external stimulus, such as:

- **Technological change**—According to Ray Kurzweil's *The Law of Accelerating Returns*, this century will see almost a thousand times greater technological change than in the prior century.[7] This means information security programs must develop the maturity to respond to even greater challenges in managing risk. Many technologies with risk factors that are being managed today (e.g., cloud computing and smartphones) did not even exist a decade ago. Many established best practices might become obsolete because technology or other innovations may create new best practices to replace existing ones. A good example is bring your own device (BYOD). Just a few years ago, it was considered best practice for organizations to supply and control phones and other mobile devices used for business activities. The IT consumerism trend, as well as economic benefits, has replaced this accepted practice with BYOD and spurred the creation of technology solutions to secure business communications on a personally owned device. Technology drives information security programs to evolve and mature to meet the challenges created by innovation.

> "Knee-jerk responses to compliance requirements may fail to yield a mature, holistic approach toward information security."

- **New regulatory requirements**—In addition to technology, the regulatory environment has continued to expand with, for example, the Payment Card Industry Data Security Standard (PCI DSS) and the US Health Insurance Portability and Accountability Act (HIPAA). Many organizations do not create a separate information security program until an external impetus forces them to do so. However, these knee-jerk responses to compliance requirements may fail to yield a mature, holistic approach toward information security. The newly minted program often thrashes around, attempting to meet security challenges and expectations with limited experience and undeveloped processes, while its executives may perceive the information security program as exhibiting a significantly higher maturity level. One reason this occurs is due to confusion between the usages of security technology and the maturity of the information security program. One defining symptom of the first stage of an information security program's maturity is the silver bullet[8] syndrome, in which the answer to all problems is the acquisition of technology. However, an information security program at lower maturity levels may lack the required expertise to implement the technology to optimize its full benefits. Without appropriate leadership and executive support, the resulting information security program may remain in an early compliance-centric state.
- **Significant external cybersecurity events**—Major external security events often fuel increases in maturity because they put security into the spotlight and get the attention of executives. This can fuel the maturity of information security programs by increasing executive support and budgets to fund security initiatives. Over the last decade, some cybersecurity-related incidents that have driven new investment in information security programs include:
  - Major breaches (e.g., those against TJX, Sony and Target)
  - Insider incidents, such as the information leaked by Edward Snowden
  - Corporate espionage
  - Malware

Enjoying this article?

- Read *Transforming Cybersecurity*.
  www.isaca.org/cybersecurity-cobit
- Discuss and collaborate on information security management in the Knowledge Center.
  www.isaca.org/topic-information-security-management

THE NOLAN STAGES MODEL AND OTHER MATURITY MODELS

An information security program represents the sum of all information security processes, technology, policies, governance, business alignments, awareness activities and other elements necessary to effectively manage the organization's security posture. "The Golden Triangle" of people, process and technology composes an information security program.

Many existing information security models have their roots in the Capability Maturity Model (CMM), which is based on a process model. The Software Engineering Institute (SEI) at Carnegie Mellon University (Pittsburgh, Pennsylvania, USA) developed the CMM in the mid-1980s. Process models use a structured collection of practices that describe the characteristics of effective processes against five maturity levels, with a focus on standardization. The CMM model has been applied to software/system engineering, systems, project management, risk management and information technology (IT) services. CMM has its primary focus on the process dimension rather than the two other attributes—people and technology. However, it is the human dimension that acts as a catalyst for transformation and growth required to move the maturity continuum.

Another approach, such as the one used by Security Innovation's Corporate InfoSec Maturity Path, looks at information security maturity as a grid with two axes, with people and process on the x-axis and tools and technology on the y-axis.[9] A point on the grid represents the information security's maturity and path toward security. This approach does offer a way to gauge maturity progress and does take into consideration people, process and technology. However, it lacks precision and exact stages in assessing the maturity of the information security program.

After reviewing the various approaches available for assessing an information security program's maturity, the Nolan Stages Model was adopted. Richard Nolan's Stages Model is the best-known and most widely cited model of computing evolution in organizations and the concepts it introduced influenced subsequent maturity models. Nolan proposed stage benchmarks that management can use to gauge where an IT-related function currently stands and what developments lay ahead of it in its maturity journey. The Nolan Stages Model is unique in both its simplicity and adaptability, and continues to be used by many organizations.[10] The Nolan Stages Model was selected for the following reasons:

- It was originally designed to assess information technology, so it is easily adapted for another function that has a program focus around the use of people, process and technology.
- It is easy to understand and explain to management.
- An experienced practitioner can use the model to evaluate maturity based upon interviews with key personnel and stakeholders, as well as with personal observations.
- It provides a qualitative measure of maturity.
- The original model[11] used four stages, and later expanded to six, including a data administration stage. The data administration stage is particularly relevant to information security that focuses on data as a critical asset and their protection.
- These Nolan stages discuss budget as an indicator of penetration and use within an organization. Few models discuss the budgeting aspect of a program or function despite its criticality in growing and supporting program activities.

USING BENCHMARKS TO DETERMINE THE INFORMATION SECURITY PROGRAM'S MATURITY STAGE

It is possible to perform an *ad hoc* assessment of information security maturity by using benchmarks that are indicative of an information security program's development. The following are benchmarks of development:

- Planning duration (short- and long-term planning)
- Focus and activities (internal, external or both)
- Policies
- Security awareness
- Budgeting
- Primary concerns
- Business alignment
- Prerequisites to move to next stage of development

No single benchmark is indicative of the information security program's overall maturity. However, the benchmarks, when considered together, can yield an excellent approximation of where an information security program exists on the maturity life cycle continuum.

THE SIX STEPS OF INFORMATION SECURITY MATURATION

This adaptation of the Nolan model for information security organizations uses a six-step maturity paradigm.[12] The model can be envisaged as a flight of stairs that the information security program must climb to increase its effectiveness. Like stairs, an information security team can ascend or descend based upon the actions and attitudes of the information security program.

Step 1: Initiation

This step denotes the formal creation of an information security program by the organization as the result of an executive-level decision. This decision can be driven by either internal requirements or external influences, such as new compliance regulations or a security breach. The first visible evidence of the newly minted information security program is the creation of a formal high-level information security policy, which offers proof of executive management support. Former security administrators or other technical staff with limited formal training or expertise in the information security discipline may staff the team. The defining characteristic of this stage is the rapid acquisition of security technology with limited formal processes around their use (**figure 1**).

Figure 1—Traits Associated With the Initiation Stage

Benchmark	Traits
Planning duration	• Short-term in duration (under six months)
Focus and activities	• Purely reactive (always in fire-fighting mode)
Policies	• First formal high-level policies issued by executive management • May be driven by compliance requirements • May be created from templates or copied from external resources
Security awareness	• Compliance mandated training sessions
Budgeting	• Usually a part of the IT budget
Primary concerns and prerequisites to progress	• Recruiting experienced staff • *Ad hoc* processes • Implementing technology with limited efforts in developing supportive and repeatable processes
Business alignment	• Limited
Prerequisites to move to next stage of development	• Recruitment of strong and experienced leadership • Recruitment of a few key experienced staff members to put repeatable processes in place and mentor others • Inclusion of metrics

Step 2: Contagion

During the contagion step, the silver bullet syndrome may continue with regular acquisition and replacement of security technologies. This approach may obscure the need to integrate people and process to optimize technology investments. Information security staff members still often find themselves fighting fires rather than establishing repeatable and automated processes. The information security policy often needs enhancement beyond a basic policy to include standards, guidelines and procedures. This expansion may involve inclusion of a standardized exception process to manage issues of noncompliance. Primitive metrics and logging may be introduced in an effort to identify risk trends, monitor user behaviors and create baselines for comparisons (**figure 2**).

Figure 2—Traits Associated With the Contagion Stage

Benchmark	Traits
Planning duration	• Short-term in duration (under 12 months)
Focus and activities	• Primarily reactive and technically focused • First serious efforts at consistent monitoring of data
Policies	• Expansion to include standards, guidelines and procedures • Introduction of exception process
Security awareness	• Increasing focus on awareness efforts vs. simple compliance-mandated training classes
Budgeting	• Budget may remain a component of another budget, rather than a separate budget to support information security operations
Primary concerns	• Recruiting and retaining experienced staff • Still dependent upon a few key individuals (sole living experts) • Limited use of automation and formalized processes
Business alignment	• Limited unless tied to a security-related project
Prerequisites to move to next stage	• Strong leader with experience developing information security function • Additional recruitment of a few key practitioners to expand skills portfolio • Focus on training to develop less-experienced staff • Process documentation

Step 3: Control

The control step represents a critical juncture in maturity development. It may represent a shift from a compliance-centric view of the information security program to a risk-based paradigm. The information security program begins to address specific gaps based on a formal assessment process. Policy development becomes increasingly formalized to include a governance model that extends across the organization. Potential security solutions are evaluated against a specific set of criteria based upon their capabilities to resolve identified risk, potential for return on investment (ROI) and compatibility with the organization's strategic direction.

As the information security program expands, there is increasing specialization of job functions. Senior staff may assume informal leadership roles. A job ladder that offers career growth for technically focused positions may increase employee retention rates. A distinguishing sign of the control stage is the establishment of repeatable and automated processes (**figure 3**).

Figure 3—Traits Associated With the Control Stage

Benchmark	Traits
Planning duration	• Combination of short-term and long-term planning activities
Focus and activities	• More proactive based upon identified risk factors
Policies	• Introduction of formal governance model • Policies documents undergo regular reviews and revisions
Security awareness	• Increasing focus on awareness efforts vs. compliance-mandated training classes
Budgeting	• Budget may remain component of another budget, but may contain separate line items for projects
Primary concerns	• Retaining experienced staff • Expanding security service offerings • Increasing automation and formalized processes
Business alignment	• Limited beyond security-related projects or specific requests from business for participation in projects
Prerequisites to move to next stage	• Continued strong leadership with focus on evolving the information security function • Continuing training to maintain staff skills • Move toward program focus rather than project-centric efforts • Adoption of a defined risk framework • Use of formal metrics scorecard or dashboard to track progress

Step 4: Integration

During the integration stage, the information security program moves away from a more isolated existence and its activities merge seamlessly into business processes. Some staff assumes the role of liaisons across the various business areas. The net effect is the embedding of security across the organization. Solution acquisition becomes more deliberate and needs to be justified based upon cost-benefit analysis. The information security program's staff assumes a proactive attitude by looking for possible ways to add value to business functions, such as by participating in meetings with prospects and discussing security aspects of the products and services offered by the organization.

As the information security program matures, it seeks external influences to drive its maturity by interacting with others to gain exposure to new ideas, paradigms and knowledge. The program's staff builds upon existing external relationships, such as peer organizations and industry groups (**figure 4**).

Figure 4—Traits Associated With the Integration Stage

Benchmark	Traits
Planning duration	• Shortest planning cycle is one year with primarily three- to five-year planning intervals
Focus and activities	• Primarily reactive with some proactive activities
Policies	• Evolving policy management and governance process
Security awareness	• Targeted awareness activities based on identified knowledge and behavioral gaps
Budgeting	• Funding for core operational costs and planned capital budgeting with greater autonomy in spending decisions • Use of multiyear budgets for a few major projects
Primary concerns	• Retaining experienced staff • Expanding security service offerings • Increasing automation and formalized processes • Integrated security embedded
Business alignment	• Moderated with information security liaisons on key projects or enterprise committees
Prerequisites to move to next stage	• Leader seeks alignment with peers in other business areas • Building strong core teams and subgroups within those teams • Defined career paths • Continuing training to maintain skills • Formalized security metrics program

Step 5: Data Administration

During this stage, the information security program moves toward a strategic concentration on protecting its most critical assets: its data. This stage is defined by the adoption of a data-centric strategy with an objective of protecting data's value over their life cycle. The information security program needs to ensure that data receive suitable protection from external and internal threats. A data-centric approach offers the opportunity to achieve a market advantage by using the organization's valuable data, such as big data strategies, while still protecting these critical assets. This can result in the adoption of a formalized data classification model and tools to enforce it. In addition to managing the security concerns of data housed internally, a data-centric protection strategy looks to control risk around sensitive information shared with external parties, such as business partners and vendors. Data-centric security teams need to coordinate closely with internal functions, such as legal, procurement and IT, to ensure that sensitive data stored outside the organizational security perimeter are secured appropriately during their entire life cycle (**figure 5**).

Step 6: Continuous Renewal

Only a fraction of all information security programs make it to this stage. Continuous renewal is analogous to the Japanese *Kaizen*.[13] The origins of Kaizen began during the post World War II efforts at rebuilding Japanese industry based upon the statistical control methods of W. Edwards Deming. The Economic and Scientific Section (ESS) group was tasked with developing Japanese management skills and created a training film titled *Improvement in Four Steps (Kaizen eno Yon Dankai)*. Thus, the concept of Kaizen was introduced to Japan.[14] Kaizen is the Japanese term for continual improvement.

Achieving this stage is not the end of the road, but signifies a new maintenance phase requiring vigilance in sustaining all the people, processes and technologies, and continuing to manage emerging risk. The overall information security program has assumed proactive posture with an emphasis on forecasting nascent security threats and technologies, such as looking at regulatory or technical innovations that potentially may include a need for security. The program's staff is comfortable reviewing the current state of information security, in terms of its existing controls, level of performance and opportunities for improvement. The information security program uses key metrics to track its effectiveness. The CISO utilizes financial justification for the program's expenditures and its contributions to business activities, especially in relation to revenue creation. A compliance culture is the reward at the end of the maturation journey for the information security program (**figure 6**).

Figure 5—Traits Associated With the Data Administration Stage

Benchmark	Traits
Planning duration	• Shortest planning cycle is one year with primarily three- to five-year planning intervals
Focus and activities	• Balanced internal and external risk focus
Policies	• Creates a need for a rigorous access control policy and access audits to monitor high-risk profiles to enforce least privilege and prevent users from gaining risky combinations of access rights
Security awareness	• Security awareness expands to offer targeted training for different categories of employees, such as social engineering awareness for staff that often deal with external parties • Training may be integrated into the corporate training rather than isolated training events
Budgeting	• Annual budgeting to fund operational costs and planned capital budgeting, as well as budget planning cycle for multiyear programs for strategic initiatives
Primary concerns	• Retaining experienced staff • Embedding data protection into all processes • Increasing automation and formalized processes • Integrated security embedded into business processes
Business alignment	• Increasing integration with business functions, projects and strategies • Information security team members serve on most committees and project teams • Information security viewed as a strategic advantage by organizational executives
Prerequisites to move to next stage	• Succession planning for leaders and key staff • Building "bench strength" into all functions • Continuing training to maintain skills • Integration of information security metrics with other organization metrics • Full budgeting autonomy, if not already achieved

TIPS FOR MANAGING THE INFORMATION SECURITY MATURATION PROCESS

No information security program can stay static when managing a dynamic and challenging threat environment such as the one currently confronting organizations. Not every information security team needs to achieve the highest maturation stage. However, it needs to achieve an appropriate level of maturity to support the needs of the organization it serves. It then needs to maintain that level of maturity through continuing efforts. In general, this does not occur organically, but requires a plan and concerted effort. The following is advice on how to grow and sustain the maturity development process:

1. Remember that the appropriate destination stage for an information security program's maturity is dependent on the organization, its threat landscape, risk tolerance and business segment.
2. Be realistic in determining the existing state of the information security program on the maturation continuum.
3. Identify key benchmarks to assess the information security program's development toward higher maturity stages.
4. Have a plan B[16] in reserve to fall back on if unanticipated internal and external events occur.
5. Be prepared for setbacks. They are normal. It is the team's reaction to them that makes the difference.
6. Remember even when an information security program achieves the Kaizen stage, the program needs to continue to evolve or risk descending the maturity ladder to a lower stage.

MOVING UP THE MATURITY LADDER

Sometimes information can straddle two maturity stages, e.g., exhibiting traits of a higher step in one aspect of its functioning, such as budgeting, but still presenting primarily the characteristics of a lower state of maturity. This situation, which is both possible and common, may occur because a member of the staff with experience in a specific area drives the program to achieve a higher maturity in this function. For example, a project manager with extensive financial skills might advance budgeting procedures. In these situations, the assessment of the maturity stage should reflect the preponderance of the traits exhibited by the information security program.

Assessing and managing an information security program's maturity stage offers a number of benefits. A primary advantage is that it can help information security professionals develop a strategic approach to move the program along the maturity ladder. This can be especially true as the information security program reaches the midpoint of the maturity continuum and appears to plateau. Plateaus can result in two possible outcomes. Like a flight of stairs, the information

Figure 6—Traits Associated With the Continuous Renewal Stage

Benchmark	Traits
Planning duration	• Mix of short- and long-term planning (three to five years) • Strategic projects with duration beyond five years
Focus and activities	• Balanced internal and external risk focus • Primarily proactive activities • Reactive as required for incident management, but based upon prior planning activities
Policies	• Regular review, revision and extension of policy hierarchy
Security awareness	• Awareness moves from simple awareness messages toward promoting a culture of compliance • Awareness focused on effectively managing the "people perimeter,"[15] in which people have become the new security perimeter where decisions by individuals can create significant impacts
Budgeting	• Strategic budget management based upon multiyear projects, programs and core services • Use of a revenue-driven model for providing specific services
Primary concerns	• Adding value to new business functions, programs and projects • Retaining experienced staff • Forecasting emerging risk and opportunities • Using formalized automation • Balancing cost and risk
Business alignment	• Embedded within business strategy • Becomes integral component of all business functions, programs and projects • CISO or equivalent position attends board of directors meeting ("seat at the table")
Prerequisites to move to next stage	• Maintaining continuous improvements culture through: – Succession planning for leaders and key staff – Continuous training to maintain skills – Identification of new value opportunities within organization – A compliance culture that requires regular maintenance and continuing support at the highest level of the organization to thrive and mature

security program can move in either direction, up or down. By actively monitoring and managing the maturation of the program, it may be possible to identify factors hindering its progression to the next stage and remove obstacles to accelerate movement toward the journey to maturity. In addition, it may be possible to expedite progress up the maturity ladder by using specific tools, such as effective leadership, generous resource availability and executive support. Forward movement requires senior management support because an effective information security program requires top-down support.

ENDNOTES

[1] Nolan, Richard L., "Managing the Crises in Data Processing," *Harvard Business Review*, March 1979, *http://hbr.org/1979/03/managing-the-crises-in-data-processing/ar/1*

[2] CISO Platform, "5 Lessons from the LinkedIn Breach," 29 June 2012, *www.cisoplatform.com/profiles/blogs/5-lessons-from-the-linkedin-breach*

[3] Chabrow, Eric; "LinkedIn Has Neither CIO nor CISO: Failing to Learn Lessons from the RSA, Sony Breaches," The Public Eye, *Bank Info Security*, 8 June 2012, *www.bankinfosecurity.com/blogs/linkedin-has-neither-cio-nor-ciso-p-1289*

[4] Kitten, Tracy; "LinkedIn: Hashed Passwords Breached," *InfoRisk Today*, 6 June 2012, *www.inforisktoday.com/linkedin-hashed-passwords-breached-a-4837?webSyncID=665c8703-e514-40d4-acd9-0bcaab3d3208&sessionGUID=2902c381-3da0-b37d-7348-a49dd009a011*

[5] Chabrow, Eric; "Breach Gets Sony to Create CISO Post," *Bank Info Security*, 2 May 2011, *www.bankinfosecurity.com/breach-gets-sony-to-create-ciso-post-a-3599*

[6] Donovan, Fred; "Target Did Not Have CISO to Oversee Information Security Prior to Massive Breach," *Fierce IT Security*, 10 March 2014, *www.fierceitsecurity.com/story/target-did-not-have-ciso-oversee-information-security-prior-massive-breach/2014-03-10#ixzz32XoVSTKS*

[7] Kurzweil, Ray; *The Law of Accelerating Returns*, *www.kurzweilai.net/the-law-of-accelerating-returns*

[8] Merriam-Webster, "Silver Bullet or Magic Bullet," *www.merriam-webster.com/dictionary/silver%20bullet*

[9] Security Innovation, an information security consulting firm, developed the Corporate InfoSec Maturity Path, using this approach.

[10] Hollyhead, Andy; Alan Robson; "A Little Bit of History Repeating Itself—Nolan's Stages Theory and the Modern IS Auditor," *ISACA Journal*, vol. 5, 2012, *www.isaca.org/journal*

[11] Damsgaard, Jan; Rens Scheepers; *A Stage Model of Intranet Technology Implementation and Management*, *www.researchgate.net/publication/221409245_A_Stage_Model_of_Intranet_Technology._Implementation_and_Management/file/50463515458b50827a.pdf*

[12] Anderson, Kerry; "The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture," CRC Press, May 2014

[13] Stephenson, Steve; "What Is Kaizen Tutorial?," Graphic Products, *www.graphicproducts.com/tutorials/kaizen/*

[14] Maurer, Robert; *The Spirit of Kaizen: Creating Lasting Excellence One Small Step at a Time, 1st Edition*, McGraw-Hill, 2012

[15] The Intel Corporation introduced the concept of the "people perimeter" in the late 2000s to stress the criticality of individuals' actions on the security of the enterprise. See Jackson, Brian; "'People Are the New Perimeter' Says Intel," 2008, *www.itbusiness.ca/news/people-are-the-new-perimeter-says-intel/12443*

[16] Alternate strategy for accomplishing a function when the primary way of doing something is not available. Cambridge Dictionaries Online, "Plan B," *http://dictionary.cambridge.org/us/dictionary/business-english/plan-b*

Auditing Oracle Database

Muhammad Mushfiqur Rahman, CISA, CCNA, CEH, ITIL V3, MCITP, MCP, MCSE, MCTS, OCP, SCSA, has 11 years of IT operations, project management and custom business solutions, enterprise resource planning implementation, and information security management experience. Rahman is manager, information systems security at the Premier Bank Limited, Bangladesh. He also has 10 years of experience teaching different IT courses for end users and IT professionals. He can be reached at *mushfique98@gmail.com.*

Database auditing is the activity of monitoring and recording configured database actions from database users and nondatabase users, to ensure the security of the databases.

An administrator can perform auditing on individual actions, such as the type of Structured Query Language (SQL) statement executed, or on combinations of data that can include the user name, application or time stamp, for example. Auditors need to audit for both successful and failed activities, and include or exclude specific users from the audit:

> *Proper auditing of a database will ensure the safeguarding of the database, which means that the database and its features' installation, default account, patches, services, password policy, account lockout policy and audit policy have proven auditing to be a continuous process.*[1]

The major types of risk activities include:

- **Mistake:** Failure to maintain or operate the database as required leads to accidental disclosure of information, and unauthorized changes lead to unauthorized and accidental disclosures, inserts, updates or deletions.
- **Misuse:** Failure to maintain access rights to the database leads to abuse of privileged access and leakage of information.
- **Malicious action:** Failure to maintain a secure, logical setup of the database leads to data theft or a denial-of-service (DoS) attack.

COMMON VULNERABILITIES FOUND IN DATABASE ATTACKS

Many attacks begin with social engineering:

- **Phishing** is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails in an attempt to gather personal and financial information from recipients. Typically, the messages appear to come from well-known and trustworthy web sites. Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo and Best Buy, for example.
- **SQL injection** is a technique used to take advantage of nonvalidated input vulnerabilities to pass SQL commands through a web application for execution by a back-end database. Attackers take advantage of the fact that programmers often chain together SQL commands with user-provided parameters and, therefore, can embed SQL commands inside these parameters. The result is that the attacker can execute arbitrary SQL queries and/or commands on the back-end database server through the web application.
- **Data exfiltration** is the unauthorized copying, transfer or retrieval of data from a computer or server. Data exfiltration is a malicious activity performed through various techniques, typically by cybercriminals over the Internet or other network. Data exfiltration is also known as data extrusion, data exportation or data theft.
- **Staging server** is a server that enables assembling, deploying and testing a software or web site on a server instance, similar to the production server. Typically, software or a web site is deployed on the staging server from the development server when development is complete. A staging server helps to identify the software or web site behavior, experience and performance as it will be visible on the production server. This helps software developers or quality assurance (QA) staff identify and resolve any problems, bugs, performance or usability issues, or other issues before the software or web site is deployed on the production server. The staging server can be a staging database server, staging web site server or staging application server, for example.

Analyzing database configuration is critical to determine vulnerabilities and assure the standard auditing. Database auditing includes:

1. Finding sensitive data and privileges
2. Preventing data access
3. Validating that detection and alert mechanisms are in place

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:

There are multiple mechanisms available that must be in place when databases are configured, including:

- **Data redaction** provides selective, on-the-fly redaction of sensitive data in SQL query results, prior to application display, so that unauthorized users cannot view the sensitive data. It enables consistent redaction of database columns across application modules accessing the same database information. Data redaction minimizes changes to applications because it does not alter actual data in internal database buffers, caches or storage, and it preserves the original data type and formatting when transformed data are returned to the application. Data redaction has no impact on database operational activities, such as backup and restore, upgrade, and patch, and on high-availability clusters.
- **Data masking** obfuscates sensitive data by replacing them with other data—typically characters that will meet the requirements of a system designed to test or still work with the masked results. Masking ensures that vital parts of personally identifiable information (PII), such as the first five digits of a social security number, are obscured or otherwise deidentified.
- **Data encryption** involves converting and transforming data into scrambled, often unreadable, ciphertext using nonreadable mathematical calculations and algorithms. Restoring the message requires a corresponding decryption algorithm and the original encryption key.

DATABASE AUDITING STEPS

The following steps need to be followed for database auditing.

Step 1: Determine if Default Accounts Have Been Changed or Disabled

Default privileged Oracle accounts continue to be the highest risk issue commonly encountered. It is an easy issue to fix and prevent. After installation, Oracle has a number of default accounts, each with a default preset value. Following database install, the Oracle database configuration assistant (DBCA) automatically locks and expires the majority of the default database user accounts. Additionally, DBCA changes the SYSTEM account to the value specified during the installation routine.

If an Oracle database is manually installed, the DBCA never executes, and those dangerous default privileged accounts are never locked and expired. By default, their password is the same as their username. These will be the first credentials that a hacker will attempt to use to connect to the database. As a best practice, each of these accounts should be configured with a strong unique password, and if an account is not required, it should be locked and expired.

To change the password, the following SQL code should be executed:

```
sqlplus> connect mydba
sqlplus> alter user SYSTEM account lock and expire
```

The following SQL can be used to lock and expire those default accounts:

```
sqlplus> connect mydba
sqlplus> alter user SYSTEM account lock and expire
```

The default accounts installed with Oracle vary by version. **Figure 1** provides a quick reference of the accounts that are installed by default (if the DBCA is never executed) in Oracle 9, 10 and 11 in an open state.

Figure 1—Oracle Default Accounts

Oracle 9i	Oracle 10g 2	Oracle 11g
SYSTEM	SYSTEM	SYSTEM
SYS	SYS	SYS
SCOTT		SYSMAN
DBSNMP		MGMT_VIEW
		DBSNMP

Source: Muhammad Mushfiqur Rahman. Reprinted with permission.

Starting with Oracle version 11g, database administrators (DBAs) can easily locate any accounts with default passwords (same as username) by using the database view DBA_USERS_WITH_DEF_PWD.

Step 2: Audit the Strength of Oracle Database SID

The Oracle system ID (SID) is a unique value that is required for all clients to connect to the Oracle database. Because it must be unique, there cannot be more than one database with the same SID on the same Oracle server.

If a client connection uses an incorrect SID to connect to an Oracle database, it will get the message "ORA-12505: TNS:listener does not currently know of SID given in connect descriptor." However, SIDs can be brute forced. There are numerous tools to brute force the Oracle SID, including

Metasploit modules, operational acceptance testing (OAT) and SIDGuess.

The key to thwarting SID brute-force attacks is to select a SID that is strong. When creating an Oracle SID, the selection should:

- Not be a dictionary word
- Be at least 10 characters in length
- Include at least one special character

Incorporating these elements ensures that the SID is strong, i.e., difficult for an attacker to brute force.

Why does a strong SID matter when the SID is stored as a cleartext value within the Oracle client configuration file, TNSNAME.ora, on every single system that is configured to connect to the database? It matters because as long as an attacker can compromise at least one system that is configured to connect to the Oracle database, obtaining the SID from the TNSNAMES.ORA file is trivial. However, it is important to consider instances where the attacker is external to the organization and has compromised a single host that does not have an Oracle client connection configured. A strong SID will not in and of itself prevent hackers from gaining a connection to an organization's Oracle database, but it is a good practice as part of a defense-in-depth approach to security.

Step 3: Audit the Oracle Critical Patch Updates

This is one of those security best practice recommendations with which most organizations commonly struggle. Depending on the database schema, Oracle critical patch updates (CPUs) can have significant impact on the Oracle database—significant enough that the organization might have to perform extensive regression testing to ensure that applying the latest Oracle CPUs has no impact on database functionality.

Oracle releases CPUs quarterly on the Tuesday closest to the 17th day of the month. Oracle has a special bulletin page that describes all of the most recent Oracle Critical Patch Updates and Advisories.[2] Fortunately, CPUs are cumulative in nature. One can simply install the latest Oracle CPU to gain all of the security patches since the product's initial release.

The key to an effective CPU patch process is creating a regimented regression testing process that corresponds to Oracle's four scheduled releases every year. Even in organizations with the most stringent regression testing processes, the CPUs can usually be architected in such a manner that they can be applied no more than three months after the last CPU release. Additionally, all DBAs should register with the Oracle email Security Alert Advisory Service[3] to ensure timely notification of Oracle patches and security alerts.

There is also a mechanism that Oracle employs if a critical vulnerability is discovered that warrants immediate patch release. Oracle refers to patches released immediately under this program as "off-schedule security alerts." Since the CPU program began in 2005, there have only been a few times when Oracle released patches under this emergency process. Organizations should develop a method for applying these emergency released patches, but given their historic low volume, the focus should be on the routine applying of CPU patches every quarter.[4]

Step 4: Audit PUBLIC Role for Identification of Unncecessary Privileges

In Oracle, extended routines exist that allow minimally privileged users to execute functions that they otherwise would not be able to execute. These extended routines are called packages, and are roughly equivalent to Extended Stored Procedures in Microsoft SQL Server. A special role, called PUBLIC, acts as a default role assigned to every user in the Oracle database. Any database user can execute privileges that are granted to PUBLIC. This is commonly exploited for database privilege escalation.

These packages and subtypes should be revoked from PUBLIC and made executable for an application only when absolutely necessary.

Step 5: Check That Database Auditing Is Enabled

To identify the malicious or authorized activities in a database, it is important to check that database auditing options are enabled. To ensure that database auditing is enabled, one needs to perform the following activities during the database audit:

- **Audit SYS operations**—By default, Oracle databases do not audit SQL commands executed by the privileged SYS and users connecting with SYSDBA or SYSOPER privileges. If a database is hacked, these privileges are going to be the hacker's first target. Fortunately, auditing SQL commands of these privileged users is very simple: sqlplus> alter system set audit_sys_operations=true scope=spfile.
- **Enable database auditing**—Again, by default, Oracle auditing of SQL commands is not enabled. Auditing should be turned on for all SQL commands. Database auditing is

turned on with the audit_trail parameter: sqlplus> alter system set audit_trail=DB, EXTENDED scope=spfile. (Note: The command enables auditing from the database, but not the database vault information, into the table SYS. AUD$.) There are actually four database auditing types: OS, DB, EXTENDED and XML.

- **Enable auditing on important database objects**—Once auditing has been enabled, it can be turned on for objects where an audit trail is important.

Step 6: Audit to Ensure That Database Triggers for Schema Auditing and Logon/Logoff Events Are Configured

To effectively audit schema changes and logon and logoff events, Oracle provides Data Definition Language (DDL) triggers to audit all schema changes and can report the exact change, when it was made, and by which user.

- **Logon trigger**—By using a logon trigger, one can send logon and logoff events in real time to another system. Think of it as a syslog daemon for your database events. The following example would send all logon and logoff events to a web server in real-time.

  SQL> create or replace trigger sec_logon after logon on database.

- **DDL trigger**—Using the DDL triggers, an Oracle DBA can automatically track all changes to the database, including changes to tables, indexes and constraints. The data from this trigger are especially useful for change control for the Oracle DBA. The following example sends events for GRANT, ALTER, CREATE, DROP.

  Command (as user SYS):

```
SQL> create or replace trigger DDLTrigger
AFTER DDL ON DATABASE
DECLARE
rc VARCHAR(4096);
BEGIN
begin
rc:=utl_http.request('http://192.168.2.201/user='||ora_
login_user||';
DDL_TYPE='||ora_sysevent||';DDL_OWNER='||ora_dict_
obj_owner||';DDL_NA
ME='||ora_dict_obj_name||';sysdate='||to_char(sysdate,
'YYYY-MM-DD
hh24:mi:ss');
exception
when utl_http.REQUEST_FAILED then null; end;
END;
/
```

- **Error trigger**—Error triggers are Oracle error messages. They can be useful for detecting attacks from SQL injection and other attack methods.

  For example, command (as user SYS):

```
SQL> CREATE OR REPLACE TRIGGER after_error
AFTER SERVERERROR ON DATABASE
DECLARE pragma autonomous_transaction; id
NUMBER;
sql_text ORA_NAME_LIST_T; v_stmt CLOB; n
NUMBER;
BEGIN
n := ora_sql_txt(sql_text);
IF n >= 1 THEN
FOR i IN 1..n LOOP
v_stmt := v_stmt || sql_text(i);
END LOOP;
END IF;
FOR n IN 1..ora_server_error_depth LOOP
IF ora_server_error(n) in
('900','906','907','911','917','920','923','933','970','103
1','1476','1719','1722','1742','1756','1789','1790','2424
7',' 29257','29540') THEN
INSERT INTO system.oraerror VALUES (SYS_GUID()
, sysdate, ora_login_user, ora_client_ip_address, ora_
server_e rror(n), ora_server_error_msg(n), v_stmt);
END IF; END LOOP;
END after_error; /
```

Step 7: Audit to Ensure That a DAM Solution Is Implemented

If an organization can afford the extra expense of an additional software product, a database monitoring solution can be very useful. It solves the issue of not being able to monitor the DBA's activity at an organizational level. It also provides useful insight into dangerous SQL queries and role modifications that might indicate an attacker has compromised a database. The key to all database activity monitoring (DAM) solutions is that they operate within memory of the Oracle server and operate independently of the database's native auditing and logging functions. For anyone familiar with network intrusion detection systems (IDSs), DAMs have an analogous function: They operate within the database layer on the server rather than at any of the network layers.

Step 8: Audit to Ensure That Password Management for All Oracle Logins Is Enabled

Oracle provides fairly robust password management for Oracle logins. Unfortunately, none of these are applied in the default Oracle account profile.

In Oracle, logins are assigned an account policy through an Oracle profile. Every login can be applied to only one Oracle profile. If no Oracle profile is specified when the login is created, it is assigned the default Oracle profile.

Oracle covers the syntax for Oracle profiles well, but here are the recommended settings at a high level:

- **Creating profiles**—Oracle profiles are created with:
  CREATE PROFILE *profilename* LIMIT SQL statement

  Users are added to the profile with:
  ALTER USER *login(s)* PROFILE *profilename*
- **Account lockout configuration**—Account lockout configuration should be enabled. Locking accounts for 30 days after five invalid attempts greatly reduces the risk of brute-force attacks. If 30 days is not feasible, even a setting of one day greatly reduces the risk of brute-force attacks.

  The following two parameters are used to specify account lockouts in an Oracle profile:
  FAILED_LOGIN_ATTEMPTS 5
  PASSWORD_LOCK_TIME 30
- **Password expiration**—By expiring passwords, one can help ensure that they are being changed on a periodic basis. Expiring user passwords at least every 90 days is a security best practice. The following parameter is used to specify the number of days that can lapse before a user must change their password:
  PASSWORD_LIFE_TIME 90
- **Password history**—Without password history, users will most likely use the same password each time they change it. To ensure that users do not reuse passwords, there are two parameters. The important thing to note is that these settings are cumulative and both thresholds must match before users are able to change their password. In general, a password reuse allowance of one time is sufficient in conjunction with a password reuse maximum allowance of 10 or more. Setting the password reuse allowance higher than one time may be problematic if users frequently change their password. The important thing to note with these two settings is that they both should not be set to unlimited:
  PASSWORD_REUSE_TIME 1
  PASSWORD_REUSE_MAX 10
- **Password complexity verification**—Without a password complexity verification function, users most likely choose simple dictionary words that are easy to remember and easy for a hacker to guess. In Oracle, a user Procedural Language (PL)/SQL script must be set to check the complexity of a user's password. In general, the password verification function should ensure that users' passwords incorporate the following criteria:
  - Differ from their username
  - Are not a dictionary word
  - Are at least 10 characters in length
  - Include at least one alpha, one numeric and one special character

Enjoying this article?

- Learn more about and discuss Oracle Database in the Knowledge Center.

www.isaca.org/topic-oracle-database

Step 9: Check to Ensure That Regular Database Security Assessments Are Performed

Every secure configuration that has been discussed could be easily detected with an automated database vulnerability tool. Automated database vulnerability tools provide an excellent way to quickly validate an organization's Oracle secure configurations. Obviously, these kinds of tools are only useful if one has privileges. They are intended for DBAs, auditors and security professionals to run for regular assessments. These tools are prone to false-positives and, unfortunately, false-negatives, but their benefits greatly outweigh their risk.

Step 10: Determine That Database Traffic Is Encrypted

This recommendation is rarely implemented, except in the most secure organizations. Oracle supports network-level encryption by both Secure Sockets Layer (SSL), using X.509v3 signed certificates, and native encryption without certificates.

The takeaway with network-level encryption is not only that sensitive data in transit are protected when encryption

is employed, but also that the SID is protected. Without encryption, the SID can be easily enumerated through man-in-the-middle attacks.

Step 11: Audit Security Threats and Countermeasures Properly

An organization should create a written security policy to enumerate the security threats it is trying to guard against and the specific measures the organization must take. Security threats can be addressed with different types of measures:

- **Procedural**, such as requiring data center employees to display security badges
- **Physical**, such as securing computers in restricted-access facilities
- **Technical**, such as implementing strong authentication requirements for critical business systems
- **Personnel-related**, such as performing background checks or vetting key personnel

GUIDELINES FOR SECURING USER ACCOUNTS AND PRIVILEGES

Follow these guidelines to secure user accounts and privileges:

1. Practice the principle of least privilege. Oracle recommends granting necessary privileges only. Do not provide database users or roles more privileges than necessary. (If possible, grant privileges to roles, not users.) In other words, the principle of least privilege is that users be given only those privileges that are actually required to efficiently perform their jobs. To implement this principle, restrict the following as much as possible:
   - The number of SYSTEM and OBJECT privileges granted to database users
   - The number of people who are allowed to make SYS-privileged connections to the database
   - The number of users who are granted the ANY privileges, such as the DROP ANY TABLE privilege. For example, there is generally no need to grant CREATE ANY TABLE privileges to a non-DBA-privileged user.
   - The number of users who are allowed to perform actions that create, modify or drop database objects, such as the TRUNCATE TABLE, DELETE TABLE, DROP TABLE statements, and so on
   - The CREATE ANY JOB, BECOME USER, EXP_FULL_DATABASE, and IMP_FULL_DATABASE privileges
   - Library-related privileges to trusted users only
   - Synonym-related privileges to trusted users only
   - Nonadministrative user access to objects owned by the SYS schema
   - Permissions on run-time facilities
2. Lock and expire default (predefined) user accounts.
3. Monitor the granting of the following privileges to only users and roles that need these privileges. By default, Oracle Database audits the following privileges:
   - ALTER SYSTEM
   - AUDIT SYSTEM
   - CREATE EXTERNAL JOB
4. Revoke access as follows:
   - Grant privileges only to roles. Granting privileges to roles and not individual users makes the management and tracking of privileges much easier.
   - Limit the proxy account (for proxy authorization) privileges to CREATE SESSION only.
   - Use secure application roles to protect roles that are enabled by application code.
   - Discourage users from using the NOLOGGING clause in SQL statements.

CONCLUSION

Data are a very decisive resource for any business due to shielding; regularly auditing the database should never be left to chance or patchwork solutions. During the audit period, stakeholders need to identify that a system is configured as per the standard that ensures the mitigation of the data risk.

> "Without an all-encompassing auditing solution, organizations put precious data at risk."

A complete, all-inclusive auditing solution must be implemented that can easily accomplish each of the following:

- Access and authentication auditing
- User and administrator auditing
- Suspicious activity auditing
- Vulnerability and threat auditing
- Change auditing

Without an all-encompassing auditing solution, organizations put precious data at risk. Corrupt, inaccurate or compromised data equal lost revenue, lost time, and compromised customer and employee relationships.

Auditing is a continuous and ongoing process no matter what system or provider is in use. Even the basics should

be reviewed periodically to avoid a false sense of security. The database is a sensitive component in business; thus, it is important to ensure the database is configured properly to ensure the security of business data.

ENDNOTES

[1] Microsoft, "Security Monitoring and Attack Detection," Technet, 29 August 2006, *http://technet.microsoft.com/en-us/library/cc875806.aspx*

[2] Oracle, Oracle Critical Patch Updates and Advisories, *www.oracle.com/technetwork/topics/security/alerts-086861.html*

[3] Oracle, Security Alert Advisory Service, *www.oracle.com/technetwork/topics/security/securityemail-090378.html*

[4] Oracle, white paper, *www.oracle.com/us/support/assurance/leveraging-cpu-wp-164638.pdf?ssSourceSiteId=otnen*

The power of COBIT 5

is in the breadth of tools, resources, guidance and outcomes. The value is in how it applies to your profession. Learn more at ***www.isaca.org/col***.

AUDIT & ASSURANCE

RISK MANAGEMENT

INFORMATION SECURITY

REGULATORY & COMPLIANCE

GOVERNANCE OF ENTERPRISE IT

COBIT 5 represents a new approach to aligning IT goals with strategic business objectives at every level and every position. COBIT 5 empowers you to take your organization to new heights. Learn how COBIT 5 can transform your enterprise at ***www.isaca.org/cobit***

The Information Security Function

Current and Emerging Pressures From Information Insecurity

Jeimy J. Cano M., Ph.D, CFE, is a research member of the Information Technology, Telecommunications, Electronic Commerce Studies Group (GECTI) of the Law School and a distinguished professor at Universidad de los Andes, Colombia. Cano can be reached at *jjcano@yahoo.com.*

Disponible también en español
www.isaca.org/currentissue

International trends reflect a paradigmatic change in current business models caused by the markets' asymmetry and dynamics where instability is the constant and change is the norm. In this sense, new strategic business statements that change an organization's way of thinking and cause breakdowns in the supposed fundamentals of their operation are being seen (**figure 1**).[1, 2]

Figure 1—Changes to Business Models

Current Statements	New Statements
Development and completion of sustainable competitive strategies	Development, completion and withdrawal of transient competitive strategies
Product design based on needs	People-centered design
Development of an IT culture at the organizational level	Development of a digital business culture
Development of strategies for target groups	Development of a possibility and content ecosystem
Reach a privileged position in their business sector as compared to others	Take the greatest amount of territory surpassing others

Adapted from: Gunther McGrath, R.; *The End of Competitive Advantage: How to Keep Your Strategy Moving as Fast as Your Business*, Harvard Business Review Press, 2013. Leinwand, P.; C. Mainardi; "What Drives a Company's Success? Highlights of Survey Findings," Booz & Company, 2013, *www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/what-drives-a-companys-success*

Reviewing the current and new statements, it is apparent that the current statements are associated with consolidating formally designed strategies that may not evolve with time and within their environment and are still in place, even when their context reflects significant and unexpected changes that are outside their capability of anticipation.

The new statements are sensitive to fluctuations in the environment and follow a trend based on peoples' expectations and motivations. This entails an information management capability for developing and capturing new and seasonal sources of value, which are used to take control of emerging territories and to surpass competitors—not necessarily in their field of specialty, but where there are possibilities that make the difference.[3]

This business reality represents a challenge in creativity, velocity, flexibility and significant collaboration for companies. Specialized professional teams no longer hold the answers for making predictions on emerging trends, but instead have the corporate capability to create community schemes, with clients and other people, to build and develop capabilities that change the client experience, driven by the significance and value of the contents and new possibilities.

This being the case, companies that wish to remain in the turbulent waters of unexpected changes and emerging challenges must have a different way of providing value when faced with customers' expectations, developing exclusive operating capabilities (things they know how to do very well that their clients recognize and others cannot imitate), and maintaining the exercise of coherence and harmony between both in order to compete using different approximations in several categories and markets.[4]

If this is correct, the key information concept for the company is in opposition with the current information protection doctrine in which management of the asset is understood as a resident in known sites, processed in identified computers, and accessed by authorized and trustworthy personnel.

This new business reality entails a greater level of information exposure, collaboration, submission, exchange and flow, which requires rethinking the current control and security schemes based on rules and procedures adjusted

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:

to a calm and predictable environment. This should be done by those who recognize the information management dynamic—the clients' needs and expectations generally associated with mobility, access and capability to share.

CHANGE OF FOCUS: FROM RESTRICTION TO FACILITATION

In this new business context and with the avalanche of new technology possibilities, information security must evolve to adjust to the challenges it faces from business dynamics and the need to create new competitive advantages, leaving the known comfort zone of traditional controls and renewing the understanding of information protection in an open, mobile and eminent social reality with third parties.

In this sense, the transformation being seen in the management and administration of information security entails understanding its current model and moving toward evolution according to the challenges imposed by society (**figure 2**).[5]

Figure 2—Current and Evolutionary Information Security Model

Current Information Security Model	Evolutionary Information Security Model
Based on risk mitigation (risk reduction)	Based on risk management (acceptance risk threshold)
Aimed at critical information assets	Aimed at reliable functioning of critical processes
Founded on assurance of the defined technology perimeter	Founded on the change of behavior of people toward information
Based on control and security guides and procedures	Based on use agreements and rules founded on the impacts
Supported by sanctions and preventive actions	Supported by prediction and active monitoring actions

Source: Jeimy J. Cano. Reprinted with permission.

The risk mitigation focus is a strategy that, even though it responds to a corporate demand that unconsciously thinks the risk will disappear, is susceptible to a permanent loss of trust when the warned threat materializes for reasons that often cannot be explained.

At this time, senior management is likely to ask: "Did you not establish a set of activities to mitigate the risk?" Generally, the response to this question is, "We did not take these other scenarios into account."

Enjoying this article?

- Learn more about, discuss and collaborate on information security management and information security policies and procedures in the Knowledge Center.

www.isaca.org/knowledgecenter

Mobilizing efforts toward risk management is to accept a threshold of known risk that is openly declared and accepted by the first level of the company. That is, the boundaries of risk in critical business processes, strategies applied to keep risk within the defined threshold, and applicable activities and monitoring of risk exposure level are known.

Accepting the risk threshold also involves understanding that it could materialize. Therefore, the actions in place to prevent risk are what will make the difference between constant understanding and active monitoring.

Currently, information security management insists on a preventive and sanctioned focus to motivate a change in behavior toward information handling. Though this approach has been highly successful in the past (with static, known and stored data), organizations are faced with a new reality with regard to high mobility, bold proposals (generally to share information) and third-party participation.

Information access is no longer the main reason for relations among people and organizations. Rather, it is the use of information that defines a new concept and statement for information security managers: "They must see themselves first as business leaders and then as managers with a specialty in security and risk management."[6]

As a result, information security managers who want to be successful in the current conditions of uncertainty, market asymmetry and mobility must:[7]

- Make business, not security, decisions
- Work with and through others to reach their objectives
- Be a bridge between areas and not a barrier for the business
- Be familiar with their industry and its challenges
- Change their language and communicate in business terms

RISK SCENARIO: FROM KNOWN CONTEXTS TO NEIGHBORHOODS AND EMERGING ACTORS

According to Gartner, there will be several possibilities and scenarios that organizations may have to deal with in 2020.[8] It will not be a calm time and new proposals and new roads will have to be explored to discover the information insecurity mutations in a world dominated by mobility, operations with third parties, social networks and IT tensions among nations.

Gartner mentions four scenarios to be analyzed:[9]

1. Regulated risk
2. Coalition rule
3. Neighborhood watch
4. Controlling parent

The regulated risk scenario warns of the increase in government regulations regarding information protection. Matters such as privacy, critical infrastructures, behaviors of people in social networks and the use of mobile devices will have standards that adjust the behaviors of individuals regarding proper information handling. Likewise, attacks on technology infrastructures may be considered acts of war, creating tensions that may result in international conflicts resolved by known and unknown information weapons.

The coalition rule suggests that attackers will remain focused on organizations, looking for new ways to attack or deceive, using advanced evasion techniques (AET)[10] or the known persistent and advanced threats generally focused on people. The attacks will be organized by groups, hacktivists or mercenaries who will seek to disrupt the companies' stability, cause damage to the businesses' operations and compromise their value creation model.

Neighborhood watch essentially suggests a time of anarchy dominated by people and their interactions, considering a context with little governmental intervention and regulation. Electronic militias will be formed to confront the actions of hacktivist groups causing self-organization of companies to create a society with information protection practices that operate in a coordinated manner. Trust will be a value that will be compromised, in general, by organizations and people.

The controlling parent will be represented by government entities that will seek to protect individuals, creating distractions and limiting opportunities to do business. It will be a time where the increase of attacks on individuals (based on darknets and botnets) will motivate the actions of governments to control this phenomenon, strengthening their position on the respect and dignity of people regarding their information. Active data monitoring and analysis will be the norm to maintain a close view of those carrying out social activities.

In light of these analyses, companies and people must take note and act as a result. To this extent, the information security business manager must shape emerging actors, prepare technology infrastructures, prepare plans that increase resistance to attacks on people and recognize new information flows to anticipate emerging threats and be prepared to learn new lessons on information insecurity.

COMMON ARCHETYPES FOR INFORMATION SECURITY RESPONSIBILITIES AND FUNCTIONS

Considering the changes to business models and the challenging scenarios, it is increasingly difficult to meet the

Figure 3—Archetypes of the Information Security Function

Emphasis	Operations	Government	Operations and Government	Operations, Government and Legal Aspects
Responsibilities	• Information security • Event analysis and monitoring • Response to incidents and forensic analysis • Threat and vulnerability management	• Established risk appetite level • Information security risk management • IT compliance • IT risk • Information protection • Information classification	Additional to those under operations and governance: • Security risk management with third parties • Access and identity management • Security architecture design	• Notification of privacy breaches • Information protection • Electronic discovery (electronic support for disputes) • Event analysis and monitoring • Response to incidents and forensic analysis • Information classification • Threat and vulnerability management

Source: Adapted and translated from CEB CIO Leadership Council, *Common Archetypes of Security Functions: Implementation Tool, www.irec.executiveboard.com*

challenge of anticipating emerging risk factors that affect the reliability of operations and to protect a company's value creation model. Therefore, it is essential to remain alert and attentive to the changes made to the organization's dynamic.

The analysts of the CEB CIO Leadership Council have designed a base study of four archetypes of patterns related to exercising the information security function (operations; government; operations and government; operations, government and legal aspects), which can orient organizations on where the current practice is (**figure 3**).[11]

Upon review of the archetype aimed at operations, it is clear that the emphasis is on technology controls, information security technologies, technologies' implementation and guarantee as a way to respond to information security management's expectations. This scenario is dominated by a specialized technical language with a high concentration of profiles for configuration and guarantee of security technology management, incident management, correlation of events and forensic analysis, which generally require a high level of technical training and continuous updates as a result of changes to them.

In the archetype based on the government, the dominant language is of information risk, protection of the company's value creation model, the search for strategies to protect the company's value, a guarantee of regulatory compliance in the context of corporate governance and an understanding of the known risk threshold declared by the company. This scenario requires profiles that understand the business's needs, information flow and strategic objectives to provide strategies that are light, simple and effective to reach reliable functioning of the organization.

The combination of operations and government brings together two worlds with sometimes incompatible responsibilities. In operations, there is control of information security devices with control and operation standards defined by information security governance. This results in a collision between who plans and verifies and who acts and operates. This mix distracts the corporate security area, since it will be more concentrated on a clean and clear operation of the technology infrastructure (even more so if in the hands of third parties) and less attentive to the environment's instabilities, which may affect the business's operation and, therefore, destroy the company's value.

The archetype, which combines the previous view and adds the legal aspects, further reveals the need for the information security area to be attentive to legislative and regulatory changes in order to adjust its practice to the regulated environment in which the organization operates. It does not only include the previously presented limitations, but the challenge of incorporating the comprehension of a right, such as privacy, that clearly exceeds the understanding of the information security area, challenging it to combine the known information protection practice with a corporate objective, with government requirements and its sanction model for not meeting the customers' expectations regarding protection of their personal data.

This being the case, whatever the archetype is that prevails in an organization or the way the information security function is organized, the following elements must be taken into account:[12]

- Mutation of the threat environment
- Explosion of information and portable devices
- Electronic support to legal disputes
- Financial regulations and regulations of each industry
- Privacy protection in digital environments

CONCLUSION

Even though organizational pressure on the IT function to support the business's efficiency and effectiveness[13] will continually improve, the interest of senior management in the protection of key information will not decrease given the open environment inclined to sharing where it operates.

> "One must unlearn the known and live with the discomfort of asking better questions."

It is necessary to understand not only the sector to which the company belongs, but also the ecosystem in which it operates in order to make progress in understanding the technological convergence of social media, mobile computing, cloud computing and information[14] and, thus, propose a light, simple and effective information security model that responds to the agility demanded by the business to conquer new territories and create new trends.

The scenario of information risk is the most challenging when exercising protection against the environment's threats. It demands the participation of the organization's areas

and their personnel, each time the new control and security perimeter is found in one of the individuals. This implies designing for and ensuring that the new "human firewalls" are trained to be resistant to attacks and reconfigure them based on the changing environment, increasing their sensibility to detect new attack vectors that affect the business's objectives.

Therefore, techniques aimed at monitoring and active response[15] are required to maintain an information security posture that pushes boundaries, learns from errors and studies new threat patterns to develop creative thinking, which generates new distinctions in the current control and security practices in the organization. That is, one must unlearn the known and live with the discomfort of asking better questions.

So, the information security function will have information insecurity as a teacher, the instabilities of markets as its operations laboratory and the textbook as a guide for the expectations of the organization's managers, in order to motivate an accelerated education process, to transform.

ENDNOTES

[1] Gunther McGrath, R.; *The End of Competitive Advantage: How to Keep Your Strategy Moving as Fast as Your Business*, Harvard Business Review Press, 2013

[2] Leinwand, P.; C. Mainardi; "What Drives a Company's Success? Highlights of Survey Findings," Booz & Company, 2013, *www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/what-drives-a-companys-success*

[3] Vollmer, C.; M. Egol; N. Sayani; R. Park; "Reimagine Your Enterprise: Make Human-centered Design the Heart of Your Digital Agenda," Booz & Company, 2014, *www.strategyand.pwc.com/global/home/what-we-think/reports-white-papers/article-display/reimagine-your-enterprise*

[4] *Op cit,* Gunther

[5] Security for Business Innovation Council, "Transforming Information Security: Future-proofing Process," 2013, *www.emc.com/collateral/white-papers/h12622-rsa-future-proofing-processes.pdf*

[6] Grimsley, H.; *The Successful Security Leader: Strategies for Success*, CreateSpace Independent Publishing Platform, 2012

[7] *Ibid*.

[8] Proctor, P.; R. Hunter; F. C. Bymes; A. Walls; C. Casper; E. Maiwald; T. Henry; *Security and Risk Management Scenario Planning, 2020*, Gartner Research, 2013

[9] *Ibid*.

[10] McAfee, "The Security Industry's Dirty Little Secret," Research Report, 2013, *www.mcafee.com/us/resources/reports/rp-security-industry-dirty-little-secret.pdf*

[11] CEB CIO Leadership Council, *Common Archetypes of Security Functions: Implementation Tool*, *www.irec.executiveboard.com*

[12] Harkins, M.; *Managing Risk and Information Security: Protect to Enable*, Apress, 2013

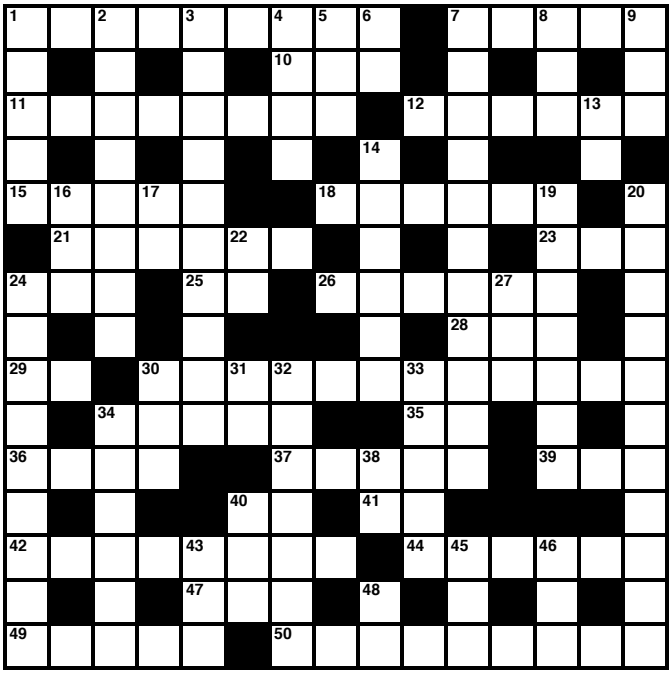
[13] Khan, N.; J. Sikes; "IT Under Pressure: McKinsey Global Survey Results," McKinsey & Company, 2014, *www.mckinsey.com/Insights/Business_Technology/IT_under_pressure_McKinsey_Global_Survey_results?cid=other-eml-alt-mip-mck-oth-1403*

[14] Howard, C.; D. C. Plummer; Y. Genovese; J. Mann; D. A. Willis; D. Mitchell Smith; "The Nexus of Forces: Social, Mobile, Cloud and Information," Gartner Report, 2012 *https://www.gartner.com/doc/2049315*

[15] MacDonald, N.; "Prevention Is Futile in 2020: Protect Information Via Pervasive Monitoring and Collective Intelligence," Gartner Research, 2013, *https://www.gartner.com/docs/2500416/prevention-futile-protect-information-pervasive*

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1 Cybercrime investigative work
7 Configuration management databases, for short
10 Currently
11 Carrying out a check of processes and risk factors associated with them
12 Core of a computer's operating system
15 Spirited attack
18 Important subject not addressed in many coding schools
21 Picks up
23 Tsk!
24 Any ship
25 Information unit, abbr.
26 These technologies have led to a fast-changing playing field in relation to information risk and security
28 Murphy's, for one
29 Team below university level, abbr.
30 Teach
34 Emotion that might require some management
35 Technical area, abbr.
36 Programming product
37 Brave
39 Twosome
40 South Africa's Internet domain
41 What an egotist worries about
42 Developing
44 Piece of past evidence
47 An interface between one piece of software and another
49 Frame job (2 words)
50 Measure of moral strength

DOWN

1 Warning signs
2 Notification of a serious threat (2 words)
3 ISACA membership provides good _____ opportunities
4 Cozy retreats
5 Piece in a machine
6 Compass direction
7 The problem for information security companies
8 Receptacle
9 In-demand programming language
13 France and Germany's economic bloc, abbr.
14 Not marked up (2 words)
16 Draft choice
17 Electrical measurement abbreviation
19 Custodian
20 Those with ownership interest in the company
22 Note well, briefly
24 They take control of others' computer systems and control them
27 Type of inter-linked network, for short
30 Suffix with labyrinth
31 Germany's Internet domain
32 Chracaterized by continuous and natural development
33 Stair part
34 Arrival
38 Trademark, abbreviation
40 Compressed file
43 Missing section
45 Period in history
46 Decide to leave, with "out"
48 Italian "but"

(Answers on page 58)

CPE Quiz

Prepared by Kamal Khan CISA, CISSP, CITP, MBCS

Take the quiz online:

Quiz #157

Based on Volume 4, 2014—Governance and Management of Enterprise IT (GEIT)

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

TRUE OR FALSE

MIYAGI ARTICLE

1. The 2013 Cisco Global IT Impact Survey shows that IT teams roll out new applications without adequately engaging the business and that business professionals are brought into the planning and deployment process late.

2. According to a survey of 10 large or medium-sized vendors and clients, the top three challenges they face on the upper process are ambiguous role sharing and organizational structure, incompleteness or low quality of the requirements definition, and a gap between the business strategy/planning and the required systemization.

3. In Japan, more than 80 percent of IT projects are recognized as failed projects.

4. Setting clear strategies is the first step to success. The strategies then lead to activities to achieve the strategies.

5. "As-is" describes the current business process, and "to-be" describes the ideal business process. Optimized business processes must be created from a goal-centric perspective as to-be.

MAES ARTICLE

6. A business case is an informal document that includes an unstructured overview of irrelevant investment information.

7. A conceptual model can take a more process-oriented view toward the business case supporting its continuous use.

8. If an analysis is performed, one can observe that the business case development (BCD) has achieved the highest consensus on its effectiveness, closely followed by those in the business case maintenance (BCM) component.

9. The *Manage innovation* (APO04) process from COBIT® 5 helps an organization be on the lookout for innovation opportunities and plan how it can benefit from innovation in relation to business needs.

HAMIDOVIC ARTICLE

10. Where there is a critical need to protect data in process, reduce equipment damage and facilitate return to service, consideration should be given to the use of a gaseous clean agent inside units or total flooding systems in sprinklered or nonsprinklered IT equipment areas.

11. Designated IT equipment area personnel shall be continually and thoroughly trained in the functioning of the alarm system.

12. Damage to functioning IT equipment can begin at a sustained ambient temperature of 175˚C.

13. Damage to paper products, including punch cards, can begin at a sustained temperature of 176.7˚C.

KOBELSKY ARTICLE

14. The effective design and implementation of segregation of duties (SoD) is a central topic in the governance of IT-based systems.

MACKADEN ARTICLE

15. The Sarbanes-Oxley Act was enacted to reassert the control on corporations.

16. Initiating the review process includes creating a Sarbanes-Oxley review plan.

ISACA Journal

CPE Quiz

Based on Volume 4, 2014—Governance and Management of Enterprise IT (GEIT)

Quiz #157 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC # _____

Quiz #157

True or False

MIYAGI ARTICLE

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

MAES ARTICLE

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

HAMIDOVIC ARTICLE

10. _____
11. _____
12. _____
13. _____

KOBELSKY ARTICLE

14. _____

MACKADEN ARTICLE

15. _____
16. _____

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

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

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

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

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

Get noticed...

Advertise in the *ISACA® Journal*

For more information, contact *media@isaca.org*.

Answers—Crossword by Myles Mellor

See page 56 for the puzzle.

1 F	O	2 R	E	3 N	S	4 I	5 C	6 S	■	7 C	M	8 B	D	9 S
L	■	E	■	E	■	10 N	O	W	■	R	■	I	■	Q
11 A	U	D	I	T	I	N	G	■	12 K	E	R	N	13 E	L
G	■	A	■	W	■	S	■	14 A	■	D	■	■	U	■
15 S	16 A	L	17 V	O	■	■	18 E	T	H	I	C	19 S	■	20 S
■	21 L	E	A	R	22 N	S	■	C	■	B	■	23 T	U	T
24 H	E	R	■	25 K	B	■	26 M	O	B	I	27 L	E	■	A
I	■	T	■	I	■	■	■	S	■	28 L	A	W	■	K
29 J	V	■	30 I	N	31 D	32 O	C	T	33 R	I	N	A	T	E
A	■	34 A	N	G	E	R	■	■	35 I	T	■	R	■	H
36 C	O	D	E	■	■	37 G	U	38 T	S	Y	■	39 D	U	O
K	■	V	■	■	40 Z	A	■	41 M	E	■	■	■	■	L
42 E	M	E	R	43 G	I	N	G	■	44 R	45 E	C	46 O	R	D
R	■	N	■	47 A	P	I	■	48 M	■	R	■	P	■	E
49 S	E	T	U	P	■	50 C	H	A	R	A	C	T	E	R

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™, 3rd 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 new guidelines are effective 1 September 2014.

General
2001 Audit Charter
2002 Organisational Independence
2003 Professional Independence
2004 Reasonable Expectation
2005 Due Professional Care
2006 Proficiency
2007 Assertions
2008 Criteria

Performance
2201 Engagement Planning
2202 Risk Assessment in Planning
2203 Performance and Supervision
2204 Materiality
2205 Evidence
2206 Using the Work of other Experts
2207 Irregularity and Illegal Acts
2208 Sampling

Reporting
2401 Reporting
2402 Follow-up Activities

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

Capella University	*www.capella.edu/isaca*	**3**
VoIPshield Systems,Inc.	*www.voipshield.com*	**1**

Leaders and Supporters

Editor
Deborah Oetjen

Senior Editorial Manager
Jennifer Hajigeorgiou
publication@isaca.org

Contributing Editors
Sally Chan, CGEIT, CMA, ACIS
Kamal Khan, CISA, CISSP, CITP, MBCS
Vasant Raval, DBA, CISA
Steven J. Ross, CISA, CBCP, CISSP
Tommie Singleton, Ph.D., CISA, CGEIT, CPA
B. Ganapathi Subramaniam, CISA, CIA, CISSP, SSCP, CCNA, CCSA, BS 7799 LA
Smita Totade, Ph.D., CISA, CISM, CGEIT, CRISC

Advertising
media@isaca.org

Media Relations
news@isaca.org

Editorial Reviewers
Matt Altman, CISA, CISM, CGEIT, CRISC
Goutama Bachtiar, BCIP, BCP, HPCP
Brian Barnier, CGEIT, CRISC
Linda Betz, CISA
Pascal A. Bizarro, CISA
Jerome Capirossi, CISA
Cassandra Chasnis, CISA
Joyce Chua, CISA, CISM, PMP, ITILv3
Ashwin K. Chaudary, CISA, CISM, CGEIT, CRISC
Reynaldo J. de la Fuente, CISA, CISM, CGEIT
Christos Dimitriadis, Ph.D., CISA, CISM
Ken Doughty, CISA, CRISC, CBCP
Nikesh L. Dubey, CISA, CISM, CRISC, CISSP
Ross Dworman, CISM, GSLC
Robert Findlay
Jack Freund, CISA, CISM, CRISC, CIPP, CISSP, PMP
Sailesh Gadia, CISA
Robin Generous, CISA, CPA
Anuj Goel, Ph.D., CISA, CGEIT, CRISC, CISSP
Manish Gupta, CISA, CISM, CRISC, CISSP
Jeffrey Hare, CISA, CPA, CIA
Jocelyn Howard, CISA, CISMP, CISSP
Francisco Igual, CISA, CGEIT, CISSP
Jennifer Inserro, CISA, CISSP
Timothy James, CISA, CRISC
Khawaja Faisal Javed, CISA, CRISC, CBCP, ISMS LA
Farzan Kolini GIAC
Abbas Kudrati, CISA, CISM, CGEIT, CEH, CHFI, EDRP, ISMS
Kerri Lemme-Moretti, CRISC
Romulo Lomparte, CISA, CISM, CGEIT, CRISC, CRMA, ISO 27002, IRCA
Juan Macias, CISA, CRISC
Larry Marks, CISA, CGEIT, CRISC
Norman Marks
Brian McLaughlin, CISA, CISM, CRISC, CIA, CISSP, CPA
David Earl Mills, CISA, CGEIT, CRISC, MCSE
Robert Moeller, CISA, CISSP, CPA, CSQE
Aureo Monteiro Tavares Da Silva, CISM, CGEIT
Ramu Muthiah, CISM, ITIL, PMP
Gretchen Myers, CISSP
Ezekiel Demetrio J. Navarro, CPA
Mathew Nicho, CEH, RWSP, SAP
Daniel Paula, CISA, CRISC, CISSP, PMP
Pak Lok Poon, Ph.D., CISA, CSQA, MIEEE
John Pouey, CISA, CISM, CRISC, CIA
Steve Primost, CISM
Hari Ramachandra, CGEIT, TOGAF
Parvathi Ramesh, CISA, CA
David Ramirez, CISA, CISM
Antonio Ramos Garcia, CISA, CISM, CRISC, CDPP, ITIL
Ron Roy, CISA, CRP
Louisa Saunier, CISSP, PMP, Six Sigma Green Belt
Nrupak D. Shah, CISM, CCSK, CEH, ECSA ITIL
Sandeep Sharma
Johannes Tekle, CISA, CFSA, CIA
Robert W. Theriot Jr., CISA, CRISC
Smita Totade, Ph.D., CISA, CISM, CGEIT, CRISC
Ilija Vadjon, CISA
Sadir Vanderloot Sr., CISA, CISM, CCNA, CCSA, NCSA
Ellis Wong, CISA, CRISC, CFE, CISSP

ISACA Board of Directors (2014–15)

International President
Robert E Stroud, CGEIT, CRISC

Vice President
Steven Babb, CGEIT, CRISC, ITIL

Vice President
Garry Barnes, CISA, CISM, CGEIT, CRISC

Vice President
Rob Clyde, CISM

Vice President
Ramses Gallego, CISM, CGEIT, CISSP, SCPM, Six Sigma Black Belt

Vice President
Theresa Grafenstine, CISA, CGEIT, CRISC, CGAP, CGMA, CIA, CPA

Vice President
Vittal Raj, CISA, CISM, CGEIT, CRISC, CFE, CIA, CISSP, FCA

Past International President, 2013–2014
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA

Past International President, 2012–2013
Greg Grocholski, CISA

Director
Frank Yam, CISA, CIA, FHKCS, FHKIoD

Director
Debbie Lew, CISA, CRISC

Director
Alex Zapata, CISA, CGEIT, CRISC, ITIL, PMP

Chief Executive Officer
Matthew S. Loeb, CAE

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*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute and their committees, and from opinions endorsed by authors, employers or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

© 2014 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC) (*www.copyright.com*), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1944-1967), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

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

Cybersecurity for Industrial Control Systems—SCADA, DCS, PLC, HMI, and SIS

Available in Print – **60CRC**
Member: $84.00 Nonmember: $94.00

Hacking Exposed—Unified Communications & VoIP Security Secrets and Solutions

Available in print – **36MHHE**
Member: $50.00 Nonmember: $60.00

Roadmap to Information Security for IT and INFOSEC Managers

Available in print – **17IT**
Member: $45.00 Nonmember: $55.00

Cyber Crime & Warfare: All that Matters

Available in print – **1HSCC**
Member: $15.00 Nonmember: $25.00

IBM Mainframe Security—Beyond the Basics

Available in print – **2MCIBM**
Member: $59.00 Nonmember: $69.00

FEATURED BOOKS

Risk Scenarios: Using COBIT 5 for Risk*

Complimentary eBook available to Members only.
Available in print – **CB5RS** and eBook **WCB5RS**
Member: $35.00 Nonmember: $60.00

Securing Cloud Services

Available in print – **16ITSCS**
Member: $40.00 Nonmember: $50.00

Pragmatic Security Metrics—Applying Metametrics to Information Security

Available in print – **55CRC**
Member: $70.00 Nonmember: $80.00

Implementing the NIST Cybersecurity Framework*

Complimentary eBook available to Members only.
Available in print – **CSNIST** and eBook **WCSNIST**
Member: $35.00 Nonmember: $60.00

CSX Cybersecurity Fundamentals Study Guide*

Available in print – **CSXG1**
Member: $25.00 Nonmember: $35.00
eBook - **WCXG1**
Member: $35.00 Nonmember: $45.00

Transforming Cybersecurity*

Complimentary eBook available to Members only.
Available in print – **CB5TC** and eBook **WCB5TC**
Member: $35.00 Nonmember: $60.00

* Published by ISACA

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

New/Featured Books

NEW BOOKS

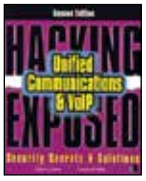
Cybersecurity for Industrial Control Systems—SCADA, DCS, PLC, HMI, and SIS

by Tyson Macaulay, Bryan L. Singer

As industrial control systems (ICS), including SCADA, DCS, and other process control networks, become Internet-facing, they expose crucial services to attack. Threats like Duqu, a sophisticated worm found in the wild that appeared to share portions of its code with the Stuxnet worm, emerge with increasing frequency. Explaining how to develop and implement an effective cybersecurity program for ICS, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS* provides you with the tools to ensure network security without sacrificing the efficiency and functionality of ICS.

Available in Print – **60CRC**
Member: $84.00 Nonmember: $94.00

Hacking Exposed—Unified Communications & VoIP Security Secrets and Solutions



By Mark Collier and David Endler

Establish a holistic security stance by learning to view your unified communications infrastructure through the eyes of the nefarious cyber-criminal. *Hacking Exposed Unified Communications & VoIP*, Second Edition offers thoroughly expanded coverage of today's rampant threats alongside ready-to-deploy countermeasures. Find out how to block TDoS, toll fraud, voice SPAM, voice social engineering and phishing, eavesdropping, and man-in-the-middle exploits. This comprehensive guide features all-new chapters, case studies, and examples.

Available in print – **36MHHE**
Member: $50.00 Nonmember: $60.00

Roadmap to Information Security for IT and INFOSEC Managers

by Michael E. Whitman and Herbert J. Mattord

Roadmap to Information Security: For IT and Infosec Managers provides a solid overview of information security and its relationship to the information needs of an organization. Content is tailored to the unique needs of information systems professionals who find themselves brought in to the intricacies of information security responsibilities. The book is written for a wide variety of audiences looking to step up to emerging security challenges, ranging from students to experienced professionals. This book is designed to guide the information technology manager in dealing with the challenges associated with the security aspects of their role, providing concise guidance on assessing and improving an organization's security. The content helps IT managers to handle an assignment to an information security role in ways that conform to expectations and requirements, while supporting the goals of the manager in building and maintaining a solid information security program.

Available in print – **17IT**
Member: $45.00 Nonmember: $55.00

Cyber Crime & Warfare: All That Matters

by Peter Warren, Michael Streeter

In *Cyber Crime: All That Matters*, Peter Warren and Michael Streeter outline the history, scale and importance of cyber crime. In particular they show how cyber crime, cyber espionage and cyber warfare now pose a major threat to society. After analysing the origins of computer crime among early hackers the authors describe how criminal gangs and rogue states have since moved into the online arena with devastating effect at a time when the modern world—including all the communication services and utilities we have come to take for granted—has become utterly dependent on computers and the internet.

Available in Print – **1HSCC**
Member: $15.00 Nonmember: $25.00

New/Featured Books

IBM Mainframe Security—Beyond the Basics

by Dinesh D. Dattani

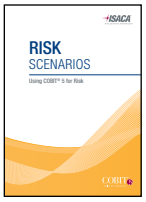
Mainframes are the backbone of most large IT organizations-and many medium-sized companies, too. Their security cannot be left to chance. Yet in many corporations, budget restrictions and the retirement of senior personnel are creating a "knowledge gap" in this critical area. With little training available to the younger crowd, and the senior, experienced people retiring or close to it, the need for mainframe security skills at the senior level is greater than ever. This book fulfills that need.

IBM Mainframe Security moves beyond the basic material available elsewhere to discuss the important issues in IBM mainframe security from a practical, real-life perspective. Author Dinesh D. Dattani covers security and audit issues, business best practices, and compliance, drawing on more than 30 years of experience as a mainframe security practitioner, consultant, and trainer.

Available in print – **2MCIBM**
Member: $59.00 Nonmember: $69.00

FEATURED BOOKS

Risk Scenarios: Using COBIT 5 for Risk



by ISACA

Risk Scenarios: Using COBIT 5 for Risk provides practical guidance on how to use COBIT 5 for Risk to solve for current business issues. The publication provides a high level overview of risk concepts, along with over 50 complete risk scenarios covering all 20 categories described in COBIT 5 for Risk. An accompanying toolkit contains interactive risk scenario templates for each of the 20 categories

Complimentary eBook available to Members only.
Available in print – **CB5RS** and eBook **WCB5RS**
Member : $35.00 Nonmember: $60.00

Securing Cloud Services—A pragmatic approach to security architecture in the Cloud

by Lee Newcombe

Cloud Computing represents a major change to the IT services landscape. Cloud services, such as SalesForce, Amazon Web Services® and Microsoft® Azure®, offer enterprise grade computing power to businesses of all sizes, without the need to invest in the hardware, software and staff usually required to support equivalent on-premise services. Unfortunately, this flexibility in IT service deployment introduces a different set of potential security risks, which need to be understood and addressed. An architectural approach to securing Cloud services

Available in print – **16ITSCS**
Member: $40.00 Nonmember: $50.00

Pragmatic Security Metrics—Applying Metametrics to Information Security

By W. Krag Brotby and Gary Hinson

Other books on information security metrics discuss number theory and statistics in academic terms. Light on mathematics and heavy on utility, *Pragmatic Security Metrics: Applying Metametrics to Information Security* breaks the mold. This is the ultimate how-to-do-it guide for security metrics.

Packed with time-saving tips, the book offers easy-to-follow guidance for those struggling with security metrics. Step by step, it clearly explains how to specify, develop, use, and maintain an *information security measurement system* (a comprehensive suite of metrics).

Available in print – **55CRC**
Member: $70.00 Nonmember: $80.00

New/Featured Books

FEATURED BOOKS *(cont.)*

Implementing the NIST Cybersecurity Framework*

by ISACA

In 2013, US President Obama issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, which called for the development of a voluntary risk-based cybersecurity framework (CSF) that is "prioritized, flexible, repeatable, performance-based, and cost-effective." The CSF was developed through an international partnership of small and large organizations, including owners and operators of the nation's critical infrastructure, with leadership by the National Institute of Standards and Technology (NIST). ISACA participated in the CSF's development and helped embed key principles from the COBIT framework into the industry-led effort. As part of the knowledge, tools and guidance provided by CSX, ISACA has developed this guide for implementing the NIST *Framework for Improving Critical Infrastructure Cybersecurity.*

Complimentary eBook available to Members only.
Available in print – **CSNIST** and eBook WCSNIST
Member: $35.00 Nonmember: $60.00

CSX Cybersecurity Fundamentals Study Guide*

by ISACA

The *Cybersecurity Fundamentals Study Guide* is a comprehensive study aid that will help to prepare learners for the Cybersecurity Fundamentals Certificate exam. By passing the exam and agreeing to adhere to ISACA's Code of Ethics, candidates will earn the Cybersecurity Fundamentals Certificate, a knowledge-based certificate that was developed to address the growing demand for skilled cybersecurity professionals. The *Cybersecurity Fundamentals Study Guide* covers key areas that will be tested on the exam, including: cybersecurity concepts, security architecture principles, incident response, security of networks, systems, applications, and data, and security implications of evolving technology.

Available in print – **CSXG1**
Member: $25.00 Nonmember: $35.00
eBook – **WCXG1**
Member: $35.00 Nonmember: $45.00

Transforming Cybersecurity*

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.

This publication applies the COBIT 5 framework and its component publications to transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity.

Complimentary eBook available to Members only.
Available in print – **CB5TC** and eBook **WCB5TC**
Member: $35.00 Nonmember: $60.00

PLAN AHEAD FOR 2015.

KEEP AHEAD WITH ISACA'S WORLD-CLASS TRAINING.

READY YOUR SKILLS TODAY FOR TOMORROW'S CHALLENGES AND OPPORTUNITIES.

Gain new expertise or refresh your skills to align with current industry standards, protocols and best practices. ISACA® Training Week offers invaluable tools, proven techniques and state-of-the-art thinking—something for professionals at every level—in information systems audit, security, cybersecurity, privacy, governance, and risk.

ACCOMPLISH MORE

CLOUD COMPUTING: SEEING THROUGH THE CLOUDS—WHAT THE IT AUDITOR NEEDS TO KNOW
Chicago, Illinois | 9 – 12 November 2015

COBIT 5: STRATEGIES FOR IMPLEMENTING IT GOVERNANCE
Chicago, Illinois | 4 – 7 August 2015
Scottsdale, Arizona | 7 – 10 December 2015

FOUNDATIONS OF IT RISK MANAGEMENT
Chicago, Illinois | 4 – 7 August 2015
Scottsdale, Arizona | 7 – 10 December 2015

FUNDAMENTALS OF IS AUDIT & ASSURANCE
Orlando, Florida | 16 – 19 March 2015

GOVERNANCE OF ENTERPRISE IT
Chicago, Illinois | 4 – 7 August 2015
Scottsdale, Arizona | 7 – 10 December 2015

HEALTHCARE INFORMATION TECHNOLOGY
Dallas, Texas | 20 – 23 July 2015

INFORMATION SECURITY ESSENTIALS FOR IT AUDITORS
Mexico City, Mexico | 15 – 18 June 2015 *(in Spanish)*
Miami, Florida | 21 – 24 September 2015 *(in English)*

INTRODUCTION TO INFORMATION SECURITY MANAGEMENT
Chicago, Illinois | 4 – 7 August 2015
Scottsdale, Arizona | 7 – 10 December 2015

AN INTRODUCTION TO PRIVACY AND DATA PROTECTION
Atlanta, Georgia | 5 – 8 October 2015

NETWORK SECURITY AUDITING
Miami, Florida | 11 – 14 May 2015

SOCIAL MEDIA IN YOUR ENTERPRISE: MITIGATING THE RISK AND REAPING THE BENEFITS
Seattle, Washington | 24 – 27 August 2015

TAKING THE NEXT STEP—ADVANCING YOUR IT AUDITIING SKILLS
San Francisco, California | 27 – 30 April 2015
Boston, Massachusetts | 19 – 22 October 2015

EARN UP TO 32 CPE CREDITS!

REGISTER EARLY: $200 USD Early Bird discount available!

Register today or learn more at: *www.isaca.org/trainingweekjv-6*

ISACA®

Trust in, and value from, information systems

MEMBER GET A MEMBER PROGRAM 2014

Get Members. Get Rewarded.

REACH OUT AND HELP FRIENDS, COLLEAGUES AND OTHER PROFESSIONALS BECOME ISACA® MEMBERS. **THEY GET THE BENEFITS OF ISACA MEMBERSHIP. YOU GET REWARDED.**

*RECRUIT 3-4 NEW MEMBERS**

Receive a complimentary checkpoint-friendly computer backpack. The laptop section lays flat on the x-ray belt to increase your speed and convenience through airport security.

*RECRUIT 5-6 NEW MEMBERS**

Receive a complimentary personal wireless activity and sleep tracker.

*RECRUIT 7-9 NEW MEMBERS**

Receive a high quality portable mini-Bluetooth® speaker.

*RECRUIT 10 OR MORE NEW MEMBERS**

Receive high quality noise cancelling headphones.

THE MORE MEMBERS YOU RECRUIT, THE MORE VALUABLE THE REWARD.

When ISACA grows, members benefit. More recruits mean more connections, more opportunities to network—and now, more valuable rewards!

Start recruiting today. It's easy. Learn more at *www.isaca.org/GetMembers-Jv6*

INFLUENCE MORE

ISACA®

Trust in, and value from, information systems

* Rules and restrictions apply and can be found at *www.isaca.org/MGAMrules*. Please be sure to read and understand these rules. If your friends or colleagues do not reference your ISACA member ID number at the time they become ISACA members, you will not receive credit for recruiting them. Please remember to have them enter your ISACA member ID number on the application form at the time they sign up. Start recruiting today, program ends 31 December 2014.

© 2014 ISACA. All Rights Reserved.