Volume 4, 2015

ISACA® Journal

REGULATIONS & COMPLIANCE

Featured articles:

Vendor Risk Management Demystified

Vendor Governance in the Age of Information Security

Three Ways to Simplify Auditing Software Security Requirements and Design

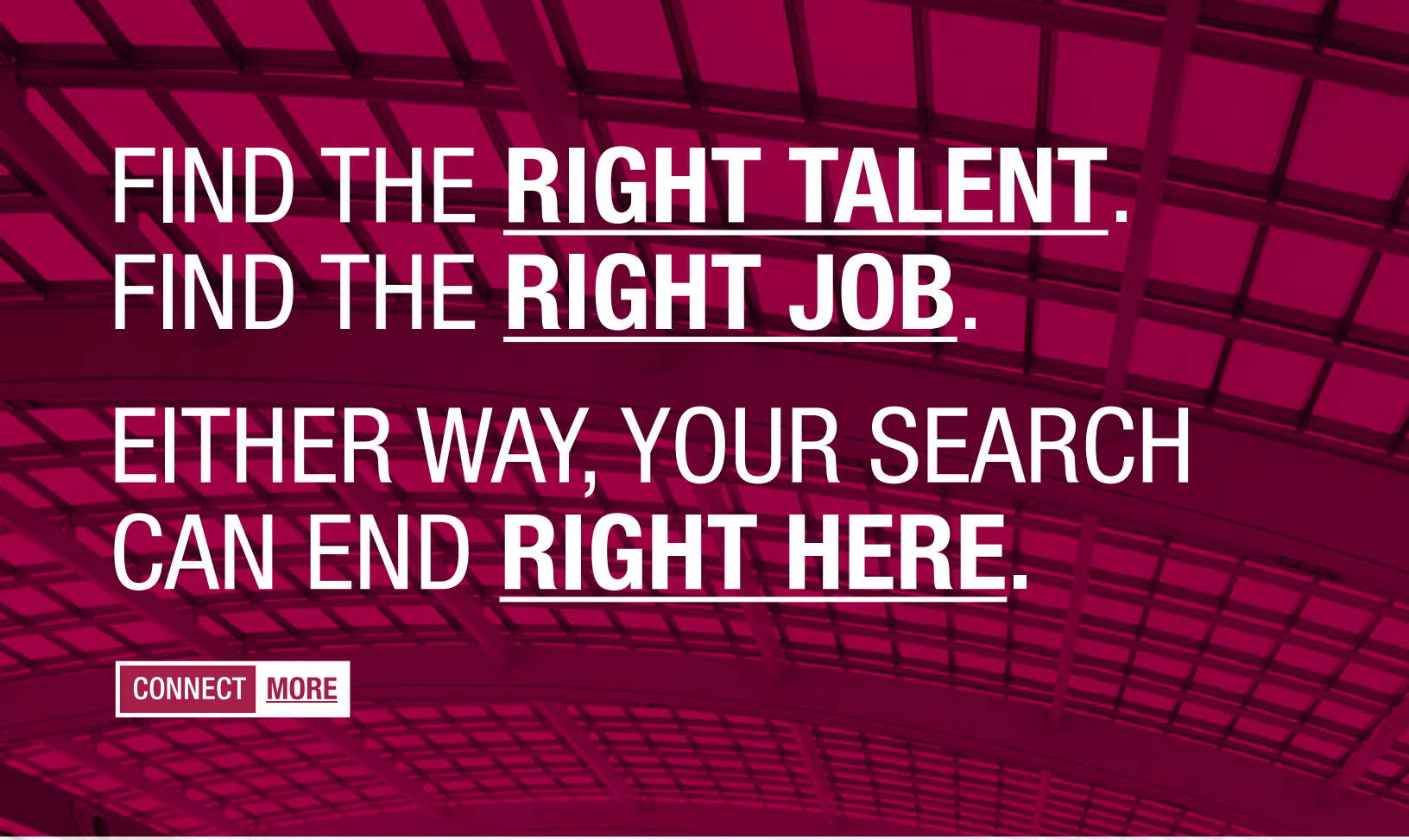
And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG


CSX™
CYBERSECURITY NEXUS
STAY AHEAD OF THREATS.
MOVE AHEAD IN YOUR CAREER.
Cybersecurity Nexus™ (CSX) is your premier resource for knowledge, tools, guidance and professional development in the critical areas of cybersecurity. And now, you can test your abilities with our new skills-based training programs and prove them with our performance-based certifications. Because it's not about showing you have the knowledge — it's about getting the job done.
Visit www.isaca.org/cybercert-jv4 for more information.
ISACA®



FIND THE **RIGHT TALENT**.
FIND THE **RIGHT JOB**.

EITHER WAY, YOUR SEARCH CAN END **RIGHT HERE**.

CONNECT MORE

Whether you are searching for a job or looking for that perfect candidate for your open position, **ISACA's Online Career Centre** is *the* source for IS/IT audit and information security professionals.

EMPLOYERS:

Designations and experience are highlighted providing a special opportunity for those interested in hiring CISA®, CISM®, CGEIT® or CRISC™ holders and applicants with COBIT experience.

JOB SEEKERS:

Take advantage of advanced search features, job alerts, career advice and much more!

More than **450** new jobs posted

350+ new employers posted jobs

735 searchable resumes on average

240,000+ unique page views in 2014

Nearly **50,000** new visitors in 2014

ISACA®

Trust in, and value from, information systems

Visit our Career Centre today at *www.isaca.org/CareerCenter-Jv4* to learn more.

VOLUME 4, 2015

ISACA® Journal

Columns

Features

Plus

Online-exclusive Features

Do not miss out on the *Journal's* online-exclusive content. With new content weekly through feature articles and blogs, the *Journal* is more than a static print publication. Use your unique member login credentials to access these articles at *www.isaca.org/journal.*

Online Features
The following is a sample of the upcoming features planned for July and August.

IS Audit Basics: Auditing Small IS/IT Organizations—When Is an IS/IT Organization Small?
Ed Gelbstein

Cloud Computing Success Depends on the Right Network
Corey Eng

Book Review: FISMA Compliance Handbook
Reviewed by Ibe Etea, CISA, CRISC, CA, CFE, CIA, CRMA

Book Review: Incident Response & Computer Forensics
Reviewed by Dino Ippoliti, CISA, CISM

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

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

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

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

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

Read more from these *Journal* authors...

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

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

Are Software Flaws a Security Problem?

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.*

I suspect I share with many readers of the *ISACA® Journal* an annoyance with customer service people who tell me that they cannot give me any information because the system is down. I am always tempted to yell at them, "That's a terrible excuse! Your systems should not be down." But, hey, the person on the phone is not at fault, so I keep my mouth shut.

But who is responsible? If a hacker caused customer-facing systems to crash, we would think he/she was a criminal. But if an employee in the programming department implements faulty code, we shrug and say, "Oh, well, that is the way computer systems work."

In a recent article in this space that I called "Microwave Software,"[1] I stated that "ultimately, flawed software cannot be secured." My point then was that antiquated software is often the weak spot where cyberattackers take advantage. The more I thought about nonmalicious system downtime, the more I became convinced that systems that fail are themselves insecure, regardless of the intent of the person responsible.

I cannot overstate the number of times I have seen program crashes that caused late-night phone calls, emergency patches and nervous vice presidents. I ruefully admit that I was a terrible programmer in my early career and often was the recipient of those phone calls. Was I a security threat? I would say that, yes, I was, and I resolved the problem by never coding for a living ever again. But what about all those who are still at it and are still putting broken programs into production? Many of the causes of unexpected downtime that I encounter are the same as those that lead to security breaches, as the term is more commonly understood.

> "Systems that fail are themselves insecure, regardless of the intent of the person responsible."

COMPLEXITY

Edgar Dykstra, perhaps the greatest theorist of programming who ever lived, was famous for writing that it was impossible to prove that any but the simplest programs would work. "The art of programming is the art of organizing complexity, of mastering multitude and avoiding its bastard chaos as effectively as possible."[2] If, indeed, Dykstra was correct, then any organization that implements enormous, highly complex systems is, in fact, introducing the possibility of error into its value chain. Application and infrastructure systems are engineered products, which are bound to fail at some point—the concept known as the mean time to failure (MTTF). I am not aware of any organization that attempts to calculate the MTTF of its systems prior to putting them into production. So the business users who rely on the systems are, in effect, involved in a crap shoot. To me, this is a security problem.

INEFFECTIVE INTERFACES

Despite complexity, most applications and infrastructure software work as intended most of the time. That is because whoever wrote the programs (most often a software vendor these days) was able to test their functioning to a generally acceptable extent. (Please spare me the horror stories of vendors using customers for beta testing. That is simply bad practice and is inexcusable.) However, applications interact with other applications and infrastructure. They require interfaces to exchange and jointly use data. It is extremely difficult for programmers (especially, but not only, software vendors) to know all the other systems with which their programs will interface, now or in the future. Since interfaces connect two disparate systems, the programmer of the interface may be insufficiently knowledgeable about one or the other systems, or both. When interfaces themselves are poorly designed or written, programs fail. Hackers know this and attack the interfaces.[3] What difference does it make, in terms of security, if systems abort or mismanage data due to error rather than malice?

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:

FAILURE TO UNDERSTAND THE DATA

When I was a young and very inept Cobol programmer, a mentor said to me, "Kid, get the Data Division right, and the Procedure Division will take care of itself." Cobol has gone the way of the dodo bird, but his advice has not. Programs, like security, follow the data. When a programmer does not understand all the implications of the data that a program affects, the results can include database integrity failures, incorrect calculations or orphaned records. Any of these, and many other data errors,[4] can cause a system to falter or stop.[5] If a database can be infiltrated with errors in this manner, it is not secure.

POOR CHANGE CONTROL

Let us posit for a moment that a program might indeed be perfect at the time it was put into production. Then, it is changed. It is not particularly original to observe that poor change control leads to problematic programs. I would argue that it also leads to insecure programs. Perhaps it is in the nature of change control itself. In an excellent article, Edward Stickel suggests that change control by itself "is not sufficient to cover all the necessary factors and tasks in making well-advised decisions on changes and implementing them effectively." Further, "because the value of the change control process is not apparent to the parties involved, it is seen as a superfluous, bureaucratic exercise and is not taken seriously, which results in poor compliance."[6] I would only add the words *and security* to the end of the previous sentence.

CHANGE MANAGEMENT AND QUALITY

Program failures and security breaches are related, but not equivalent, risk factors. The first stems from incompetence, the second from malign intent. They both can create damage. Is it worth arguing whether fools or felons do the most harm? From my perspective, it is sufficient to know that risk exists and to build safeguards to protect against both.

It has long been a programmer's joke that users want systems to be developed fast, good and cheap; they can have two, but not all three. Who implements in haste repents at leisure, and it is always true that you get what you pay for. To my mind, both programs and security must be built with quality as the foremost design criterion.

Perhaps the best way to achieve quality in both systems and security would be to start fresh with totally new applications with all the latest security techniques. This is a luxury that is unavailable to any organization of which I am aware, except for start-ups (which usually have neither the time nor the money to afford quality). Since all new applications and safeguards must be introduced into existing environments, change management is the core of quality assurance.

I said earlier that one of the causes of flawed programs is poor change *control*. Change *management* is protection of a higher order. The first is a matter of procedure. Change management, however, begins with the rationale for change and, while including formal processes, promotes business benefit while minimizing the risk of disruption of services.[7] Effective change management leads to higher quality in all endeavors, including both programming and information security.

ENDNOTES

[1] Ross, Steven J.; "Microwave Software," *ISACA Journal*, vol. 1, 2015, *www.isaca.org/archives*. I was referring to software that is as old as my microwave—not as good as the new devices, but good enough for my needs.

[2] Dykstra, Edgar; *Notes on Structured Programming*, (EWD249), Section 3, April 1970, p. 7

[3] For just one example, the Target cybertheft in 2013 occurred at the interface of programming on a point-of-sale device and on a server on the retailer's network. One source states that "the average retailer has seven infections [presumably annually] communicating out from its network." Lemos, Robert; "Target Breach Involved Two-Stage Cyber-Attack: Security Researchers," *eWeek*, 21 January 2014, *www.eweek.com/security/target-breach-involved-two-stage-cyber-attack-security-reseachers.html*

[4] See "What Data Errors You May Find When Building A Data Warehouse," *www.dwinfocenter.org/errors.html.*

[5] The most infamous such data error was the Y2K bug. Today, people think that the whole thing was a hoax. They do not realize the billions of staff hours that were required to make sure that the bug did not bite. Was that a security problem?

[6] Stickel, Edward; "Change Control vs. Change Management: Moving Beyond IT," Technology Executives Club, *http://www.technologyexecutivesclub.com/Articles/management/artChangeControl.php*

[7] *Ibid.*

Helping Auditees Prepare for an IS/IT Audit

Ed Gelbstein, Ph.D., has worked in IS/IT in the private and public sectors in various countries for more than 50 years. He did analog and digital development in the 1960s, incorporated digital computers in the control systems for continuous process in the late 60s and early 70s, and managed projects of increasing size and complexity until the early 1990s. In the 1990s, he became an executive at the preprivatized British Railways and then the United Nations global computing and data communications provider. Following his (semi)retirement from the UN, he joined the audit teams of the UN Board of Auditors and the French National Audit Office. He also teaches postgraduate courses on business management of information systems.

Having been audited many times over the years, it would have been of great help if the auditors had taken the time to brief us on what they were going to do, why and how this would be done, and what our role in the process would be.

Many years later, having become an auditor, my choice was to make such briefings regular events, and, through them, it became apparent that many auditees did not really know what auditors do and were unfamiliar with audit terminology and methods of work.

These briefings made it clear that auditors are often seen as looking to criticize how things are done and make auditees look bad in the eyes of their senior management. To complicate matters, an organization's audit plan may require certain audits be done at a particular time that may not be convenient to auditees, as audits inevitably disrupt their work. This column suggests a way to facilitate the preparation for and conduct of an IS/IT audit.

> "Auditors are often seen as looking to criticize how things are done."

EXPLAINING THE AUDIT PURPOSE TO THE AUDITEES

There are examples of audit offices that have published brochures[1] explaining their role and the way audits are planned and conducted, but this may not be common practice. Too bad, because lack of understanding and clarity leads to a lack of trust before the audit has even begun and risks creating confusion about roles and responsibilities.

Auditors are accountable to senior management to provide independent and objective statements of the measures taken by auditees (whatever their role) to mitigate business risk. This implies that auditors are meant to examine, probe and challenge activities; obtain and evaluate evidence; and then report their findings and observations, including recommendations where necessary.

The internal auditors (including specialists who may be engaged for a particular audit) and the auditees work for the same organization, and, regardless of their perspectives, they should not be regarded as the enemy (but sometimes this is precisely how they are regarded).

Facts and dialog are vital components of any audit, and collaboration between auditor and auditee helps a great deal in ensuring that the final report, when produced, is a fair representation of the current status. Remember that auditors and auditees are human beings trying to do a good job.

NOT ALL AUDITS ARE THE SAME

A list of what *could* be audited is long, and, in practice, the most likely activities to be audited are those that link to significant business risk.

It is likely that if previous audits raised issues and included recommendations, the auditors will be interested in what has changed since these were made and may choose to re-audit some of them.

It can be assumed that documented and current business impact analyses, business continuity plans and risk assessments will be of interest to the auditors. Questions will be raised if these are incomplete, out of date or not available. Not a good start.

In addition, a short list of what could be audited would include:

- **Data center audits**—Including physical and logical security, process documentation and metrics. Of course, there is much more to this, including, for example, examination of controls at various levels (e.g., operating systems, applications, databases, networks, cryptography).
- **IS/IT process audits**—Often a COBIT® 5 -based audit, which includes the *COBIT® Process Assessment Model (PAM): Using COBIT® 5*[2] (It replaces the capability maturity model used up to COBIT® 4.1.)
- **Information security audits**—Focusing on the controls used to manage the availability, confidentiality and integrity of information
- **IS/IT systems development audits**—Focusing on the specification, development, testing, initial

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 loading, accreditation, and, in particular, security and business process controls

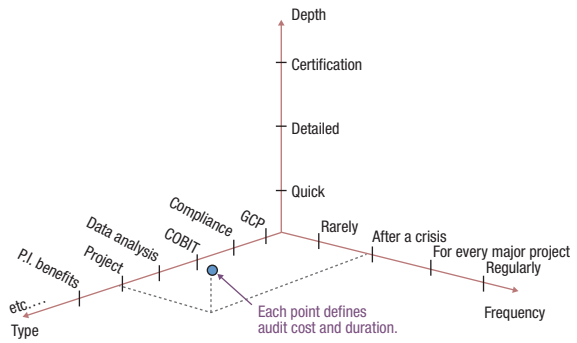
- **IS/IT large software projects audits**—Related to the previous item, but focusing on project management processes, change management and reporting (A series of columns on this topic is planned for future issues of the *ISACA® Journal*.)
- **Postimplementation benefits audits**—Occur once a project has been completed and has been operational for some time. These audits are intended to validate whether the benefits identified in the original business case for investing in the project have been achieved.
- **Business continuity audits**—To review the resiliency, recovery and other contingency plans prepared to restore an appropriate level of normalcy after a situation that heavily disrupts the organization's IS/IT facilities
- **IS/IT management/governance audits**—Particularly important when relying on external service providers (i.e., outsourcing and offshoring service providers). Such audits examine cost recovery or charging systems, budgeting and cost control, and organizational structure.
- **Change management audits**—Reviewing the procedures and systems used to control changes to infrastructure, software and the changes in relationships arising from organizational changes and/or the introduction of new technologies (such as bring your own device [BYOD])

And there are more areas of audits generally conducted by other, often external, auditors, such as those for compliance certifications (e.g., ISO 27001 or the Payment Card Industry Data Security Standard [PCI DSS]) and IS/IT strategy audits. This list excludes investigations because these require a different skill set and good knowledge of the legal requirements for collecting and preserving evidence in case the investigation leads to litigation.

Figure 1 illustrates the three dimensions of all audits: the type of audit, the depth of detail for which it aims and the frequency at which the audits are performed.

Each selection point has identifiable resource requirements, as well as a cost and duration—all of which support the audit planning process.

Figure 1—The Three Dimensions of Audit



Source: Ed Gelbstein. Reprinted with permission.

WHAT THE AUDITEES SHOULD KNOW ABOUT THE AUDIT PROCESS

Auditors are expected to know exactly how an audit is planned and executed, but auditees may not be in a position to share this knowledge and may find themselves poorly prepared. A presentation or brochure on the audit process should have concise descriptions of each stage:

- **Audit stage 1**—Notification to the auditee stating the purpose of the audit, who will conduct it and the target timing
- **Audit stage 2**—Scoping the audit, defining the areas to be covered and including a first list of documentation to be provided to the auditors
- **Audit stage 3**—Fieldwork consisting of interviews, site visits, documentation reviews and tests
- **Audit stage 4**—Reporting, ranging from discussions, a draft report, obtaining comments from the auditees, and exit conference and the issuance of a final report
- **Audit stage 5**—Following up at a later date to assess the progress made on issues identified in the report

Auditees should consider the following activities[3] immediately after receiving notification of an audit:

- Review the audit history and the status of past recommendations.
- Review the documentation relevant to the scope of the audit for completeness.
- Brief the team to be audited. The message: The auditors are not the enemy and they may help the IS/IT function raise issues with management.

- Prepare to treat auditors as team members: Exchange names, accompany them, share coffee breaks and lunches (at least from time to time), and provide them with adequate office facilities and support.
- Request clarifications whenever there is doubt or ambiguity in a question, request or statement.
- Request time to study the draft report findings and observations, and point out items that may not be an accurate description of the situation (providing facts, not opinions, to make the point).
- Participate in the exit conference and ensure that any points that need to be made are, in fact, made.

CONCLUSIONS

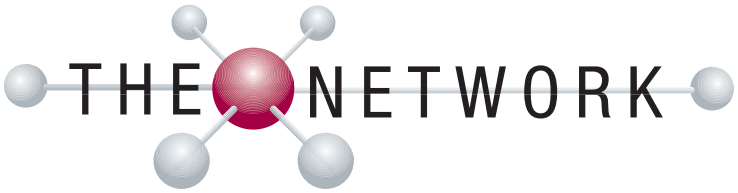
The topics discussed here are considered to be necessary, but not sufficient to ensure that the audit will be a collaborative exercise and that the auditees will approach the process in a positive manner. On the other hand, ignoring these points will likely result in a difficult audit.

ENDNOTES

[1] Office of Internal Audit, "Preventing, Detecting and Managing Fraud," South Carolina University, undated

[2] ISACA, *COBIT® Process Assessment Model (PAM): Using COBIT® 5*, USA, 2013, *www.isaca.org/COBIT/Pages/COBIT-5-PAM.aspx*

[3] Gelbstein, Ed; "Successful Audits Do Not Just Happen," *ISACA Journal*, vol. 2, 2015, USA, *www.isaca.org/archives*



Christos Dimitriadis

Christos Dimitriadis, Ph.D., CISA, CISM, CRISC, ISO 20000 LA, is the newly elected international president of ISACA® and group director of information security at INTRALOT in Athens, Greece. INTRALOT is a leading supplier of integrated gaming and transaction processing systems, game content, game management and interactive gaming services to state-licensed gaming organizations worldwide. Dimitriadis has served ISACA as international vice president for three terms; chair of the Knowledge Board, the External Relations Committee, and the COBIT® for Security Task Force; and member of the Strategic Advisory Council, the Relations Board, Academic Relations Committee, *Journal* Editorial Committee and review team, and Business Model for Information Security Work Group. Dimitriadis has served as a member of the Permanent Stakeholders Group (PSG) of the European Network and Information Security Agency (ENISA) from 2012 to 2015. Dimitriadis has received innovation awards from the European Lotteries Association, the John W. Lainhart IV Award from ISACA and the ISACA Presidents Award.

Q: *As ISACA's incoming international president and the group director of information security at INTRALOT Group, how do you see ISACA® growing and adapting to the constantly changing marketplace and needs of its constituents over the next year?*

A: Historically, information has always been invaluable, for people, societies, businesses and countries. Nowadays, information and communications technology (ICT) is the backbone of the world economy—a part of our daily lives. Through the gaining of more value from information and ICT, enterprises seek ways to become more effective, efficient, innovative and profitable. At the same time, balancing risk and value is closely coupled with stakeholder trust; it influences the viability of products, services and operations.

ISACA is an international leader in providing the tools for creating trust in and value from information and information systems, which subsequently act as business enablers serving professionals, enterprises and governments. ISACA is used to change and has learned to adapt quickly. It has mechanisms for being proactive, monitoring market trends and constituents' needs. With an international profile and multicultural structure involving passionate volunteers from all over the world who are experts in their domains and who are shaping the state of the art, ISACA has set up an active community of professionals who network, share opinions and learn from each other.

This will be an exciting year, putting all mechanisms to the test, providing more value to our members, constituents and their enterprises.

Q: *Can you briefly describe your role at INTRALOT? What in your past experience best prepared you for this position?*

A: I am responsible for information security, information compliance and intellectual property protection at INTRALOT Group, which has a presence in 57 jurisdictions on all continents. I run a global team that creates and monitors the execution of the enterprise security strategy and framework and is responsible for all types of certifications, external audit support and stakeholder trust in general. A few months ago, I was also given the responsibility of heading the office of the chief technology officer (CTO), managing transformational activities in the area of technology.

From my studies to my early work experience and the archievement of ISACA certification, every step added to my preparation for my current role, from learning how to write scientific reports to gaining a business perspective and working in a multinational environment.

Q: *What do you see as the biggest risk factors being addressed by information security professionals? How can organizations protect themselves?*

A: I wish there was a single answer to this question. In some cases, it is the difficulty for security professionals to speak a business language, leading to lack of buy-in from upper management. This, in turn, leads to incomplete, nonholistic solutions. At the same time, the threat landscape evolves very quickly, while attacks become more and more sophisticated. What adds to the risk is the lack of appropriate cybersecurity skills and framework implementation, underestimating the governance and human aspects.

In all cases, the need for a holistic framework that embeds information and cybersecurity in the business strategy is necessary to reach an understanding of priorities and help the enterprise achieve its goals.

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

A: Working as a security professional in a global, multicultural and rapidly evolving enterprise, with an open innovation culture, is a challenge I enjoy every day. Due to their holistic and multidimensional nature, ISACA frameworks helped me communicate the right messages, understand the diversity introduced by different cultures and, most important, understand how an enterprise operates. To appreciate security needs, I first needed to gain a holistic view of corporate conduct and business processes, enable innovation rather than limit it, and deploy information security and compliance as a contributor to realizing business goals.

However, I believe that the greatest challenges are ahead, both in becoming ISACA international president and in heading the CTO office of INTRALOT.

WHAT IS THE BIGGEST SECURITY CHALLENGE BEING FACED IN 2015? HOW SHOULD IT BE FACED?

The expanding cyberthreat landscape in combination with the lack of cybersecurity skills in the market. The public, private and academic sectors must invest more in creating skilled cybersecurity professionals.

WHAT IS YOUR FAVORITE BLOG?

ISACA Now

WHAT IS ON YOUR DESK RIGHT NOW?

Laptop, tablet, phones, coffee. No paper.

WHAT ARE YOUR THREE GOALS FOR 2015?

1. Do my best to serve ISACA and the professional communities it serves from my new position.
2. Write a success story on the recently constituted INTRALOT CTO office.
3. Get married.

WHAT IS YOUR NUMBER ONE PIECE OF ADVICE FOR OTHER RISK AND COMPLIANCE PROFESSIONALS?

Maintain a business mind-set, keep learning and welcome change.

WHAT DO YOU DO WHEN YOU ARE NOT AT WORK?

Travel with ISACA, kiteboard, snowboard, and spend time with friends and family

Cloud Application Enables ViralMint to Turn Potential Disaster Into Success

Siva Mandalam is vice president of products and strategy at Appcito, driving its cloud computing and security product vision, technology partnerships and go-to-market strategy. His expertise spans cloud, virtualization, application delivery control and security technologies. Prior to Appcito, Siva grew Cisco's security business to more than US $2 billion and ran F5 Networks' US $800 million ADC product line.

Rohan Dighe is the founder and chief executive officer of ViralMint. A product guy who loves building beautiful looking products on the social web, his entrepreneurial journey started in 2007 when he quit India's top digital agency to found a social apps development company.

Social media marketing firm ViralMint rolled out a new feature that proved so popular that the increased customer traffic swamped the capabilities of the existing load balancer solution and greatly increased application response times. Lacking visibility into the volume or nature of its traffic, ViralMint had no idea how to address its issues. A fortuitous conversation led to the discovery of the Appcito Cloud Application Front End (CAFE) service, which allowed ViralMint to gain control of its cloud application traffic, retain its customers' trust and build on its unexpected success.

UNEXPECTED SUCCESS THREATENS CORE BUSINESS

ViralMint is an onsite marketing platform that helps retailers harness social media marketing to boost their marketing return on investment (ROI): acquire new fans, increase sales, improve conversion and boost engagement. ViralMint's products—such as customized offers (e.g., coupons, discounts), a referral engine, exit targeting technology and on-screen promotions—depend on fast response times no matter how many customers are trying to access the ViralMint servers.

Founded in 2011, ViralMint was using the NGINX system as its load balancer and reverse proxy (i.e., an intermediary for one or more servers, allowing them to be contacted by any client) on its four application servers. This system worked fine initially, while traffic through the ViralMint servers was still relatively modest and predictable.

> "The popularity of the new feature was good news…until the unexpected traffic surge started affecting response times."

Recently, however, ViralMint added a new capability to its product suite that proved extremely popular with both active customers and many who had been dormant for some time. The popularity of the new feature was good news for ViralMint—until the unexpected traffic surge started affecting response times.

The NGINX system was not able to handle the increased load. Servers were dying and response times kept increasing. In addition, NGINX was unable to provide ViralMint with visibility into the incoming traffic, so the social media marketing company had no way to adequately plan its capacity to handle the influx.

GETTING BACK ON TRACK

The ViralMint team attempted all kinds of approaches to solving their problem. The team tried installing New Relic software analytics but could not get the correct plug-in installed. The New Relic software was providing status on ViralMint's control processing unit (CPU), memory and disk space; however, these were the least of their concerns at that time.

The team looked at the query time in their database server and found it to be normal. They found that when the server was placed independently, response time was fine. But when the server was placed behind the load balancer, response time skyrocketed.

ViralMint's founder and CEO, Rohan Dighe, mentioned his company's difficulties to a friend, who is also a product manager at Appcito. The friend suggested that the Appcito CAFE service might be what ViralMint needed. The Appcito CAFE service is a unified and cloud-native service that combines advanced load balancing and content-switching capabilities with integrated performance, security and continuous deployment services, as well as an insights engine that delivers fine-grained visibility into cloud application health and performance.

After some initial investigation, the decision was made to try the CAFE service. Using the CAFE Barista management module, it took only five minutes to set up and provision the as-a-service CAFE solution.

Immediately, CAFE provided the ViralMint team with the visibility to see what needed to be done—as well as the tools to act. Able to distinguish wanted from unwanted traffic, CAFE stopped spurious traffic, provided an

accurate picture of all the incoming traffic, and enabled ViralMint to estimate the correct number of application servers needed and provision them quickly.

Appcito CAFE enabled ViralMint's existing staff to deploy advanced cloud application delivery capabilities with minimal effort or additional training. The CAFE service's autoscaling capabilities, even with multiple instances, meant that load balancing was no longer a bottleneck in ViralMint's operations. ViralMint expanded from four to 10 application servers and was comfortably handling more than eight million requests per day with fast response times.

As a result of the Appcito CAFE service, ViralMint was able to retain the new customers attracted by its new feature, as well as attract additional customers. ViralMint and its customers are now confident in the availability of its products and services to share information, capture reviews and deliver offers—all with fast, predictable response times.

Enjoying this article?

- Read *Controls and Assurance in the Cloud: Using COBIT® 5*.

  www.isaca.org/controls-and-assurance-in-the-cloud

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

  www.isaca.org/topic-cybersecurity

The Lure: The True Story of How the Department of Justice Brought Down Two of the World's Most Dangerous Cyber Criminals

By Steve Schroeder

Reviewed by A. Krista Kivisild, CISA, CA, CPA, who has had a diverse career in audit while working in government, private companies and public organizations. Kivisild has experience in IT audit, governance, compliance/regulatory auditing, value-for-money auditing and operational auditing. She has served as a volunteer instructor, training not-for-profit boards on board governance concepts; has worked with the Alberta (Canada) Government Board Development Program; and has served as the membership director and CISA director for the ISACA Winnipeg (Manitoba, Canada) Chapter.

On a day in late November 1999, the system administrator for an Internet cafe in Seattle, Washington, USA, was about to perform some housekeeping, when he received a message that popped up in his command-line interface from someone who inquired about the system's security and asked him to Internet Relay Chat (IRC) on the subject. What followed over the next three years was an investigation to identify who was responsible for sending this message; determine what other businesses they targeted; and, eventually, lure those responsible onto American soil to obtain enough evidence of the crimes committed, ultimately resulting in a trial, conviction and eventual sentencing. *The Lure: The True Story of How the Department of Justice Brought Down Two of the World's Most Dangerous Cyber Criminals* is the story of these events and the case that would become a sensation among IT professionals and law enforcement agents, as told by the lead prosecutor in the trial.

What makes this book a compelling read is the detail and breadth of knowledge the author used to paint a picture for the reader about what led to the initial event and the world's approach to security and computer crime in the US at the time these crimes occurred. The story reads like a prosecutor presenting the case to a jury. The readers get the complete story of the different hacking activities conducted at various companies, actual testimony from witnesses during the trial and evidence from the government's exhibits supporting the case. Along this entertaining journey, the reader is educated on the history of computer crime and prosecuting such crimes in the US. While many people may know some aspects of this event and subsequent trial, Schroeder is able to provide a more complete picture of the attacks, which could be particularly beneficial to today's generation of young professionals who have always lived in the world of the Internet.

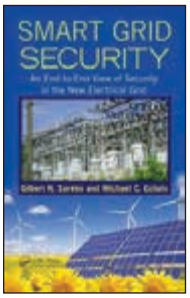
The reader is led through the discovery of how many companies were hacked, the involvement of the hackers, who was really in charge of these hacks and the details of the crimes committed. Readers also learn the reality of trying complex cases in a court, and this book provides much of the information jurors for this case would have seen. This book allows readers to see the complete investigation process, which is especially useful for those involved in only a portion of an investigation, such as security/audit, governance and controls, or compliance.

Interestingly, the method of operation of the hackers really was not much different than approaches used today—a random phishing expedition targeting those companies whose weaknesses were found and exploited. The only difference is that one could argue today this type of activity can be carried out with a much wider net and using different tools, such as social media, to identify potential targets.

The Lure is an interesting jaunt through computer crime and hacking history in the US. This book entertains as well as educates the reader. If the US is not the reader's area of practical focus, the book may be of slightly less interest. However, it still offers a highly entertaining, informative and captivating read.

EDITOR'S NOTE

The Lure: The True Story of How the Department of Justice Brought Down Two of the World's Most Dangerous Cyber Criminals is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.



By Gilbert N. Sorebo and Michaels C. Echols

Reviewed by Dino Ippoliti, CISA, CISM, an expert consultant at inspearit. He has been a practitioner in information and computer security, IT system auditing, and software and system engineering process improvement for more than 17 years in multiple industries. He is a member of the ISACA Publications Subcommittee and a mentor in ISACA's Pilot Mentoring Program.

Smart Grid Security: An End-to-End View of Security in the New Electrical Grid

What is a smart grid? There is no singular definition, but *Smart Grid Security: An End-to-End View of Security in the New Electrical Grid* describes it as "the idea of integrating enhanced communications technologies with enhanced decision making and automation of actions, both centrally and in the field."

As components of the smart grid have to be deployed in big areas and to so many users, they need to be cheap and able to make the best use of their computing power to ensure the reliable delivery of energy. Therefore, traditional security mechanisms and approaches are not applicable.

This unique security challenge is part of what makes *Smart Grid Security* so valuable to information security professionals. The book provides an overview of the smart grid and addresses security concerns associated with it. *Smart Grid Security* comprehensively covers what information security professionals need to know, including:

- An overview of smart grid concepts, security concerns, and the US legal and regulatory environment (chapters 1 and 2)
- A description and analysis of the most important security concerns and possible solutions related to smart grid components, e.g., advanced metering infrastructure (AMI), home area network (HAN), distribution and transmission, distributed generation, and operations (chapters 3-8)
- A look at the future, addressing topics including energy storage, the consumer relationship, recovering from cyberdisaster and speculation on future cybersecurity challenges (chapters 9-12)

The authors provide readers with basic information on the technical and business context of the smart grid so that even a security professional who does not have any previous experience in the energy sector could enjoy and benefit from reading this book. Although the book focuses on the US organizational and technological context, readers from across the world can benefit from the experience of the authors and the effectiveness of their explanations.

Most important, the book clarifies the differences and the challenges that security professionals face when IT technologies are used for automation and management of critical infrastructure, such as the energy grid. While this book is smart-grid-specific, many of these same challenges present themselves whenever IT technologies are used to enhance or substitute traditional technologies.

One of the most critical issues when creating a smart grid is likely to be the cultural gap between a professional from the energy grid sector, who does not understand IT technologies, and a professional from IT security, who has little knowledge and understanding of the energy grid. This can endanger business objectives and smart grid reliability in two different ways: Security threats may be dangerously underestimated, leading to security incidents. Or, in contrast, too much emphasis may be placed on security threats, thus increasing energy cost or decreasing smart grid infrastructure reliability.

To successfully protect smart grids from cyberthreats, it is necessary for security professionals to fully understand both the business and the technological contexts in which they are going to operate, especially because these contexts might be different from those encountered in most IT organizations. Because of this necessity, *Smart Grid Security: An End-to-End View of Security in the New Electrical Grid* is certainly a useful tool for security professionals interested in embarking on the smart grid security challenge.

EDITOR'S NOTE

Smart Grid Security: An End-to-End View of Security in the New Electrical Grid is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

Feature

Vendor Risk Management Demystified

Dipti Patel, CISA, CISM, ISO 27001 LA, ITIL V3, is a security consultant at Tata Consultancy Services, a leading IT services company with worldwide experience in information security and cyberresilience. Patel brings an excellent understanding of governance, risk and compliance (GRC) aspects and is a follower of trending GRC concepts and techniques. She can be reached at *diptiapatel@gmail.com*.

Also available in Japanese
日本語版も入手可能

Outsourcing is often a default strategy for today's businesses. While it has huge potential benefits to offer enterprises, outsourcing has also given rise to security threats that are persistent, large-scale and devastating. In the past two years, sophisticated cyberadversaries have launched powerful attacks through vendor networks/connections and siphoned off money, millions of credit card records and customers' sensitive personal information.

There has been a noticeable jump in those organizations that attribute security incidents to current service providers and contractors (23 percent) and former partners (45 percent).[1] Changes in targets and threats outside the enterprise are shaping the current and near-future risk landscape. Looking at these anticipated changes in a strategic manner will enable security and risk leadership to unearth new opportunities while managing this emerging risk. Thus, it is clear that enterprises require adequate oversight of vendor security risk as part of a comprehensive cyberrisk management policy.

THE HEART OF THE MATTER

Most people did not expect that connectivity with vendors would result in exploits on retailers, many of which would go unnoticed for several months. Very few risk management programs would have considered such a risk, which is not only large impact but also hard to predict. Such events were rare and typically beyond the realm of normal expectations.

Attackers, organized cybercriminals and some nation-states have captured news headlines as a result of high-profile security breaches. Almost one-third (32 percent) of respondents to a PricewaterhouseCoopers survey said that insider crimes are more costly or damaging than incidents perpetrated by outsiders.[2] Most people know that employees are not the only source of insider threat; insider threat can also include former employees, service providers, consultants, contractors, suppliers and business partners.

Verizon labeled 2013 "the year of retailer breach." There were 467 retailer breaches worldwide. Massive breaches were seen again in 2014, once again targeting credit card data, personal information, sensitive health records and financial information.[3] Large-scale heists of consumer data were reported in South Korea, where 105 million payment card accounts were exposed in a security breach.[4] In Verden, Germany, city officials announced the theft of 18 million email addresses, passwords and other information.[5]

Regulators around the world are climbing on the bandwagon of tightening vendor security. Regulators are revisiting their guidelines on vendor security and are directing organizations to increase their focus on vendor risk as organizations continue to expand the number and complexities of their vendor relationships. For example, the US Office of the Comptroller of the Currency (OCC) and the Board of Governors of the US Federal Reserve System released updated guidance on the risk management of third-party relationships. This guidance signals a fundamental shift in how financial institutions need to assess third-party relationships. In particular, it calls for robust risk assessment and monitoring processes to be employed relative to third-party relationships and specifically those that involve critical activities with the potential to expose an institution to significant risk.[6]

Enterprises must elevate their vendor-related security practices to keep pace with ever-evolving threats and security needs.

TAKING ACTION ON VENDOR SECURITY GOVERNANCE

Given today's interconnected business ecosystem in which exponentially more data are generated and shared with suppliers and business partners, the lack of risk oversight and due diligence regarding third parties is concerning. Vendor risk oversight from a security point of view will demand a program that covers the entire enterprise—outlining the policy and guidelines to manage and

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:

mitigate vendor security risk—combined with clearly articulated vendor contracts.

Such oversight will not only help organizations improve cybersecurity programs but also potentially advance their regulatory and legal standing in the future. The following six steps can help organizations start their vendor security governance policy (**figure 1**):

Figure 1—Vendor Risk Management Program and Components

Source: Dipti Patel. Reprinted with permission.

1. **Executive oversight**—Executive alignment and business context is critical for appropriate implementation throughout the organization. Proper alignment is like a command center, providing the required policies, processes and guidelines for the program. The decision to outsource is strategic and not merely a procurement decision. It is, therefore, of the utmost importance that executive committees provide direction for the vendor risk management program. The program should obtain executive guidance from:
   - The compliance function to provide regulatory and other compliance requirements that have specific rules regarding vendor risk management to which the organization must adhere
   - The IT risk and control function to determine the risk and the risk level, depending on the nature of access/data sensitivity shared with the vendors. The vendor risk management program should utilize the key risk indicators provided by this function to address risk during assessments.
   - The contract governance function to ensure that vendor contracts adequately address the need for security assessments and vendors' obligations to complete these assessments
2. **Vendor and contract database**—Most organizations today deal with a considerable amount of third parties and service providers. Missing contact information, responsibility matrices or updated contracts are typical areas of concerns for which risk managers would have to initiate assessments. This poses a significant challenge, especially when there are multiple teams involved for procurement purposes. A vendor and contract database (VCD) ensures that an accurate and complete inventory of vendors is maintained, including other third-party relationships (e.g., joint ventures, utilities, business partners, fourth parties).
3. **Assign trust level**—For the vendor risk management program to be effective, one cannot conduct the same type of risk assessment for all vendors. Rather, it is necessary to identify those vendor services deemed to carry the greatest risk and prioritize them accordingly. The first step is to understand which vendors and services are in the scope from an active risk management perspective. Once this subset of vendors has been identified and prioritized, due diligence assessments are performed for the vendors, depending on the level of internal versus vendor-owned controls. The results of these assessments help establish the appropriate trust-level rating (TLR) and the future requirements in terms of reassessments and monitoring. This approach focuses resources on the vendor relationships that matter most, limiting unnecessary work for lower-risk relationships. For example, a vendor with a high TLR should be prioritized over a vendor with a low TLR.

4. **Security assessment**—Proper control and management of vendor risk requires continuous assessments. It is important to decide the types of assessments to be performed on vendors depending on the TLR and frequency. **Figure 2** provides an example of assessment types that can be included in a program.

Figure 2—Assessment Types Based on TLR

Trust-level Rating (TLR)	Assessment Types
Low	Vendor self-assessment
Moderate	Desktop review, infrastructure assessment
High	Onsite review, infrastructure and application assessment

Source: Dipti Patel. Reprinted with permission.

As a good practice, areas of assessment could be drawn from security standards and practices (e.g., ISO 27001, COBIT®, OWASP) combined with specific compliance requirements (e.g. Payment Card Industry Data Security Standard [PCI DSS]) as applicable.

5. **Validate trust level**—Outsourced relationships usually go through iterations and evolve as they mature. As the client organizations strategize to outsource more, they should also validate trust level in anticipation of more information and resources being shared. With technological advancements, a continuously changing business environment and increased regulatory demands, validating trust level is a continuous exercise. To get the most rational and effective findings, it is best to use the results of ongoing assessments.
6. **Monitor and report**—In a reiterative process, it is necessary to continuously monitor and routinely assess vendors based on the trust level they carry. The program should share information about the vendor security posture and risk levels with an executive sponsor, who can help the organization progress toward the target profile. Narrating risk with the business perspective can be an additional feature, especially when reports are furnished to inform internal stakeholders, internal audit functions, lines of business and the board of directors, if necessary.

CONCLUSION

Vendor risk management is the next step to elevate information security from a technical control process to an effective management process. Regular security assessments of vendors give organizations the confidence that their business is aware of the security risk involved and is effectively managing it by transferring, mitigating or accepting it. Comprehensive vendor security assessments provide enterprises with insight on whether their systems and data are being used consistently with their security policies.

Vendor risk management is not a mere project; it is an ongoing program and requires continuous trust to keep the momentum going. Once the foundational framework has been established, organizations can look at enhancing maturity through initiatives such as improving guidelines and procedures, rationalizing assessment questionnaires, and automation. Awareness and communication are key to ensure that the program is effective and achieves its intended outcome—securing enterprises together with their business partners and vendors.

ENDNOTES

[1] PricewaterhouseCoopers, "Managing Cyber Risks in an Interconnected World. Key Findings From The Global State of Information Security Survey," 2015, *www.pwc.com/gx/en/consulting-services/information-security-survey/*

[2] *Ibid*.

[3] Verizon, 2014 Verizon Data Breach Investigations Report, *www.verizonenterprise.com/DBIR/2014/*

[4] *Op cit*, PricewaterhouseCoopers 2015

[5] Brewster, Thomas; "Germany Investigating Data Breach Affecting 18 Million," *TechWeek Europe*, 7 April 2014, *www.techweekeurope.co.uk/workspace/germany-id-theft-18m-143269*

[6] Office of the Comptroller of the Currency, "OCC Bulletin 2013-29. Description: Risk Management Guidance," USA, *http://occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html*

Vendor Governance in the Age of Information Security

Arian Eigen Heald, CISA, CGEIT, CEH, CISSP, GCFA, is leading BerryDunn's government consulting information technology security practice, with more than 22 years in IT. She is the subject matter expert for information security at BerryDunn and a regular speaker on the topic at conferences. She has written a blog for *TechTarget* and is a frequent author on *berrydunn.com*.

From businesses to government agencies, nearly every entity contracts some aspect of software development, system integration and hosting services—creating an emerging crisis in accountability.

How does an organization that has an IT department with average skills implement a large, complex, far-from-average new technology, such as electronic health records or asset management systems? In this age of specialized skill sets, it seems perfectly sensible to outsource such a deployment. Managing how to secure the confidential data contained within the new technology—and the welter of regulatory requirements that must be met to do so—is one of the most important and underappreciated challenges of this decade.

With hundreds of frequently overlapping security requirements, it can seem deceptively simple to contractually require that the vendor be compliant with all the appropriate regulations. What cannot be overlooked, however, is that the contracting organization must have sufficient resources to provide adequate oversight of vendor compliance activities.

RESPONSIBILITY CANNOT BE OUTSOURCED

Whether the vendor is developing and integrating new technology that the organization will maintain or the vendor is also hosting the new technology, the compliance requirements for securing confidential data are the same.

In the US, for example, federal regulations require that even if a vendor agrees to provide security services, the owner of the data be responsible for ensuring that the vendor protects the data.

Though a vendor may be the source of a data breach, in the court of public opinion, the negligent party is the entity that has contracted the services of an inadequate vendor.

For example, in the case of the Target breach, the name of the third-party vendor that was the source of the breach was eventually identified, but the breach itself was publicized as, "Target has been hacked." At Target's highest management levels, heads rolled and the company's bottom line took a major hit.

The accountability and compliance crisis goes far beyond the retail world, touching all industries: commercial, not-for-profit and, perhaps most urgently, government.

FEDERAL FUNDING TRIGGERS FEDERAL COMPLIANCE STANDARDS FAR AND WIDE

Although US state, city and town agencies are not federal entities, by accepting federal funding, they must meet federal standards to connect to federal sources of information, such as the US Internal Revenue Service (IRS), the US Social Security Administration, and the US Department of Health and Human Services (HHS). The funding of these systems has fueled the implementation of these standards.

Correspondingly, many business and nonprofit entities that provide services to cities and states based upon confidential information are finding that they are contractually required to become compliant with such standards in order to continue doing business with these government entities.

Over the past five years, the US National Institute of Standards and Technology (NIST), Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*,[1] has emerged as an information security standard for compliance among US state and local government entities.

Regulations such as the US Health Insurance Portability and Accountability Act (HIPAA), the US Affordable Care Act (ACA), and the US Federal Information Security Act (FISMA) have had additional impact on IT security controls for personal health information (PHI). IRS Publication 1075 is a complementary set of standards for federal tax information (FTI).

In the rollout of the new health insurance exchanges across the US, the Center for Medicaid and Medicare Services (CMS) has mandated the

use of NIST SP 800-53 for those state entities choosing to accept funding. The latest set of compliance requirements (the CMS *Minimum Security Requirements, or MARS-E, Minimum Acceptable Risk Safeguards for Exchanges*[2]) maps directly to NIST SP 800-53. These standards are now being attached to funding to update or implement new Medicaid management information systems (MMIS) and eligibility systems run by states across the country.

Commercial and nonprofit support services for these new and updated health systems are feeling the trickle-down effect of these mandates when contracting entities require periodic inspection of their controls to determine if they are compliant.

One of the requirements specifically called out by the CMS and the IRS has been for those entities to have periodic independent third-party security assessments. These and other assessments have revealed critical and persistent challenges involved in managing the complexity of third-party contracts for services.

THIRD-PARTY ASSESSMENTS REVEAL GAPS IN THE GOVERNANCE PROCESS

Governance problems become visible when mandated independent security assessments examine vendor practices. The most frequent findings appear in these NIST-designated areas:

- Secure software development (SA)
- Access controls (AC)
- Configuration management (CM)
- Logging and monitoring (AU)

These areas map to the following gaps in governance activities by the contracting organization:

- Lack of resource planning for sufficient technical oversight
- Limited in-house knowledge of the security requirements for the new technology
- Over-reliance on generic contract language for technical compliance requirements

A new technology compounds existing problems. Layers of technology continue to increase, creating more layers of security risk. Virtual technologies, for instance, have added the ability to build out incredibly powerful operating systems in a far smaller physical space. These technologies make possible a security breach much bigger than the compromise of one server. Compromise of the hypervisor (the virtual machine host managing the virtual operating systems) can mean that the hacker has access to all the servers and data inside that virtual system.

As new products are deployed, there is more chance for documentation of security features to be minimal or rushed, and existing documentation can quickly become outdated. For example, service-oriented architecture (SOA), with its certificate architecture for authentication, can become a black hole for compliance analysis. For a contracting organization, lack of documentation can mean being held captive to a vendor and expensive consulting fees.

Project risk assessments have not adequately captured many aspects of vendor oversight, including managing the development, test and production system rollouts. It is not uncommon for vendors to have unfettered control over all aspects of the new development, test and production systems, often denying the contracting entity any access.

> “Vendors scramble to get code to work on a deadline or to fix emergencies, too often at the expense of security.”

This allows code to be created in undocumented systems that will be more likely to have problems in a secure production environment. Vendors scramble to get code to work on a deadline or to fix emergencies, too often at the expense of security. The risk brought about by this deeply engrained pattern in this outsourcing culture cannot be overestimated.

MORE OUTSOURCING MAY HELP SOLVE OUTSOURCING PROBLEMS

Contracting organizations often struggle with the question of how to better monitor their vendors. Many are not prepared to assign in-house engineers who already have significant duties to provide oversight of vendor activities. Often, the reason organizations turn to outsourcing in the first place is that their employees have insufficient expertise to understand all aspects of the technology. Even organizations trying to monitor their vendors may not be set up to handle the necessary level of reporting duties. Front-line technical personnel often do not have sufficient access to higher-level project managers to report problems.

Ironically, the solution to outsourcing problems may be more outsourcing. In the same way an organization outsources for technology development and deployment expertise, it may need to consider whether to outsource technical compliance from an independent party that has no relationship with the vendor.

This establishes segregation of duties (SoD) so that the secure development and implementation of the systems and software underlying new technology are adequately protected. Rather than waiting for a security assessment just prior to, or just after, rollout into production, contracting organizations would be better served by implementing continuous monitoring throughout the project.

IMPROVING VENDOR GOVERNANCE

Improving vendor governance may require a shift in priorities or culture for the contracting organization. The security challenges discussed previously generally manifest themselves in five distinct areas where the contracting organization can take steps for better oversight:

1. **Recalculate the risk and cost of secure software development.** For many, especially cash-strapped government agencies, cost has been the limiting factor for providing sufficient vendor oversight. Today's rising incident rates for data breaches, coupled with increased regulations, call for a fresh look at the cost-benefit analysis of putting more resources into vendor oversight.

   Both the NIST and the US National Aeronautics and Space Administration (NASA)[3] have completed studies on the differences in cost for remediating code errors during the different phases of software development. The studies revealed that it can cost up to 30 times more to resolve code errors once the product is in production status.

   The Ponemon Institute's ninth annual report, *2014 Cost of Data Breach Study: Global Analysis*,[4] highlights the fact that the average cost for each record lost or stolen increased from US $136 to $145 (9 percent) from the previous year. The longer the delay in implementing and overseeing secure software development, the higher the cost when the breach occurs.

   In addition to data breach record costs, there is significant compliance risk[5] in not providing sufficient oversight of vendor activities, as is required in CMS' MARS-E, FISMA and IRS 1075[6] regulatory documents. For example, one of the requirements from SP 800-53 is SA-10 Developer Configuration Management:

   > *The organization [meaning the contract holder] requires the developer of the information system, system component, or information system service to:*
   > *a. Perform configuration management during system, component, or service development, implementation, and operation;*
   > *b. Document, manage, and control the integrity of changes to configuration items under configuration management;*
   > *c. Implement only organization-approved changes to the system, component, or service;*
   > *d. Document approved changes to the system, component, or service and the potential security impacts of such changes; and*
   > *e. Track security flaws and flaw resolution within the system, component, or service and report findings to defined personnel or roles (defined in the applicable security plan).*[7]

2. **Mandate secure software development.** Security controls should be built into every phase of software development, regardless of which software development model the vendor uses. NIST provides an excellent template in its Special Publication 800-64, *Security Considerations in the System Development Life Cycle*.[8]

   Although a system integrator may take on the task of building out the infrastructure (e.g., servers, databases, virtual hosts, routers) to support the new application, this type of vendor's primary focus is to develop a software product that meets the requirements of the client in the most cost-effective way possible.

Unfortunately, cost-effective does not necessarily translate into secure. In many third-party environments, security is a much-delayed add-on, and documentation is focused primarily on application development and meeting business requirements.

One could say that it is an occupational hazard that IT vendors want to implement infrastructure in a way that is most conducive to software development. The fastest approach for software development is when the applications have complete access rights to all data. Fortunately, regulatory requirements mandate better controls, but if the contracting entity does not mandate secure development systems and detailed access control documentation of the systems, it risks a disaster. The application could break in a locked-down production environment or be hacked due to lack of controls in an open one.

These requirements should be put into place upon commencement of the contract and not applied in the final deployment into production, where it is far more costly to resolve.

How a software developer builds the development environment is critical to the delivery of a secure application and infrastructure.

3. **Maintain access controls.** With adequate resources, a contracting entity can better ensure that vendors implement compliant controls and develop secure software that meets business requirements. Vendors ought not to be allowed to develop in a security vacuum where use of generic administrator identifications (IDs) is the norm and password controls are minimal.

   When new systems are first booted up for the initial development environment, the vendor should have a documented server build ready for deployment. The contracting entity should provide oversight for the standard build to confirm that security engineering principles form the backbone of the development environment.

   For example, the NIST SP 800-53 Control SA-8 *Security Engineering Principles* offers the following guidance:

   Security engineering principles include, for example:
   - *Developing layered protections;*
   - *Establishing sound security policy, architecture, and controls as the foundation for design;*
   - *Incorporating security requirements into the system development life cycle;*
   - *Delineating physical and logical security boundaries;*
   - *Ensuring that system developers are trained on how to build secure software;*
   - *Tailoring security controls to meet organizational and operational needs;*
   - *Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and*
   - *Reducing risk to acceptable levels, thus enabling informed risk management decisions.*[9]

   The contracting entity should require and maintain administrative access to all development, test and production systems. If the vendor has implemented proper logging and monitoring of access, any unauthorized changes should be easily tracked to the source of that activity.

   It cannot be overstated that the contracting entity, not the vendor, is the owner of those systems and must maintain control. The vendor must never control the systems to the exclusion of the data owner. The simplest way to achieve this is to always have administrative access to the systems from the very beginning of the project.

   Equally, the contracting entity must maintain ownership of the code that is being developed because it is a form of intellectual property for which the entity is paying. Therefore, consistent and complete access to the vendor's code repository provides for continued possession and allows the entity to monitor the vendor's controls over the code.

   Using PHI, personally identifiable information (PII) and federal tax information (FTI) data in development environments often helps to develop code that will eventually use these data. However, maintaining access

controls over who sees the data is the responsibility of the data owner, not the software developer.

Products in the marketplace can obfuscate confidential data for testing purposes, but many organizations find them cost-prohibitive. With adequate controls over access, waivers from federal entities (the IRS, in particular) can be obtained.

SoD is often nonexistent in development environments and, quite frequently, in production environments. Software developers should not have any more than read-only access to production environments. Database administrators should not have server administrator rights and vice versa. Implementing these controls in the development environments means that systems are managed more securely from the beginning of the project.

Some vendors resist this approach, claiming that it could create security problems when the code is moved into production, but the reverse is actually true if the development systems are configured securely.

4. **Start configuration management from the beginning.** In the eyes of NIST, the IRS and FISMA, "configuration management" has become an umbrella term that incorporates a range of activities, including:
   - Documented baseline configurations based on national standards
   - Implementation of least functionality
   - Change control management
   - Information systems component inventory
   - Testing of changes prior to deployment
   - Security impact analysis of changes
   - Access restrictions for changes
   - Software usage restrictions

   Generally, these requirements have not been addressed until much later in a project. As a result, undocumented changes, unpatched systems and a lack of standardization lead to the contracting organization not having firm control over the security architecture.

   Patching and updating critical system components that work in layers can lead to expensive crashes and downtime when systems are not configured to a single standard across the architecture. A patch may work perfectly on one Linux server and fail on the next because someone made a change to the server that was not documented. When this is replicated across more than 200 servers, the cost to managing updates can become prohibitive and lead to insecure systems.

   Monitoring changes on systems is much easier when a common standard is implemented. Small changes can also be the first alert of a data breach in progress.

   Monitoring system changes is a core element in meeting, for example, the NIST requirement in AU-2 Audit Events:

   > *Generate audit records for the following events in addition to those specified in other controls:*
   > *a) All successful and unsuccessful authorization attempts.*
   > *b) All changes to logical access control authorities (e.g., rights, permissions).*
   > *c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services.*
   > *d) The audit trail shall capture the enabling or disabling of audit report generation services.*
   > *e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).*[10]

5. **Control logging and monitoring.** Possibly the largest security gaps exist in the areas of logging and monitoring. In implementing security controls, contracting organizations often focus on product performance and delivery to the detriment of security controls.

   It is common practice for the contracting organization to require the vendor to perform all monitoring of the new systems. Unfortunately, this usually means that the organization expects the vendor to monitor vendor administrative activities. This is an obvious conflict of interest for the vendor and is in direct conflict with security best practices.

   Consider the NIST SP 800-53 Audit and Accountability (AU) control AU-9(4) Access by a Subset of Privileged Users:

> *The organization* [the contracting entity] *authorizes access to management of audit functionality to only those individuals or roles who are not subject to audit by that system, and is defined in the applicable security plan."*

Reasonably, the organization would want to retain control of audit logs that may contain confidential information, in order to determine whether the vendor is performing activities that are compliant with federal requirements. Logs can be stored at a vendor location without the vendor having access, beyond read only, or can be transferred to another location.

Alternately, another third-party vendor could be engaged to perform monitoring activities as long as that party reports to the contracting organization, not to the vendor performing the administrative activities.

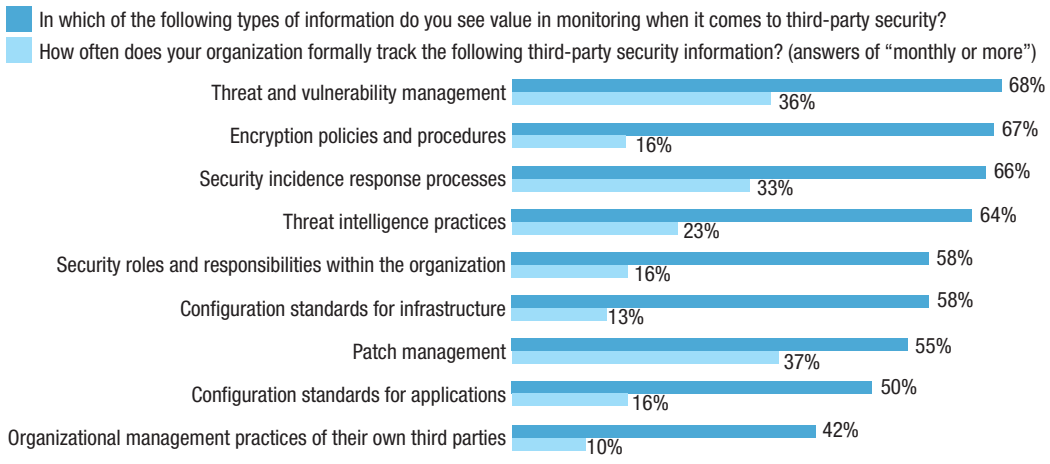
This is not to say that the vendor should be exempt from monitoring application and performance logs. It is simply a matter of SoD, so that system administrators and database administrators are not in charge of monitoring their own actions.

> Should a contracting organization allow another group within the vendor organization to monitor their own administrative activities? There may not be sufficient SoD to be an effective practice. The vendor can overrule or delay security findings if kept to an internal group. Also, it is less likely that such decisions are transparent to the contracting organization.

Audit logs, when implemented according to requirements, are the backbone of security prevention, detection and response.

An Incident Response Plan[11] provides a process for responding to security incidents that are found in logs. Whether malware, failed logins or distributed denial of service (DDoS) attacks, there should be a process for performing an initial analysis, documentation, prioritization and notification. The contracting organization should ensure that a formal, detailed plan is in place for preparation, detection and analysis, containment, eradication, and recovery that is compliant with federal requirements and details actions, as well as reporting activities, for the vendor to incorporate.

Figure 1—Current Practices Related to Monitoring and Managing Third-party Risk



Base: 106 IT decision-makers at enterprises in the US, UK, France and Germany.

Source: BitSight Technologies, a commissioned report conducted by Forrester Consulting, November 2014. Reprinted with permission.

CONCLUSION

In October 2014, BitSight Technologies commissioned Forrester Consulting to examine the current practices of IT decision makers as they relate to monitoring and managing third-party risk. The resulting report,[12] released in January 2015, found that "there is significant appetite for monitoring various elements of third-party security, yet few firms have the resources to do so with adequate frequency or objectivity"[13] (**figure 1**).

> "How resources are applied during major technology initiatives and improvements can be the difference between a secure system and one that is constantly subject to problems."

The challenge of applying good security practices is greater than ever. How resources are applied during major technology initiatives and improvements can be the difference between a secure system and one that is constantly subject to problems.

In addition to meeting security requirements, the core areas discussed in this article lead to reliable systems. Problems are more likely to appear when controls are not in place. They also become extremely difficult to track and resolve. Without solid security principles, undetected breaches are more likely to occur.

The time and effort taken during the beginning of a project to use secure standards will result in significant savings—of money, time and trouble—throughout the life of the technology.

ENDNOTES

1 National Institute of Standards and Technology (NIST), *Security and Privacy Controls for Federal Information Systems and Organizations*, USA, April 2013, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

2 Centers for Medicare and Medicaid Services, CMS Information Security Acceptable Risk Safeguards, USA, 20 September 2013, *www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ARS.pdf*

3 NASA Johnson Space Center, "Error Cost Escalation Through the Project Life Cycle," National Aeronautics and Space Administration (NASA), *http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20100036670.pdf*

4 IBM, *"2014 Cost of Data Breach Study,"* Ponemon Institute, *www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/*

5 Compliance risk is the risk of legal sanctions, material financial loss or loss to reputation that the organization may suffer as a result of its failure to comply with laws and regulations.

6 Internal Revenue Service, Publication 1075, *Tax Information Security Guidelines for Federal*, State and Local Agencies, USA, October 2014, *www.irs.gov/pub/irs-pdf/p1075.pdf*

7 *Op cit*, NIST 2013

8 National Institute of Standards and Technology (NIST), *Security Considerations in the System Security Life Cycle*, USA, October 2008, *http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf*

9 *Op cit*, NIST 2013

10 *Ibid*.

11 See NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide* for an excellent template.

12 BitSight Technologies, *Continuous Third-party Security Monitoring Powers Business Objectives and Vendor Accountability*, January 2015, *http://info.bitsighttech.com/continuous-third-party-security-monitoring-powers-business-objectives*

13 *Ibid*., p. 3

Three Ways to Simplify Auditing Software Security Requirements and Design

Rohit Sethi, CISSP, CSSLP, is a specialist in software security requirements. In his current role, Sethi manages the SD Elements team at Security Compass, where he has worked with many of the world's most security-sensitive organizations on software security. Sethi has appeared as a security expert on several television networks, including CNBC and Bloomberg, and spoken at numerous industry conferences such as RSA and OWASP.

Ehsan Foroughi, CISM, CISSP, is an application security expert with more than 10 years of security experience. He leads product management at Security Compass. Previously, he led the Vulnerability Research Subscription Service for TELUS Security Labs.

Also available in Japanese
日本語版も入手可能

It is common knowledge that building security into software is an important prerequisite for information assurance. Besides being 30 times cheaper[1] to fix a defect in design versus fixing it after the fact, several IT control frameworks and regulations suggest or mandate the use of security requirements and design. Most auditors have a tough time assessing these controls due to a lack of artifact-based, available evidence, nor can they offer guidance to development teams on how to produce such evidence. Auditors generally rely on interview techniques and the existence of policies to make assessments. This approach leads to development teams downplaying the importance of, and often totally ignoring, security requirements and design, even though these controls are critical enough to warrant being part of several compliance frameworks.[2]

Taking one example in more detail, the Payment Card Industry Data Security Standard (PCI DSS) section 6.3 states, "Develop internal and external software applications (including web-based administration access to applications) securely… Incorporating information security throughout the software development life cycle." The testing procedures include examining written processes and interviewing development team members to ensure that the procedures are, in fact, being followed. Section 6.5 states, "Prevent common coding vulnerabilities in software-development processes as follows… Develop applications based on secure coding guidelines." The testing procedures again reference examining policies and procedures, interviews, and an additional reference to examining training records. It is imperative for auditors to ask for better evidence—documents or other artifacts—that prove security was incorporated into system requirements and design for each application. High-level requirements, such as "make the system secure" or "provide sufficient authentication and access control," are not sufficient. Much like using the Open Web Application Security Project (OWASP) Top 10,[3] vague general requirements do very little to ensure that sufficient controls are built into application design.

Fortunately, advances in technology and tool support give auditors a few different options to easily move beyond simple policy and interview-based assessments. These approaches are not necessarily mutually exclusive. Many organizations use a combination of approaches. However, auditors should seek evidence from at least one of these techniques.

THREAT MODELING APPROACH

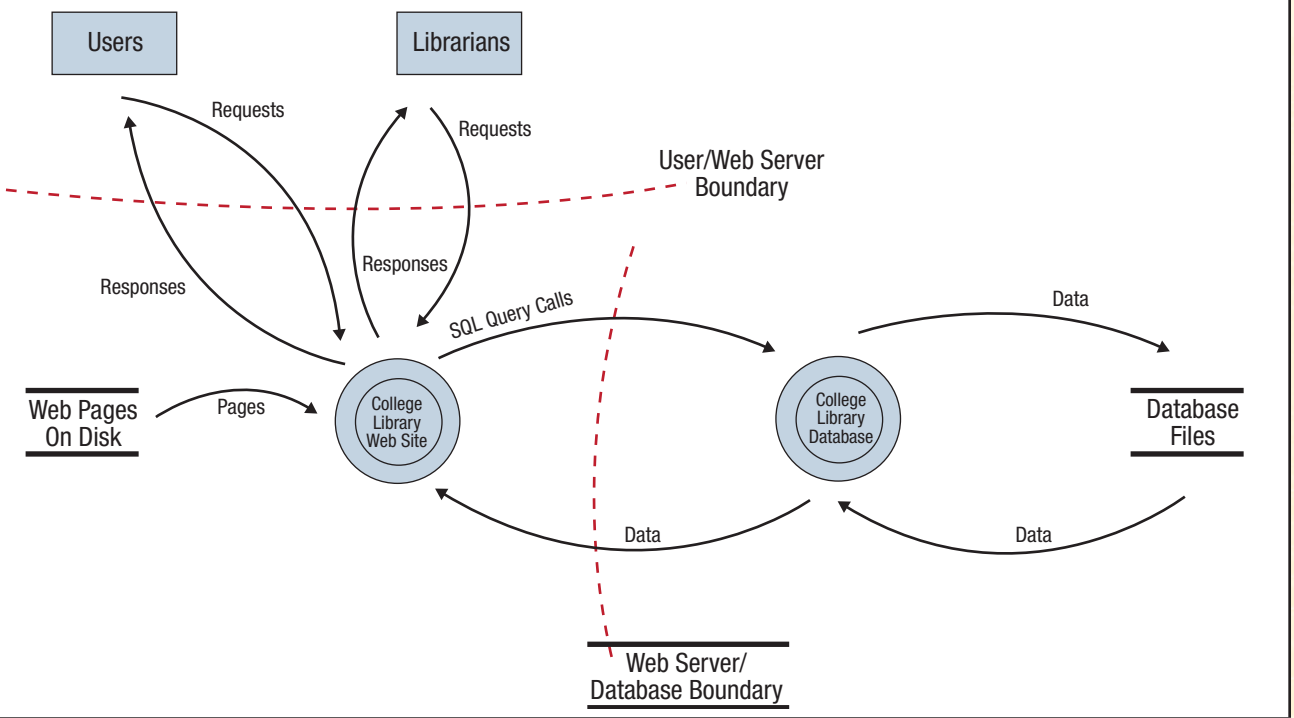
Threat modeling is a technique of modeling an application's design to uncover potential threats based on a systematic, repeatable process. Developers and security teams prioritize the resultant list of threats, along with corresponding countermeasures, and use these to incorporate security into the software design. Microsoft has been the biggest champion of threat modeling, along with extensive freely available documentation.[4]

Microsoft began championing threat modeling as part of the broader Trustworthy Computing[5] initiative, after which other organizations have proposed their own version of threat modeling, e.g., the OWASP Application Threat Modeling methodology (**figure 1**).[6]

Not surprisingly, Microsoft also has a free tool[7] that it has released to help implement threat modeling. MyAppSecurity[8] also offers a threat modeling tool. Both tools allow development teams to provide evidence that they have incorporated security into software design.

Threat modeling is the most comprehensive of the three approaches. Done correctly, threat modeling can reveal an exhaustive list of all potential security issues within an application and drive holistic defensive approaches. Its incorporation of data flow diagrams also allows

Figure 1—An Example of the OWASP Threat Modeling Methodology



Source: OWASP, *https://www.owasp.org/index.php/File:Data_flow1.jpg#filelinks*. Reprinted with permission.

development teams to understand not only what their security concerns are but also where defensive controls should fit with respect to system components. Conversely, threat modeling's comprehensiveness is also a shortcoming for many organizations. Although most tools can be used without information security expertise, in most cases, proper threat modeling requires people with security experience to determine comprehensive threats. This is challenging due to a global shortage of information security expertise.[9] It also requires certain documentation, such as architecture diagrams, while increasingly agile teams adopt the mentality of working software over comprehensive documentation.[10]

From an auditor's perspective, a documented threat model shows clear evidence of application security being incorporated into software design. For organizations that adopt threat modeling, auditors should seek to review standard output from threat models for specific applications. Examples include:

- A documented list of threats along with appropriate countermeasures
- A data-flow diagram illustrating processes and trust boundaries

A comprehensive audit should include examination of the details of these documents, but some auditors may not have a sufficient technical background to perform a thorough review. In such cases, auditors may wish to examine the following through interviews and basic artifact examination:

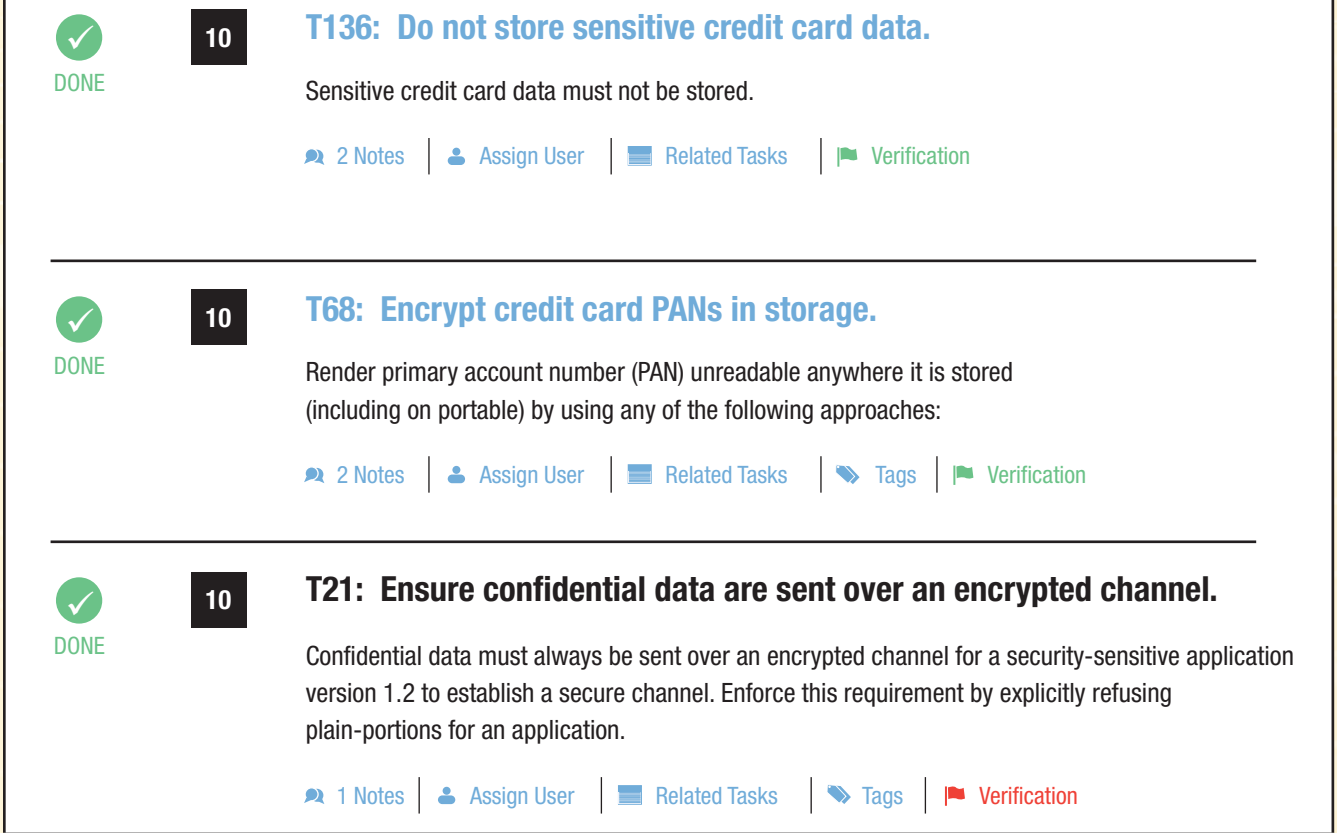
- Was the threat model documented within the time period in question (e.g., current financial year)?
- Was the threat model uniquely generated for the particular application in question? A generic threat model applied to multiple applications is of little value, as the threats to each application are unique.
- Were the identified countermeasures adopted into application design, and, if so, is there any evidence to support this (e.g., tickets in bug tracking tools, email trail, meeting minutes)?
- Were any threats deemed to be accepted risk or were they all mitigated? If threats were accepted, who accepted the risk and is there any audit trail to support this?

THE CONTROLS LIBRARY APPROACH

The emerging ISO 27034[11] application security standard from the International Organization for Standardization (ISO) outlines a process of defining application security controls systematically across the organization. In layman's terms, it requires organizations to define a library of common software security controls (**figure 2**). It then requires each application team to select a subset of these controls based on a variety of business, regulatory and technological factors. Developers assert their conformance to the applicable controls during development, and another party (often security or quality assurance [QA]) verifies that the controls are in place. While some organizations may not have plans to comply with ISO 27034, the standard serves as a useful reference to anyone planning to create an application security program. ISO 27034 has evolved with participation from many industry stakeholders. Several organizations with strong application security maturity have naturally built a similar approach over time.

The controls library approach is easily implemented within the context of a software development process, with the entire process generally taking between two to four hours when leveraging automation. Implemented correctly, it can also generate a robust set of requirements to address most well-

Figure 2—Example View of a Controls Audit Tool



Source: R. Sethi and E. Foroughi. Reprinted with permission.

known, preventable software security issues. It is, thus, a middle ground between being comprehensive and lightweight. It is not as comprehensive or potentially accurate as threat modeling. Moreover, it does not help inform developers where security controls should fit within an application's architecture. It generally requires more time to implement upfront and maintain than something as lightweight as a security checklist.

Organizations that adopt a tool for following the controls library approach should be able to generate an audit report that documents all appropriate requirements and their status in terms of development and verification. Auditors should make note to examine the following:

- Is the set of business, technological and regulatory factors used to decide upon the security controls documented?
- Was each control implemented and verified? If any control was not implemented or verified, is there audit evidence that it will be implemented/verified later or are the risk factors accepted?
- If applicable, is there evidence that the controls were integrated into development, such as linkage to an application life cycle management (ALM) tool (e.g., JIRA)? Organizations may elect to document completion status within the controls library tool itself or they may elect to use an ALM tool instead.

THE SECURITY CHECKLIST APPROACH

Another common approach to improving application security is to provide comprehensive checklists that enumerate all known threats and corresponding countermeasures. At its most basic form, organizations often build a static, secure programming guide to accomplish this. There are, however, several challenges with a large static checklist or guide:

- **Time pressure**—Developers under time pressure to deliver a feature, iteration or release rarely have time to sift through a 40-plus page document looking for best practice guidance.
- **Seniority**—Senior developers can often feel they already have sufficient expertise in security, often ascribing security problems to more junior developers. It is natural for them to feel skeptical that any general best practice guidance can really benefit their application.
- **Static content**—A single document can quickly grow out of date with advances to attacks and defensive technologies. Developers need actionable information relevant to today's threats.
- **Context switch**—Studies show that developers lose productivity every time they shift context out of their development tools.[12] Asking developers to switch between their regular tools and a static document means lost productivity, which, in turn, reduces the likelihood of the document being read.

Fortunately, automated tools that integrate with development environments help reduce the burden of having to parse large documents. Security Innovation's TeamMentor[13] product provides a dynamic, tool-based method for secure programming. It offers much more functionality than a standard checklist but is just as easy to use and implement.

Security checklists are the lightest weight of all three methods. On the other hand, they are often not uniquely tailored to an application like the threat modeling and application security controls approaches.

Auditors should ask to review the following:

- A copy of the completed checklist that the development team used
- An audit trail of who completed the checklist
- Audit evidence that the checklist items were integrated into development
- An understanding of which specific checklist items were not implemented and if they were simply not applicable or if they were accepted risk

Figure 3—Table Summarizing Three Approaches

Approach	Pros	Cons
Threat modeling	• Comprehensive • Visualization with diagrams	• Time consuming • Security expertise required for good models
Controls library	• Balance between being lightweight and comprehensive • Blends naturally into development process	• Not as exhaustive as threat modeling • Not as easy to get started as checklists • Not visual
Checklist	• Very lightweight • Easy to get started	• Static, can be overwhelming • Not visual

Source: R. Sethi and E. Foroughi. Reprinted with permission.

Overall, organizations have several tools and techniques at their disposal to incorporate security into requirements and design. The three approaches are not necessarily alternatives (**figure 3**). Several organizations use two or all three of the approaches described. Relying on process documentation and interviews alone to assess these controls is no substitute for real evidence that the process has been followed during application development. Since many organizations form their information security programs primarily to address audit requirements, the consequence of lax audit requirements means many software development teams place very little emphasis on software security requirements and design. Advances in automation allow auditors to build trust, but verification via reviewing the real artifacts that prove development teams are building in security is still needed.

ENDNOTES

[1] IBM, *Minimizing Code Defects to Improve Software Quality and Lower Development Costs*, Development Solutions white paper, 2008, *ftp://ftp.software.ibm.com/software/rational/info/do-more/RAW14109USEN.pdf*

[2] A nonexhaustive list includes: ISO 27001:2013 sections A.14.1.1 and A.14.2.5; PCI DSS sections 6.3 and 6.5; FFIEC IT Handbooks, Security Controls Implementation Systems Development, Acquisition, and Maintenance Software Development and Acquisition; COBIT® 4.1: AI2 Acquire and Maintain Application Software; COBIT® 5: BAI02 and BAI03.09; NIST 800-37: Common Control Identification Task 2-1 and Security Control Selection Task 2-2; and NIST 800-53: SA-15, SA-17

[3] Sethi, R.; "Why You Shouldn't Use the OWASP Top 10 as a List of Software Security Requirements," Infosec Island, 21 February 2013, *www.infosecisland.com/blogview/22951-Why-You-Shouldnt-Use-the-OWASP-Top-10-as-a-List-of-Software-Security-Requirements.html*

[4] Meir, J. D., *et al.*; *Improving Web Application Security: Threats and Countermeasures*, Microsoft Corp., USA, 2003, chapter 3, *https://msdn.microsoft.com/en-us/library/ff648644.aspx*

[5] Microsoft, Trustworthy Computing, *www.microsoft.com/en-us/twc/*

[6] OWASP, Application Threat Modeling, *https://www.owasp.org/index.php/Application_Threat_Modeling*

[7] Microsoft, Threat Modeling Tool 2014, *www.microsoft.com/en-ca/download/details.aspx?id=42518*

[8] My App Security, Enterprise Threat Modeler, *http://myappsecurity.com/threatmodeler-3-0-2/*

[9] Olstik, Jon; "New Research Indicates Cybersecurity Skills Shortage Will Be a Big Problem in 2015," *NetworkWorld*, 8 January 2015, *www.networkworld.com/article/2866913/it-skills-training/new-research-data-indicates-that-the-cybersecurity-skills-shortage-will-be-a-big-problems-in-2015.html*

[10] Beck, K., *et al.*; *Manifesto for Agile Software Development*, *http://agilemanifesto.org/iso/en/*

[11] International Organization for Standardization, ISO/IEC 27034-1:2011, *www.iso.org/iso/catalogue_detail.htm?csnumber=44378*

[12] Kerseten, M.; *Focusing Knowledge Work With Task Context*, University of British Columbia, Vancouver, Canada, 2007, *https://tasktop.com/docs/publications/2007-01-mik-thesis.pdf*

[13] Security Innovation, Team Mentor, *https://www.securityinnovation.com/training/application-security/knowledgebase/use-cases.html*

Deep Web Data Extraction Based on URL and Domain Classification

B. Aysha Banu is a research scholar at Mohamed Sathak Engineering College in Ramanathapuram, Tamil Nadu, India.

M. Chitra, Ph.D., is a professor in the department of information technology at Sona College of Technology, Salem, Tamil Nadu, India.

The rapid development of computer and networking technologies has increased the popularity of the web, which has led to the presence of more and more information on the web. However, the explosive increase of information online leads to some search problems—specifically search engines usually return too many unrelated results on a given query.

Deep web is content that is dynamically generated from data sources, namely file systems or databases. Unlike the surface web, pages in the deep web are collected by following the hyperlinks embedded within collected pages. Data from the deep web are guarded by search interfaces such as web services, HTML forms or programmable web, and they can be retrieved by database queries only. Surface web content is defined as static, crawlable web pages. The surface web contains a large amount of unfiltered information, whereas the deep web includes high-quality, managed and subject-specific information.[1] The deep web grows faster than the surface web because the surface web is limited to what is easily found by search engines.

> "The deep web grows faster than the surface web because the surface web is limited."

The deep web covers domains such as education, sports and the economy. It contains huge amounts of information and valuable content.[2] Because deep web information can be found only by queries, it is necessary to design a special search engine to crawl deep web pages. Deep web data extraction is the process of extracting a set of data records and the items that they contain from a query result page. Such structured data can be later integrated into results from other data sources and given to the user in a single, cohesive view. Domain identification is used to identify the query interfaces related to the domain from the forms obtained in the search process. The domain classifications are done based on the number of matching results obtained in the similar criteria among the query interface and the domain, based on the database summary.

DWDE FRAMEWORK BASED ON URL AND DOMAIN CLASSIFICATION

The Deep Web Data Extraction (DWDE) framework seeks to provide accurate results to users based on their URL or domain search. The complete steps of the framework for DWDE are shown in **figure 1**. Initially, the collected web sites are categorized into surface web or deep web repositories based on their content. The user gives a query to retrieve the relevant web pages. The user can search the query based on the following two criteria:

1. URL
2. Domain

If the user searches by URL, then the proposed framework validates whether it is a live web site. If it is a valid web site, the necessary and important contents are extracted from the web site based on the tag information. If the keyword or domain information is directly given to the search engine, the contents are extracted based on the given keyword and web site content matching.

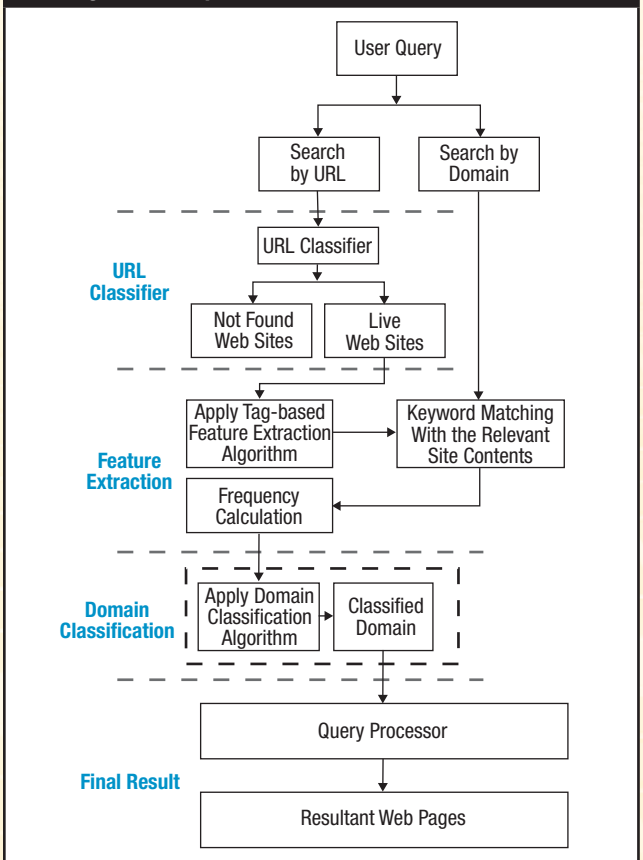
For both searching criteria, a frequency calculation is applied to calculate the number of occurrences among the given query with the relevant web sites. The domain classification algorithm is designed to predict the classified domains, and it retrieves the accurate web pages for users.

Classifying the Web Site

The Internet contains a huge number of web pages and web content. Web pages can be categorized into two types, namely surface web repository and deep web repository. This classification is based on the static and dynamic nature of the web pages. The web

sites are classified based on the tag information. If the web site includes any form tags, it is classified as a deep web site. (It includes dynamic information.) If the web site does not include any form tags, it is classified as surface web repositories. (It includes only static information.) The DWDE framework helps process deep web pages to provide the accurate and necessary web pages to the users.

Figure 1—Deep Flow Web Data Extraction Framework



Source: Banu and Chitra. Reprinted with permission.

Tag-based Feature Extraction (TFE)

Tags, such as title, header, anchor, metadata about the Hypertext Markup Language (HTML) document, paragraph, group in-line elements in a document and images, are utilized to extract the feature's domain classification. Most of the domain-specific necessary terms appear under these tags. The existing web-page classification mechanism uses the HTML tags for domain classification. In this classification method, a stop word removal is applied to all the information from each of those tags to extract the essential features. Each stemmed term with corresponding tag creates a feature. For example, the word "mining" in the title tag, the word "mining" in the <b> tag and the word "mining" in the <li> tag are all considered different features from similar HTML tags.

The DWDE framework uses limited tags to extract the most important features to recognize the domain of the given URL. These tags are used to avoid spending time extracting the less-important features.

Domain Classification

After extracting the source information, a visual block tree is constructed using the tags. Constructing a tag tree from the web site is an essential step for most web content extraction methods. In the DWDE framework, the HTML tag is used to formulate the corresponding tag tree. Based on the properties of the HTML tag and text, the tag node is defined as tag-name, type, parent, child-list, data, text-num and attribute. The tag-name denotes the name of the tag; type denotes the type of each node and where nodes are divided into branch nodes; parent represents the parent node; child-list is the set of successors; data stores the content of the node; text-num denotes the total number of punctuation and words in all the descendants of each node; and attribute denotes a mapping of the characteristics of the HTML tag. The root node represents the whole page, and each block in the tree belongs to the clocks that cannot be further segmented. For each tag on the tree, keyword frequency is calculated for the extracted information.

PERFORMANCE ANALYSIS

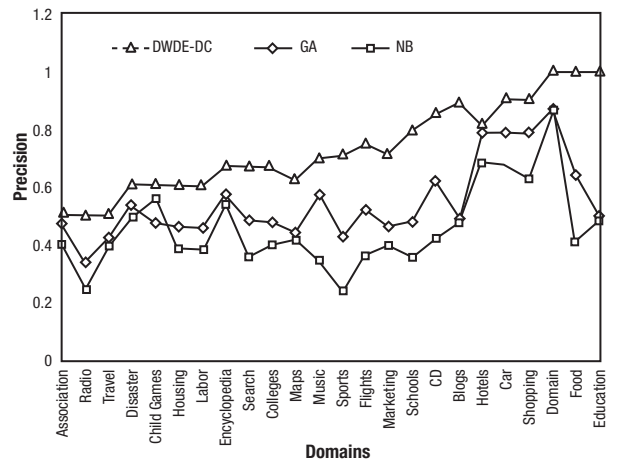
The DWDE framework was compared with the existing Genetic Algorithm (GA)[3] and Naive Bayes (NB)[4] classifiers with respect to precision, recall and F-measure. The proposed system is able to search the query with multiple keywords,

so it is also compared with the existing Multi-keyword Text Search (MTS)[5] algorithm, and the execution time is investigated. The DWDE framework can be executed for any database that collects from real-time online data sets.

Precision and Recall Analysis

Precision is the number of true positives divided by the total number of positives, providing the percentage of true positives. Recall is the number of true positives divided by the number of true positives and false negatives, providing the percentage of positives that are found.

Figure 2—Precision for DWDE Framework Compared to GA and NB Methods



Source: Banu and Chitra. Reprinted with permission.

In this experiment, the DWDE framework was validated for diverse domains, including association, radio, travel, disaster and child games. The precision and recall values are noted and the results are shown in **figures 2** and **3**. The proposed DWDE framework uses only a limited number of valuable tags to classify the domains, so the results are better and more relevant pages for the user. As a result, the framework automatically has better precision and recall values.

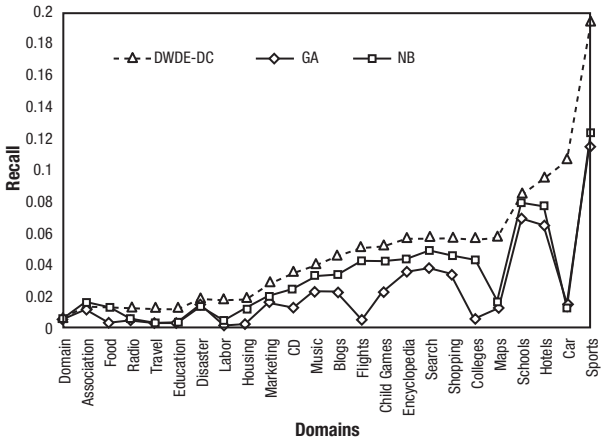
The results show that the DWDE framework results in better performance than the existing GA and NB methods.

F-measure

F-measure is the measure of a system's/method's performance by its classifiers and is based on precision and recall scores.

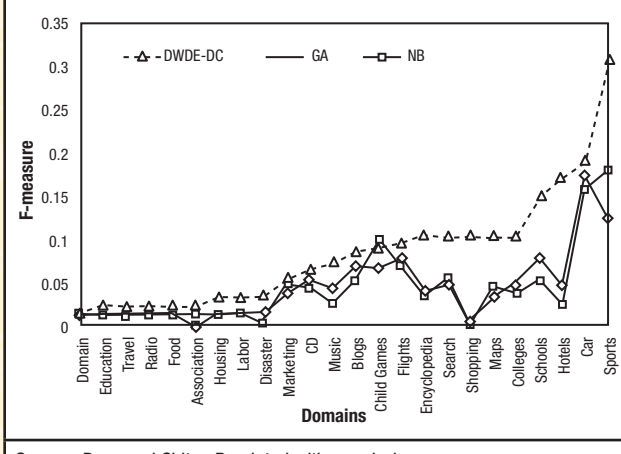
The greater the value of the F-measure, the better the performance of the system. The DWDE framework results in higher F-measure values than the GA and NB methods. As the precision and recall values for the method yield better results, it is reflected in the F-measure calculation. The DWDE framework can result in better classification of web pages than the existing methods. The result of the F-measure analysis among various domains is depicted in **figure 4**.

Figure 3—Recall Values for DWDE Framework Compared to GA and NB Methods



Source: Banu and Chitra. Reprinted with permission.

Figure 4—F-measure Values of DWDE Compared to GA and NB Methods



Source: Banu and Chitra. Reprinted with permission.

Execution Time Analysis

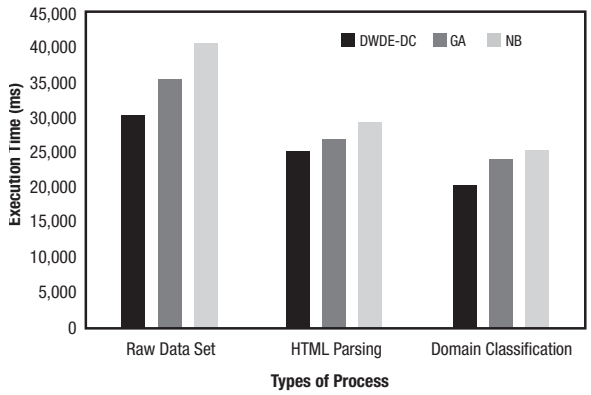
The execution time is evaluated based upon three types of processes:

- Time taken for the raw data set
- Time taken for HTML parsing
- Time taken for domain classification

The three criteria are investigated for the proposed method with the existing classifiers. The DWDE framework uses limited tags to extract the features, so it takes less time to execute the domain classification process to retrieve the resultant web pages.

The results (**figure 5**) show that the proposed framework takes less execution time to complete the task than the GA and NB methods.

Figure 5—Execution Time for Raw Data Set, HTML Parsing and DWDE



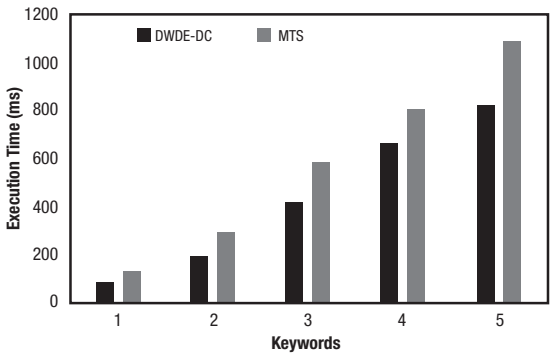
Source: Banu and Chitra. Reprinted with permission.

Multi-keyword search is also possible in the DWDE framework. The execution time experiment was conducted for multiple keywords (up to five keywords). The DWDE method takes less execution time than the existing MTS algorithm, which is shown in **figure 6**.

CONCLUSION

The DWDE framework uses the tag-based feature extraction algorithm to retrieve the necessary data. The method can process the query in two ways, searching by URL and searching by domain. Hence, it provides a user-friendly search process to deliver the results. Most of the existing algorithms process the queries on single query or multiple keyword queries, but the DWDE framework can process the single, multiple keyword queries and appropriate domain classification.

Figure 6—Execution Time for Multi-keyword Search



Source: Banu and Chitra. Reprinted with permission.

The frequency calculation is applied to compare the matching frequencies between the user query and the relevant search web sites. Based on the frequency measures, the domain classification algorithm is introduced to retrieve the accurate resultant pages.

The experiment results are compared with the existing methods, such as GA, NB and MTS algorithm. The proposed framework has better precision, recall and F-measure values than the existing GA and NB classifiers. Moreover, the time taken to execute the query search is less than the existing MTS algorithm. The DWDE framework is well suited to search the query for efficient user query retrieval.

ENDNOTES

[1] Ferrara, E.; P. De Meo; G. Fiumara; R. Baumgartner; "Web Data Extraction, Applications and Techniques: A Survey," *Knowledge-Based Systems*, vol. 70, November 2014, p. 301-323

[2] Liu, Z.; Y. Feng; H. Wang; "Automatic Deep Web Query Results User Satisfaction Evaluation With Click-through Data Analysis," *International Journal of Smart Home*, vol. 8, 2014

[3] Ozel, S. A.; "A Web Page Classification System Based on a Genetic Algorithm Using Tagged-terms as Features," *Expert Systems With Applications*, vol. 38, 2011, p. 3407-3415

[4] *Ibid*.

[5] Sun, W.; B. Wang; N. Cao; M. Li; W. Lou; Y. Hou; "Verifiable Privacy-preserving Multi-keyword Text Search in the Cloud Supporting Similarity-based Ranking," *IEEE Transactions on Parallel and Distributed Systems*, 2013

Security and Privacy Challenges of IoT-enabled Solutions

Sivarama Subramanian, CISM, is lead security tester for Center of Excellence (CoE) at Cognizant Technology Solutions, where he is leading security testing research, enabling new service rollouts and aligning new security trends to customer needs. He can be reached at *sivaramasubramanian.kailasam@cognizant.com.*

Varadarajan Vellore Gopal, CEH, is a security researcher and security testing manager at Cognizant Technology Solutions, where he manages a security testing program for a banking and financial company. He can be reached at *varadarajan.velloregopal@cognizant.com.*

Marimuthu Muthusamy is chief architect at Cognizant Technology Solutions. He can be reached at *marimuthu.muthusamy@cognizant.com.*

The Internet of Things (IoT) is captivating organizations because of its potential to rapidly transform businesses and people's lives. It is widely believed that IoT will precipitate a major shift in people's lives similar to how the Internet transformed the way people communicate and share information.

IoT comprises devices and sensors interacting and communicating with other machines, objects and environments. Gartner has predicted that there will be 26 billion devices connected to each other by 2020.[1, 2] There are still other predictions that put this number at 50 billion devices by 2020.[3] As a result of this exploding growth in interaction between devices and systems, huge volumes of data are expected to be generated and moved across information processing systems. These raw data will be processed and analyzed to generate meaningful information and to perform actionable decision making.

IOT APPLICATION DOMAINS

In its current form, IoT is expected to transform every business domain, including manufacturing and logistics (ManLog), health care, banking and financial services, life sciences, retail and industrial, and home automation. Usage cases for IoT in some of the domains[4] include the following:

- **ManLog:**
  - Machine-to-machine communication
  - Machine-to-infrastructure communication
  - Asset tracking of goods on the move
- **Health care and life sciences:**
  - Remote monitoring of patient health
  - Diagnosis and drug delivery
- **Industrial and home automation:**
  - Smart city, smart homes and automation
  - Industrial building automation
  - Appliance monitoring, such as washing machines, air conditioners and refrigerators
  - Livestock farming—tagging and devices to monitor activities
- **Retail:**
  - Replacement of bar coding and radio frequency identification (RFID) with devices that feed more data to monitoring systems, thereby improving supply chain efficiency
  - Easier product learnability and discoverability through product and smart phone communication

The diversity of services being planned using IoT means no one company can develop a full end-to-end solution and support IoT-based innovations. Of all the business domains, retail would be the first sector to see numerous IoT adoptions. This is evident as Walmart has already implemented IoT in its supply chain management.[5]

GENERIC TOPOLOGY OF IOT

IoT architecture can be typically represented by four interconnected systems, or entities, as shown in **figure 1.**

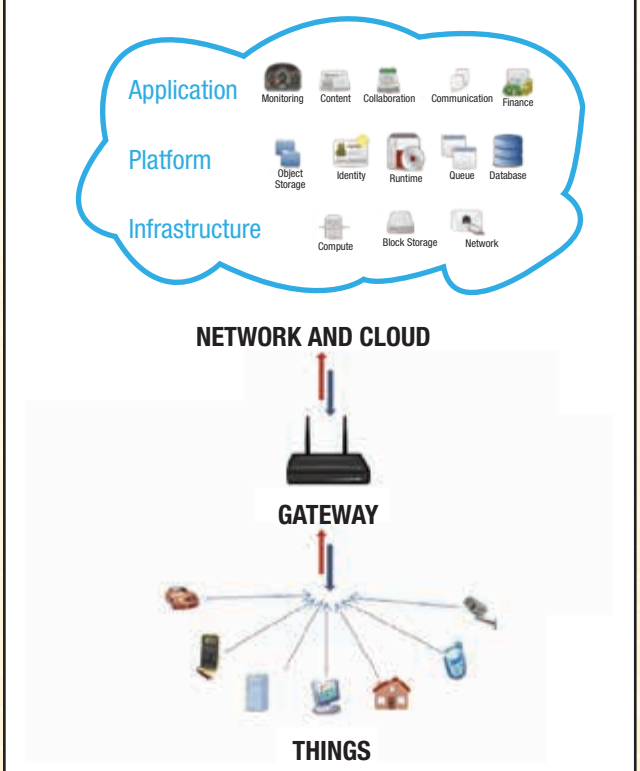
Certain organizations might do away with a cloud infrastructure for their local server.

Things or Devices

"Things" are anything that is currently interconnected in an industrial, home or business setting and has the capability to gather current state/information and act on it or send it to other systems for further analysis. All these things, or devices, are attached with sensors that help gather current state/information. There are effectively three classes of devices based on the capability and processing power:

- The smallest devices have 8-bit system-on-a-chip (SoC) controllers (e.g., Arduino boards).
- The next level of devices is based on Atheros or ARM chips with 32-bit architecture. These run a cut-down or embedded Linux platform such as OpenWRT.

Figure 1—High-level IoT Architecture



Source: Subramaniam, Varadharaj and Muthusamy. Reprinted with permission.

- The most capable are 32-bit or 64-bit platforms, such as Raspberry Pi or BeagleBone. These devices may run a full Linux OS or other OS such as Android. In many cases, these are either mobile phones or based on mobile phone technology.

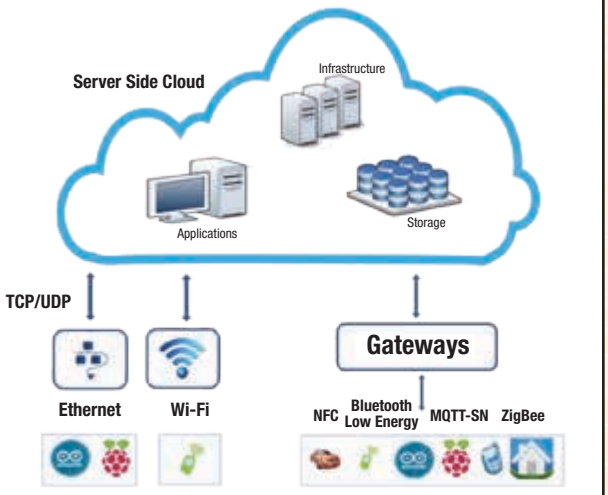
There are multiple technologies/protocols that the devices are connected to in the external world. Some of the most widely used include:

- Direct Ethernet or Wi-Fi connectivity
- Bluetooth low energy
- Near field communication
- Zigbee

Gateways

Gateways are intermediate systems that connect IoT devices through the Internet and provide much-needed support functions such as manageability and security. Gateways are needed in situations in which devices cannot directly connect to existing systems on the Internet. From an IoT standpoint, 85 percent of existing devices/things that are in use were not designed to connect to the Internet and gateways are the key to connecting these existing things to the IoT domain.[6] **Figure 2** shows various network protocols that would be used in the IoT environment.

Figure 2—IoT Network Interfaces



Source: Subramaniam, Varadharaj and Muthusamy. Reprinted with permission.

Network and Cloud Infrastructure

A network is nothing but the current Internet with connected Internet Protocol (IP) systems, such as routers, repeaters and gateways, which control data flow and connect to telecom and cable networks such as 3G, 4G and LTE.

Cloud infrastructure provides the necessary means in terms of hardware capacity and processing power required for processing the enormous amounts of data expected to be generated from IoT.

Service Creation Layer

This layer is comprised of middleware components (e.g., Service Bus; extract, transform, load [ETL]; applications; web servers) that perform the act of data massaging and presenting it for consumption through various channels such as desktop, browser and mobile applications (apps).

SECURITY AND PRIVACY CONCERNS/CHALLENGES

IoT promises to provide unprecedented and ubiquitous access to the devices that make up everything from assembly lines, health and wellness devices, and transportation systems to weather sensors. Unfettered access to that much data poses major security and privacy challenges, including:

- **Insufficient authentication/authorization—**A huge number of users and devices rely on weak and simple passwords and authorizations. Many devices accept passwords such as "1234."
- **Lack of transport encryption**—Most devices fail to encrypt data that are being transferred, even when the devices are using the Internet.
- **Insecure web/mobile interface**—Most IoT-based solutions have a web/mobile interface for device management or for consumption of aggregated data. This web interface is found to be prone to the Open Web Application Security Project (OWASP) Top 10 vulnerabilities, such as poor session management, weak default credentials and cross-site scripting vulnerabilities.
- **Default credentials**—Most devices and sensors are configured to use the default username/passwords.
- **Lack of secure code practices**—Services and business logic would be developed without adhering to secure coding practices.
- **Privacy concerns**—Devices used in the health care domain collect at least one piece of personal information; the vast majority of devices collect details such as username and date of birth. However, the fact that many devices transmit information across networks without encryption poses even more privacy risk. Privacy risk arises as the objects within the IoT collect and aggregate fragments of data that relate to their service. For example, the regular purchase of different food types may divulge the religion or health information of the buyer. This is one aspect of the privacy challenges with respect to IoT.

MITIGATING SECURITY AND PRIVACY CHALLENGES

IoT products are made secure only when security is embedded in the production life cycle. Each building block of IoT solutions should also undergo a security review to detect vulnerabilities.

Countermeasures, such as the following, can be taken to address the security challenges:

- **Base device platform analysis**—Weak platform configuration might lead to compromises such as privilege escalation.[7] A base device platform operating system and its security properties, configurations and features should be verified against the base-lined information security requirements. Verification needs to be done to ensure that any test interfaces are removed from the hardware.
- **Network traffic verification**—Network traffic (wired or wireless) should be analyzed for any interceptable, unencrypted or modifiable data.[8] There is a compromise between performance and security when encryption is recommended. Lightweight encryption algorithms can be used to cater to performance requirements.
- **Verification of functional security requirements**—High-level functional security requirements should be validated. They should also be subjected to negative testing (subversion or fuzzing).[9] IoT solutions can use Software as a Service (SaaS)-based identity management solutions for authorization and authentication requirements.
- **Trust boundary review and fault injection**—All trust boundaries across the signal path should be reviewed and subject to fault injection using negative test cases.[10] The trust boundaries can be verified using manual penetration techniques. Periodic penetration testing is recommended.
- **Side channel attack defense verification**—If side channel defenses are implemented, either in software or hardware, they should be verified using continuous penetration testing activities. Continuous penetration testing helps to minimize advanced persistent threats (APTs) for IoT solutions.
- **Secure code reviews**—Early secure code reviews lead to early mitigation techniques. Sensitive and security impact areas such as boot process, security enforcement and encryption modules should go through secure code reviews. The cost of fixing a security defect is greatly reduced when the security vulnerability is discovered during the development cycle.
- **End-to-end penetration test**—End-to-end penetration tests should be conducted across the signal path to identify any vulnerabilities in the web interface, mobile interface and cloud interface of the IoT solutions. The penetration testing would give the security posture of the IoT solution for each of its components.

Figure 3—STRIDE Approach to Identifying and Mitigating Attacks		
Components	**Attack Scenarios**	**Mitigation**
Gateway	Interception of and tampering with communication	• Implement Secure Sockets Layer (SSL) transport layer security.
Services	DoS, sending large amounts of data based on spoofed identifier	• Implement SSL transport layer security. • Implement server monitoring for high traffic from a particular user.
Web interface	Structured Query Language (SQL) injection attack on MySql databases leading to data theft and database downtime	• Use parameterized SQL statement. • Sanitize user inputs for SQL injection.
Web app to third-party apps communication	Interception of and tampering with communication	• Implement SSL transport layer security.
Data stores	Weak database credentials that can pose privacy challenges	• Collect only the required data. • Implement strong database access controls per information security standards.
Source: Subramaniam, Varadharaj and Muthusamy. Reprinted with permission.		

SECURITY ASSESSMENT OF AN IOT SOLUTION

A US-based software company developed a SecureTravel product using IoT technology. The product provides real-time data about the speed of vehicles, location of the vehicles and people traveling on the vehicles.

The technology components involved included:

- Sensors in the vehicles
- Gateways
- Services
- Web interface
- Mobile interface

Threat modeling using the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service (DoS), Elevation of privilege (STRIDE) software approach was conducted to identify the attack scenarios and formulate mitigation plans for each of the components (**figure 3**).

CONCLUSION

Introducing security in the early life cycle of the IoT solution can make mitigation design much easier. Security and privacy challenges for any IoT solution can be addressed by following secure systems development life cycle (SDLC) practices, secure coding practices and periodic penetration testing activities.

ENDNOTES

1 Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020," Newsroom, 12 December 2013, *www.gartner.com/newsroom/id/2636073*

2 Gartner, "Gartner Says the Internet of Things Will Transform the Data Center," Newsroom, 19 March 2014, *www.gartner.com/newsroom/id/2684616*

3 Cisco, "The Internet of Things," Cisco Visualizations, 2014, *http://share.cisco.com/internet-of-things.html*

4 Freescale, *What the Internet of Things (IoT) Needs to Become a Reality*, white paper, May 2014, *www.freescale.com/files/32bit/doc/white_paper/INTOTHNGSWP.pdf*

5 Hardgrave, Bill; "RFID Adoption Is on Target," *RFID Journal*, 5 January 2015, *www.rfidjournal.com/articales/view?12575*

6 Intel, *Developing Solutions for Internet of Things*, white paper, 2014, *www.intel.in/content/dam/www/public/us/en/documents/white-papers/developing-solutions-for-iot.pdf*

7 NCC Group, *Security of Things: An Implementer's Guide to Cyber-Security for Internet of Things Devices and Beyond*, 2014, *https://www.nccgroup.com/en/learning-and-research-centre/white-papers/security-of-things-an-implementers-guide-to-cyber-security-for-internet-of-things-devices-and-beyond/*

8 *Ibid*.

9 *Ibid*.

10 *Ibid*.

Auditing Linux/Unix Server Operating Systems

Muhammad Mushfiqur Rahman, CISA, CEH, CHFI, CCNA, ISO 27001 LA, ITIL V3, MCITP, MCP, MCSE, MCTS, OCP, SCSA, has 12 years of IT operations, project management and custom business solutions, enterprise resource planning implementation, and information security analysis and management experience. Rahman is an information security analyst at Eastern Bank Limited, Bangladesh. He also has 12 years of experience teaching IT courses for end users and IT professionals. He can be reached at *mushfique98@gmail.com.*

Server auditing is an important task to ensure platform-level security in an IT infrastructure and to ensure the proper configuration of Linux server security. The Linux system has its own security configuration and management system to address the security requirements in an enterprise environment. The system administrator needs to configure the Linux system to get more security assurance from the system, and IS auditors need to check the Linux system configuration as per audit standards to ensure the secure system is in place in the enterprise.

It is an exigent task for a system administrator to secure the production system from malicious attacks.

AUDITING PHYSICAL SYSTEM SECURITY

Physical security is the first and foremost task for any information system audit. Auditors must determine that the physical security of the systems configuration is standard, while also ensuring that the basic input-output system (BIOS) and the personal computer (PC) booting from CDs/DVDs, external devices and floppy drives in BIOS are rendered inoperative. Then, the auditor must ensure that the password is enabled in BIOS and that it also protects the GRand Unified Bootloader (GRUB) to ensure the restriction of physical access of the server.

In Linux or Unix-like systems, anyone can log in to the server in single-user mode using GRUB, as per the system configuration. Auditors must be certain that GRUB is protected with a strong password.

PROTECT GRUB USING PASSWORDS

To protect GRUB, administrators must use the strongest possible password and issue a command using a message-digest 5 (MD5) hash password:

```
[root@host-1[1]~]# grub-md5-crypt
```

After issuing the command, the administrator should open the /boot/grub/menu.lst or /boot/grub/grub.conf file and add the MD5 password:

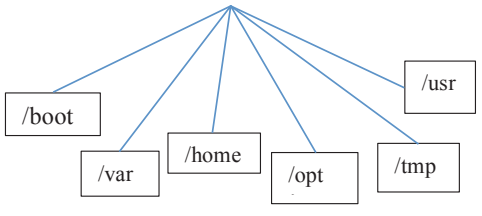
```
[root@ host-1  ~]# vi /boot/grub/menu.lst or
[root@ host-1  ~]# vi /boot/grub/grub.conf
```

The newly created MD5 password can then be added to the GRUB configuration file.

AUDITING DISK PARTITIONING IN THE AUDITED SYSTEM

In the system configuration, hard disk partitioning is critical. If any flaw exists in the partitioning, it will lead to data loss and possibly to disclosure, which could threaten the confidentiality of the data. During the audit, the auditor needs to examine and evaluate the different partitions in the audited server to ensure data security in case of any disaster. An administrator can group and separate the data among different partitions. This configuration ensures that only the data of that particular partition are lost if any unexpected accident occurs, despite the fact that the data on other partitions continue to exist. Auditors need to check that systems are configured in a way that allows separate partitions and ensure that third-party applications are installed on separate file systems. A secure directory structure is illustrated in **figure 1**.

Figure 1—Secure Directory Structure



Source: Muhammad Mushfiqur Rahman. Reprinted with permission.

AUDITING SERVERS FOR INSTALLED PACKAGES

It is recommended that when configuring the server, only the necessary packages should be installed. This ensures that the administrator may follow the standard configuration criteria of his/her organization and may scan the server using the Center for Internet Security Configuration Assessment Tool (CIS-CAT) and follow the recommendations of CIS-CAT. Unnecessary packages should not be installed into the system because such packages may create

a vulnerability in the system. During the audit program, the auditor must evaluate and check the installed packages of the audited server to minimize the risk that compromising one service may lead to compromising other services. To ensure vulnerability minimization in the audited server, installed packages must be examined and unwanted installed services identified. Services that are running on run level 3 can be identified using the "chkconfig" command:

```
# /sbin/chkconfig --list |grep '3:on'
```

To examine all installed packages in a system, the following command can be used:

```
# sudo apt-get remove package-name
```

A sample script1 can be used to check the services running in the system:

```
#!/bin/bash
if (( $(ps -ef | grep -v grep | grep $service | wc -l) > 0 ))
then
echo "$service is running!!!"
else
/etc/init.d/$service start
Fi
```

AUDIT THE LISTENING PORTS

With the help of the Netstat networking command, all open ports and associated programs can be viewed. A sample script[2] is:

```
# netstat–tulpn
```

A script for port scanning is:

```
scan() {
  if [[ -z $1 || -z $2 ]]; then
    echo "Usage: $0 <host><port, ports, or port-range>"
    return
  fi

  local host=$1
  local ports=()
  case $2 in
    *-*)
      IFS=- read start end <<< "$2"
      for ((port=start; port <= end; port++)); do
        ports+=($port)
      done
      ;;
    *,*)
      IFS=, read -ra ports <<< "$2"
      ;;
    *)
      ports+=($2)
      ;;
  esac
  for port in "${ports[@]}"; do
    alarm 1 "echo >/dev/tcp/$host/$port" &&
      echo "port $port is open" ||
      echo "port $port is closed"
  done
}
```

AUDIT REMOTE CONNECTIVITY OF THE AUDITED SERVER

Configuration of remote connectivity of the system in the network is penetrating and the remote protocol Telnet and rlogin is vulnerable because of the nonencrypted plaintext password and data transmission during the remote login. During the audit, the enabled remote connectivity services of the server should be checked, and the Secure Shell (SSH) protocol, which uses encryption technology during communication with the server should be examined. It is also necessary to check that the root login is disabled, the SSH port number is changed and the default port that is used by the audited server allows only specific authorized users access to the system. To do this, the auditor opens the main SSH configuration file and creates these parameters to restrict users' access:

```
# vi /etc/ssh/sshd_config
```

DENYHOSTS AND FAIL2BAN

During the audit, the auditor should test the DenyHosts and Fail2ban feature. This is a log-based open-source intrusion prevention script used for SSH servers. This script is used by system administrators and users to monitor and analyze SSH server access logs for failed login attempts, known as dictionary-based attacks and brute-force attacks. In this script, the administrator can set the threshold for predefined failed logins from a specific Internet Protocol (IP) address and can ban the connection from specific IP addresses.

The features of DenyHosts include:

- Keeps and tracks logs from the /var/log/secure file, noting all successful and unsuccessful login attempts, and filters them.
- Regularly monitors the host as well as failed login attempts

- Sends email notification regarding blocked hosts and suspicious logins

The features of Fail2ban include:

- Keeps and tracks logs from /var/log/secure and /var/log/auth.log, /var/log/pwdfail
- Highly configurable and multithreaded
- Regularly monitors log files

AUDITING THE ROOT LOGIN STATUS

During the audit, the auditor should check whether Linux systems allow remote login using SSH for everyone with root user status. This configuration allows users with root user credentials to directly log in to the system. To protect the server from remote login, the root user administrator must disable the root access remotely. Systems can be saved by using the strongest passwords, but it is also recommended that administrators disable the root login from the remote connection and have a separate login ID. Another recommendation is that users use sudo to gain root access in the server.

AUDITING SSH PASSWORDLESS LOGIN

During the audit, the auditor should test the SSH passwordless login. Normally, system administrators use this feature for programmed backups, remotely executed required script, file transfers and remote script management, because it allows the administrator to perform these tasks without entering a password.

AUDITING THE SYSTEM FOR UPDATED PATCHES

Systems must be updated with the latest releases' patches, security fixes and kernels when those become available:

```
# yum updates
# yum check-update
```

AUDITING THE CRON JOBS STATUS

During audits, the auditor should check the built-in feature of cron jobs (cron) where it allows one to specify who may and who may not run jobs. This is controlled by the use of files called /etc/cron.allow and /etc/cron.deny. To lock a user using cron, usernames should be added to cron.deny. To allow a user to run cron, the user must be added to the cron.allow file. To disable all users from using cron, add the ALL line to the cron.deny file:

```
# echo ALL >>/etc/cron.deny[3]
```

AUDITING THE STATUS OF USB DEVICES

During the audit, it is also important to examine and/or disable Universal Serial Bus (USB) devices. To mitigate data loss and control the spread of malware, users must be restricted from using USB devices in the systems.

AUDITING THE STATUS OF SELINUX

During audit, it is important to observe the status of Security-enhanced Linux (SELinux). It is an essential security mechanism for logical access control, which is provided in the kernel. This feature must be enabled in the system. Disabled SELinux demonstrates that the security mechanism has been deleted from the system.

The operations modes of SELinux include:

- **Enforcing**—This is the default mode of SELinux; it enforces the SELinux security policy in the machine.
- **Permissive**—This mode is used to troubleshoot SELinux-related issues; it tracks the log for each activity.
- **Disabled**—This mode speaks for itself and is not recommended.

During the audit, the auditor should use the following script to check the status of SELinux or use the system-config-selinux, getenforce or sestatus commands:

```
ENABLED=`cat /selinux/enforce`
if [ "$ENABLED" == 1 ]; then
  echo "SELinux is enabled, disable? (yes/no):"
  read disable
  if [ $disable == "yes" ]; then
    echo "disabling selinux"
setenforce 0
fi
fi
```

AUDITING THE IPV6 STATUS

During the audit, the auditor should check the activation and use of IPv6 in the system. If no one is using IPv6, it should be disabled in the system, because any unused service creates vulnerabilities for the system. During an audit, the auditor should check and confirm this. To do so, the auditor goes to the network configuration file and adds the following lines to disable IPv6:

```
# vi /etc/sysconfig/network

NETWORKING_IPV6=no
IPV6INIT=no
```

AUDITING EXISTING USER LISTS

The /etc/passwdfile stores users in Linux-based systems. To check existing users, the auditor should run the following script:

```
#!/bin/bash
# userslistinthesystem.sh

# count and Lists existing "real" users in the system.

echo
echo "[*] Existing users (sorted alphabetically):"
echo
grep '/bin/bash' /etc/passwd | grep -v 'root' | cut -f1
-d':' | sort
echo

echo -n "[*] Number of real users found: "
grep '/bin/bash' /etc/passwd | grep -v 'root' | wc -l
echo
```

AUDITING USER ACTIVITIES IN THE SYSTEM

During the audit, the auditor should check that audited systems are configured with psacct or acct. Both are open source applications for monitoring users' activities in the system. Both psacct or acct applications run in the background and keep track of each user's activity on the system, as well as what resources are being consumed. The auditor can use the following script[4] to audit user activities in the system:[5]

```
#!/usr/bin/envksh
last -Fa|awk '
   /wtmp begins/ { next; }
   /still logged in/ { next; }
   $0 == reboot { next; }

   NF > 0  {
      if( NR > 1 )
printf( "\n" );

printf( "      User:\t%s\n", $1 );     # user
printf( "     Start:\t%s %s %s %s\n", $3, $4, $5, $6 );
      if( $9 == "down" )
printf( "       End:\tshutdown\n" );
      else
printf( "       End:\t%s %s %s %s\n", $9, $10, $11, $12 );

      if( substr( $NF, 1, 1 ) == "(" )
      {
         t = $NF;
         h = "localhost";
      }
      else
      {
         t = $(NF-1);
         h = $NF;
      }

gsub( "[()]", "", t );
printf( "    Time On:\t%s\n", t );
printf( "Remote Host:\t%s\n", h );
} '
```

Furthermore, during the audit, the auditor examines the documentation for the log retention policy of the organization to ensure compliance with the law and regulations of the organization and its regulatory body.

AUDITING USERS' ABILITY TO USE OLD PASSWORDS

During the audit, it is important to check the configuration of password history in the system. It is recommended that administrators configure the system in a way so users are not able to revert to using old passwords when the password must be changed. The old password file is located at /etc/security/opasswd. This can be achieved through the following steps:[6]

- Open '/etc/pam.d/system-auth' file under RHEL:
  ```
  # vi /etc/pam.d/system-auth
  ```
- Open '/etc/pam.d/common-password' file under Ubuntu/Debian/Linux Mint:
  ```
  # vi /etc/pam.d/common-password
  ```
- Add the following line to 'auth' section:
  ```
  auth    sufficient    pam_unix.so likeauthnullok
  ```
- To disallow a user from reusing the last six passwords of his/hers, include the following line:
  ```
  Password    sufficient    pam_unix.so nullokuse_authtok md5
  shadow remember=6
  ```

After executing the command, the server stores the users' previous six passwords, so if any user tries to update his/her password using any of his/her last six passwords, he/she will get an error message.

AUDITING THE STATUS OF USER PASSWORD EXPIRATION

During the audit, the auditor should check the configuration of the password expiration of users. In Linux systems, the /etc/shadow file stores users' passwords in an encrypted format. To check a user's password expiration, one can use the change command. This command results in detailed information regarding the password expiration date, as well as the date of change of the last password. Based on these details, the system will decide when a user must change his/her password.

The following command can be used to view existing users' information regarding the age of a password:

```
#chage -l username
```

Changes to password-aging of any user can be made with the following command:

```
#chage -M 60 username
#chage -M 60 -m 7 -W 7 userName
```

Parameters

The following parameters are used to set the password age in the system:

- Parameter -M is used to set password maximum age in days.
- Parameter -m is used to set password minimum age in days.
- Parameter -W is used to set the number of warnings in days.

AUDITING THE LOCK AND UNLOCK STATUS OF USER ACCOUNTS

During the audit, the auditor should check the list of locked and unlocked users. To examine this status, the following command can be used:

```
# passwd –s accountName
```

AUDITING PASSWORD STRENGTH IN THE SYSTEM

During the audit, the auditor should check the configuration of password strength to mitigate the risk from dictionary or brute-force attacks. System administrators must use pluggable authentication modules (PAM) to ensure that users set strong passwords.

The auditor can open the following file with an editor:

```
# vi /etc/pam.d/system-auth
```

AUDITING THE IPTABLES (FIREWALL) STATUS

During the audit, the auditor can check the configuration of the Linux firewall to prevent unauthorized access of the audited servers. To control the traffic, rules can be applied in iptables, which will filter incoming, outgoing and forwarding packets. Iptables can also allow and deny specific User Datagram Protocol/Transmission Control Protocol (UDP/TCP) port numbers.

AUDITING THE ACCOUNT FOR EMPTY PASSWORDS

During the audit, the auditor should check to identify any account having an empty password, which is prohibited and would allow anyone to access the system without entering a password. The auditor must check accounts for strong passwords and be certain that no one has any unauthorized access. Empty password accounts are a security risk and can be easily exploited by an attacker. Using the following command, one can determine the existence of accounts with empty passwords:

```
# cat /etc/shadow | awk -F: '($2==""){print $1}'
```

AUDITING TIME STATISTICS OF USERS

Since organizations have a large number of users, they need to monitor the activities of users in the system, and, to do so, the auditor needs to ensure that the ac command is enabled in the system to review the activities of the users:

```
# ac
```

The command "ac -d" prints out the total login time in hours and by day:

```
# ac -d
```

The command to get the total login statistics time of user "isas" in hours is:

```
# ac isas
```

AUDITING THE LOG REVIEW STATUS

During the audit, check the logs and the frequency of the log review should also checked. As per the sensitivity of the data or based on business impact analysis (BIA), it is recommended that logs move in a dedicated log server. This may prevent intruders from easily modifying local logs. The common Linux default log file names and their usage, /var/log/message, include:[7]

1. /var/log/auth.log – Authentication logs.
2. /var/log/kern.log – Kernel logs.
3. /var/log/cron.log – Crond logs (cron job).
4. /var/log/maillog – Mail server logs.
5. /var/log/boot.log – System boot log.
6. /var/log/mysqld.log – MySQL database server log file.

7. /var/log/secure – Authentication log.
8. /var/log/utmp or /var/log/wtmp : Login records file.
9. /var/log/yum.log: Yum log files

AUDITING THE /BOOT DIRECTORY

During the audit, the auditor should check the status of the /boot directory. In Linux, kernel and its related files are placed in the /boot directory and auditors need to ensure that this folder is configured as read-only, which prevents unauthorized modification of the critical files in the Linux system. To ensure this configuration, the /etc/fstab file should be opened and the configuration checked:

```
# vi /etc/fstab
```

Then, the auditor should add the following line at the bottom, and save and close the file:

```
LABEL=/boot     /boot     ext2     defaults,ro     1 2
```

AUDITING INTERNET CONTROL MESSAGE PROTOCOL OR BROADCAST REQUEST

During the audit, the auditor should check that systems are configured in a way that ensures that the system ignores ping or broadcast requests, because excessive ping requests or broadcast echo replies slowdown the network and furthermore attackers may generate the denial-of-service (DoS)/distributed denial-of-service (DDoS) attack using the ICMP echo. To deny the ping or broadcast request, the following line should be added in the "/etc/sysctl.conf" file:[8]

```
Ignore ICMP request:
net.ipv4.icmp_echo_ignore_all = 1

Ignore Broadcast request:
net.ipv4.icmp_echo_ignore_broadcasts = 1
```

New settings can be loaded by running following command:

```
#sysctl–p
```

AUDITING THE CONFIGURATION OF THE NTP SERVER

During the audit, it is important to check the status of the Network Time Protocol (NTP) because NTP is a client-server protocol and it uses the UDP 123. Time is critical in networked systems, and the system needs to identify and track each transaction and activity of users centrally to make them accountable for their activities with the data/information of the organization. To achieve this, the auditor must examine the enablement of NTP in the server and its configuration status. To check if NTP is configured to run at system start, the following command can be issued:

```
~]$ chkconfig --list ntpd
```

By default, when NTP is installed, it is configured to start at every system start.

To check if NTP is running, the following command can be issued:

```
~]$ ntpq -p
```

To obtain a brief status report from NTP, the following command can be issued:

```
~]$ ntpstat
```

VERIFY THE EXISTING STATUS OF NTP SERVER

The auditor should use the exit status of the NTP server to verify its operations:[9]

- Exit status 0 shows that the clock is synchronized.
- Exit status 1 shows that the clock is not synchronized.
- Exit status 2 shows that the clock state is indeterminant, e.g., if NTP cannot be contacted.

CONCLUSION

Assurance and auditing are the obligatory activities to secure the information of any organization. Auditing must be a continuous and ongoing process, no matter what system or provider is being used. The audit and assurance program needs to examine the system configuration and the status of information security on a periodic basis to avoid cyberattack. Because the operating system is a penetrating component in business, it is important to make sure that it is configured properly to ensure the security of business information.

A comprehensive, all-encompassing auditing solution that can easily accomplish each of the following at the operating system level must be implemented:

- Access and authentication auditing
- User and administrator auditing

- Suspicious activity auditing
- Vulnerability and threat auditing
- Change auditing

Without a sweeping auditing solution, organizations put critical information at risk. Corrupt, inaccurate or compromised data equal lost revenue, lost time, and compromised customer and employee relationships.

ENDNOTES

[1] Akamaras blog, *www.akamaras.com*
[2] Krumins, P.: *catonmat.com*
[3] Saive, R.; "25 Hardening Security Tips for Linux Servers," Techmint.com, 24 June 2013, *http://www.tecmint.com/linux-server-hardening-security-tips/*
[4] SK, "Monitoring Users Activity Using psacct or acct Tools in Linus," Unixmen, 11 May 2013, *www.unixmen.com/monitoring-users-activitiy-using-psacct-or-acct-tools-in-linux*
[5] Argoat.net, *http://argoat.net/Blog/?paged=20*
[6] *Op cit*, Saive
[7] *Ibid*.
[8] *Ibid*.
[9] Gile, Vivek; "How to: Verify My NTP Working or Not," nixCraft, 25 March 2010, *www.cyberciti.biz/faq/linus-unix-bsd-is-ntp-client-working.com*

State and Impact of Governance of Enterprise IT in Organizations

Key Findings of an International Study

Steven De Haes, Ph.D., is an associate professor at the University of Antwerp and Antwerp Management School (Belgium), co-editor-in-chief of the *International Journal on IT/Business Alignment and Governance (IJITBAG)*, academic director of the IT Alignment and Governance (ITAG) Research Institute. He can be reached at *steven.dehaes@uantwerpen.be.*

Anant Joshi, Ph.D., is a post-doctoral researcher at the University of Antwerp and Antwerp Management School (Belgium), and a lecturer at Maastricht University (The Netherlands).

Wim Van Grembergen, Ph.D., is a professor at the University of Antwerp and Antwerp Management School, academic director of the ITAG Research Institute, and co-editor-in-chief of the *IJITBAG.*

Given the centrality of IT for enterprise risk management and value generation, a specific focus on governance of enterprise IT (GEIT) has arisen over the last two decades.[1] Enterprises are increasingly making investments in GEIT and are often drawing upon the practical relevance of generally accepted good-practice frameworks, such as COBIT® 5.[2]

This article presents some key results of a recent international study on how organizations are adopting GEIT using COBIT 5 and whether these adoptions deliver enterprise value to these organizations.[3]

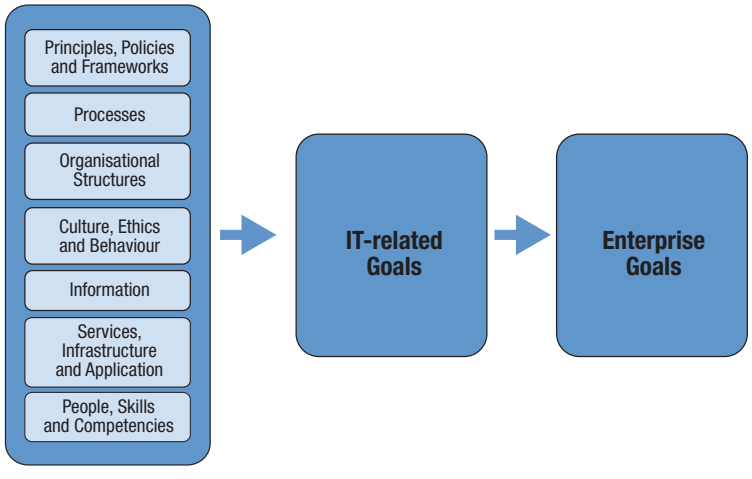
THE RESEARCH

Investments in improving GEIT are often perceived as costly and complex, while their return in stakeholder value is difficult to measure in tangible (often financial) outcomes. The recent *Benchmarking and Business Value Assessment of COBIT® 5* report attempts to demonstrate the business value achieved by applying GEIT practices in organizations. Additionally, the results of the research establish an international benchmark on how organizations are currently adopting and applying GEIT practices in their environments.

To execute this research, COBIT® was used as a lens to measure and analyze GEIT in practice. Specifically, the research provides benchmarking of the seven COBIT 5 enablers and exhibits how the level of implementation of different enterprise enablers positively links to the level of enterprise IT-related goals achievement. This, in turn, is linked to the level of enterprise goals achievement (**figure 1**). The model in **figure 1** acts as the main conceptual model grounding this research.

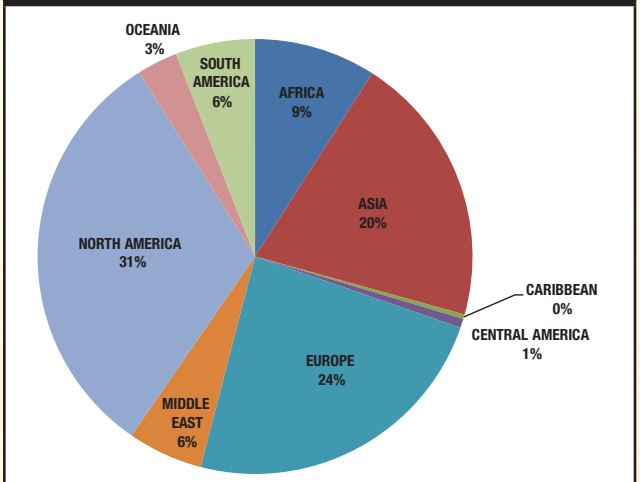
The research project, which was commissioned by ISACA® to the University of Antwerp—Antwerp Management School, was conducted as an online survey. Business, IT and audit managers across different industries were invited to complete an online questionnaire. To structure the survey, the questionnaire was mainly built around assessing different dimensions (importance, management/implementation status, ease of implementation, contribution) of the COBIT 5 enablers and how organizations are progressing toward achieving IT-related goals and enterprise goals (see **figure 1**). The final survey was conducted between 24 July and 1 September 2014. In total, 896 respondents completed the survey, of which 894 were accepted as complete responses for the final analysis. As shown in **figure 2**, respondents were spread across all regions of the world.

Figure 1—COBIT 5 Goals Cascade



Source: ISACA. Reprinted with permission.

Figure 2—Respondents Profile at Continent Level



Source: ISACA. Reprinted with permission.

RESEARCH RESULTS

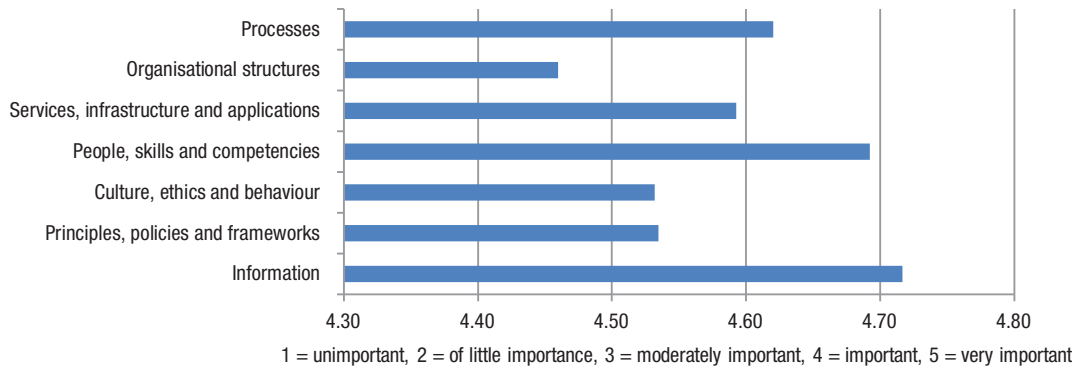
In the following sections, findings from the study are discussed and organized around key research questions.

What Is the Perceived Importance of the GEIT Enablers?

Each of the respondents in the survey was asked to rate the perceived importance of the GEIT enablers on a scale of 1 to 5, with 1 being unimportant and 5 being very important. Importance of a GEIT enabler is an indicator of how respondents assess the relevance of a particular enabler to achieving enterprise goals.

The survey results suggest that all of the enablers are considered to be very important, all having scored averages higher than 4 on a scale of 5 (see **figure 3**). This might suggest that the seven GEIT enablers, as proposed by COBIT 5, are also seen by the market as highly relevant as well as holistic and related to each other. Comparing the seven enablers relative to each other, it appears that the Information enabler and the People, Skills and Competencies enabler are perceived as the most important, closely followed by the Processes enabler. Referring to the guidance ISACA provides in support of COBIT 5 adoption and use, there is already detailed guidance published regarding the Processes and Information enablers. There is no detailed guidance published by ISACA on the People, Skills and Competencies enabler; however, the Skills Framework for the Information Age (SFIA), currently in version 5 (2011)[4] or the European e-Competence Framework[5] provide sound guidance in support of the People, Skills and Competencies enabler.

Figure 3—Enabler Importance



Source: ISACA. Reprinted with permission.

How Are Organizations Implementing and/or Managing GEIT Enablers?

The survey respondents were also asked to rate the status of the GEIT enablers' implementation or management. For the Information; Culture, Ethics and Behavior; People, Skills and Competencies; and Services, Infrastructure and Applications enablers, the respondents were asked to assess the level of management on a scale of 1 to 5, with 1 being not managed and 5 being fully managed. The Principles, Policies and Frameworks; Organizational Structures; and Processes enablers were assessed on a scale of 1 to 5, with 1 being not implemented and 5 being fully implemented.

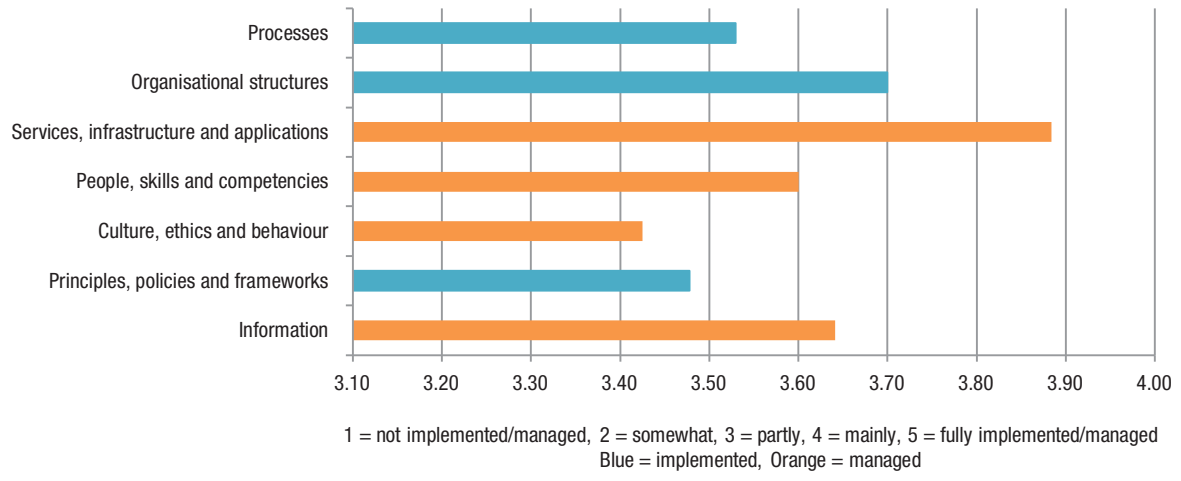
Figure 4 shows that, on average, the Services, Infrastructure and Applications (average score of 3.88) and Structures (average score of 3.70) enablers are considered to be "managed the best" as compared to other enablers. Organizations also seem to struggle with managing more human-side enablers, especially the Culture, Ethics and Behavior enabler, which received the lowest score. This result might be explained by the fact that managing infrastructure and applications (i.e., infrastructure and applications that relate to GEIT) is much more tangible compared to managing culture and ethics and, as such, is likely easier to adopt.

The study also included in-depth analysis, focusing on the Processes enabler specifically. Respondents assessed the status of implementation of the 37 COBIT 5 processes on a five-point scale with a "Do not know" option. The scale ranged from 1, "not implemented," to 5, "fully implemented."

Figure 5 presents the domain-level scores for the five domains of the COBIT 5 Process Reference Model (PRM). The average score for each domain is above 3.0, which suggests that respondents perceived that their organizations have, on average, "partly" implemented processes for the five domains. **Figure 5** also shows that for the Deliver, Service and Support (DSS) domain processes, the real executional type of operational and support processes, the implementation level is higher compared to other domains.

Respondents indicated that the process implementation level for the Evaluate, Direct and Monitor (EDM) domain is lower compared to other domains. This might be explained by the fact that these processes require high-level executive and nonexecutive board involvement. From the COBIT 5 process reference model view, the findings suggest that the implementation level of governance processes, in general, is perceived to be relatively lower when compared to management processes, which aligns with other international studies that report the low involvement of boards in GEIT.[6, 7] However, other studies underline the importance of board involvement, demonstrating a clear association between board-level involvement in GEIT and organizational performance.[8] As such, these results are a call to action for board members in the area of GEIT.

Figure 4—Level of Implementation/Management



Source: ISACA. Reprinted with permission.

Figure 5—Overall Process Average Score

Source: ISACA. Reprinted with permission.

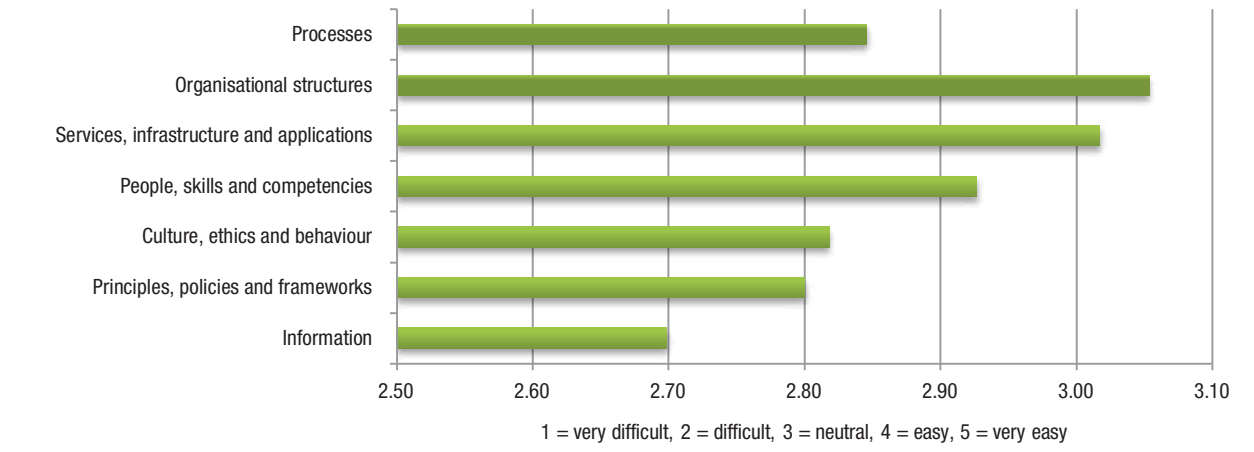
At the level of the detailed processes within these domains, the relatively better implemented COBIT 5 processes are DSS02 *Manage service request and incidents* and *Manage costs and budgets*. The relatively weakly implemented COBIT 5 processes are APO06 *Manage innovation*, *Ensure benefits delivery* and *Manage knowledge*. In general, many processes that required more business involvement achieved lower implementation scores (e.g., managing organizational changes, business process controls). This, again, is a call to action, as the importance of business involvement in IT-enabled value creation has been stressed by many researchers.[9, 10, 11] As Weill and Ross note, "If senior managers do not accept accountability for IT, the company will inevitably throw its IT money to multiple tactical initiatives with no clear impact on the organizational capabilities. IT becomes a liability instead of a strategic asset."[12]

WHAT IS THE PERCEIVED EASE OF IMPLEMENTATION AND/OR MANAGEMENT OF THE GEIT ENABLERS?

Acknowledging that each enabler requires distinct enterprise resources to manage or implement, the survey respondents were requested to assess the perceived ease of implementation of each of the GEIT enablers. The respondents rated the ease of implementation for the seven enablers on a five-point scale, with 1 being very difficult and 5 being very easy.

The findings in **figure 6** indicate that the Organizational Structures enabler and Services, Infrastructure and

Figure 6—Ease of Implementation or Management



Source: ISACA. Reprinted with permission.

Applications enabler are considered to be easy to implement and/or manage.[13] The results are consistent with the results in **figure 4**, where both the Organizational Structures enabler and the Services, Infrastructure and Applications enabler were reported as being the best implemented and managed, as compared to other enablers. However, also in line with **figure 4**, culture is perceived as more difficult to manage/implement, and the Information enabler received the lowest score in terms of ease of implementing management practices.

DO GEIT ENABLERS CONTRIBUTE TO THE ACHIEVEMENT OF IT-RELATED GOALS AND, BY EXTENSION, ENTERPRISE GOALS?

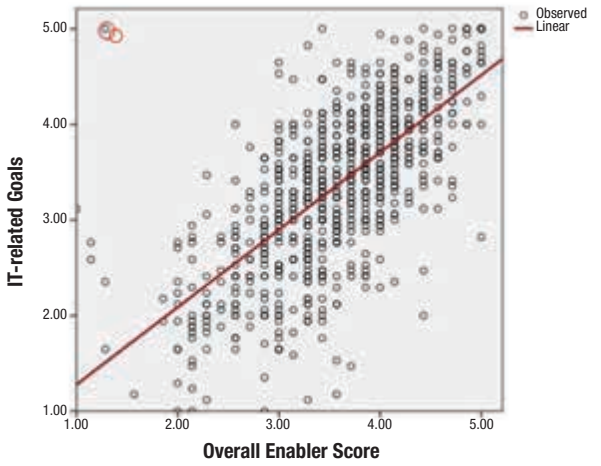
As represented in **figure 1**, COBIT 5 has introduced the goals cascade, which specifically describes an expected association between GEIT enablers and the achievement of IT-related and enterprise goals. Specifically, the goal cascade suggests that the successful implementation or management of enablers is positively associated with achieving IT-related goals, which further cascades to achieving enterprise goals. Using the sample of 894 respondents, who also assessed how they are progressing toward the achievement of IT-related goals and enterprise goals (scale of 1, not achieved, to 5, fully achieved), this study finds a strong positive association between the overall average score of implementation or management of seven enablers and the overall reported average score of IT-related goals achievement (**figure 7**). The line in the graph implies a positive correlation between the enablers' implementation or management to the IT-related goals. The findings are consistent with the proposed COBIT 5 cascade. This positive relationship is also confirmed for the 37 process enabler scores. **Figure 8** indicates a strong positive association between the overall average process enabler score and IT-related goals' achievement. Finally, this study also confirms a strong positive association between achievement of IT-related goals and achievement of overall enterprise goals, which suggests that IT-related outcomes positively link to the goals of the enterprise (**figure 9**).

CONCLUSIONS

Firms often perceive governance and management investments for their information and related technology as costly and complex. To acknowledge and address these topics, this research project used the COBIT 5 goals cascade overview to assess GEIT enablers and their relationship with achieving IT-related goals and enterprise goals.

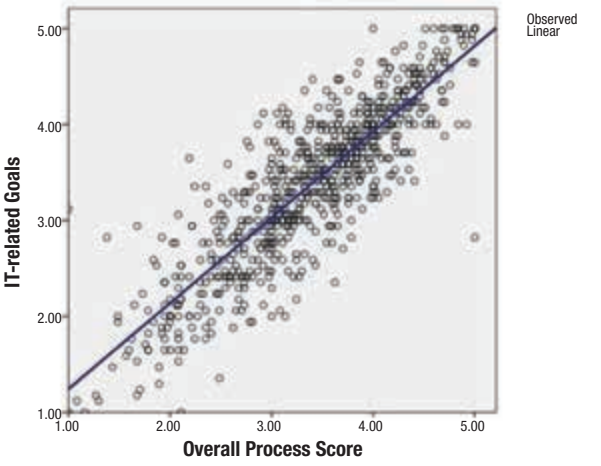
The findings suggest that professionals do perceive and experience the enablers proposed in COBIT 5 as valuable for implementing GEIT. Each of the COBIT 5 enablers is seen as highly important, and better implementation rates with the GEIT enablers clearly show positive correlations with the

Figure 7—Association Between Overall Enabler Score and IT-related Goals



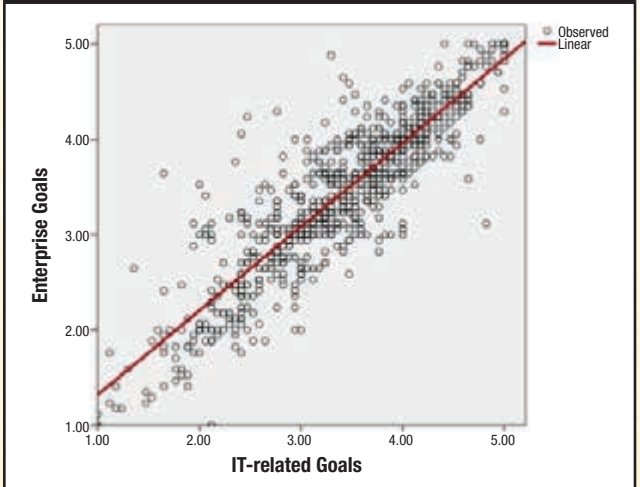
Source: ISACA. Reprinted with permission.

Figure 8—Association Between Overall Process Score and IT-related Goals



Source: ISACA. Reprinted with permission.

Figure 9—Association Between IT-related Goals and Enterprise Goals



Source: ISACA. Reprinted with permission.

achievement of IT-related goals. The findings also suggest that achieving these IT-related goals is strongly associated with the achievement of enterprise goals, which confirms the proposed conceptual cascade model in COBIT 5.

By offering empirical evidence that governing and managing those enablers does have a positive impact on enterprise value creation, management will find it easier to support investment propositions related to GEIT. Additionally, the results of this research will contribute to the relatively new domain of knowledge and theory being built, and it will assist practitioners by providing an international benchmark and more guidance on how governance and management frameworks, such as COBIT 5, can lead to higher enterprise value creation from their IT assets and resources.

ENDNOTES

[1] De Haes, S.; W. Van Grembergen; *Enterprise Governance of IT: Achieving Alignment and Value*, Springer, USA, 2015

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

[3] This article summarizes the key findings and results of a fully elaborated research report titled *Benchmarking and Business Value Assessment of COBIT® 5*, which includes detailed benchmarking results and has filtered data by sector, geography and company size. Find the full report at *www.isaca.org/benchmarking-and-business-value-assessment-COBIT-5*.

[4] SFIA Foundation, The Skills Framework for the Information Age (SFIA), *https://www.sfia-online.org/v501/en/publications/reference-guide/at_download/file.pdf*

[5] European e-Competence Framework, *www.ecompetences.eu/*

[6] *Op cit*, De Haes and Van Grembergen

[7] Andriole, S.; "Boards of Directors and Information Technology Governance: The Surprising State of Practice," *Communications of the Association for Information Systems*, vol. 24, article 22, 2009, p. 373-394

[8] Turel, O.; C. Bart; "Board-level IT Governance and Organizational Performance," E*uropean Journal of Information Systems*, vol. 23, 2014, p. 223-239

[9] Weill; Ross; *IT Governance: How Top-performers Manage IT Decision Rights for Super Results*, Harvard Business School Press, USA, 2004

[10] *Op cit,* De Haes and Van Grembergen

[11] *Op cit,* Turel and Bart

[12] Weill; Ross; *IT Savvy: What Top Executives Must Know to Go From Pain to Gain*, Harvard Business Press, USA, 2009

[13] *Op cit,* De Haes and Van Grembergen. This result is in line with the study of De Haes and Van Grembergen (2015), which also reported that IT governance structures are typically reported as being the easiest to adopt.

Data Protection Act and GAPP Alignment

Mohammed J. Khan, CISA, CRISC, CIPM, is a global audit, security and privacy professional serving the teams of the chief information security officer (CISO), chief privacy officer (CPO) and chief audit executive (CAE) at Baxter International. He has spearheaded multinational global audits in several areas over the past five years. Khan has worked previously as a senior assurance and advisory consultant for Ernst & Young and as a business systems analyst for Motorola.

With the advent of increasing privacy laws and regulations, global data privacy risk has become one of the major drivers of spotlighting the role of IT auditors and how this role can help drive, through technological means, the protection of sensitive data. For private and public enterprises alike, their data are like gold. Key channel data can be generated—particularly in the pharmaceutical industry—through clinical trials, sales and marketing, information technology, human resources (HR), procurement, regulatory affairs, physical security and surveillance, and clinical service centers. Properly managing the compliance aspects of these data, once in the hands of the data controller, is essential for keeping the company in compliance with data authorities throughout the world.

This article will align the UK Data Protection Act of 1998 (DPA) and the American Institute of Certified Public Accountants (AICPA) Generally Accepted Privacy Principles (GAPP)[1] in order to help global companies with a presence in both the US and the UK. The AICPA GAPP is aligned with the European Union (EU) Data Protection Directive (DPD) of 1995,[2] which requires member states to protect people's fundamental rights of freedoms. The DPA[3] is derived from the EU Directive and, thus, by default, is a widely accepted framework that is applied specifically to companies operating in the UK.

EU AND UK DATA PROTECTION ACT

Companies that operate in the EU are required to follow basic principles that are set forth by the EU's data protection commissioner. The data protection commissioner is responsible for upholding the rights of individuals as set out in the DPD and enforcing the obligations upon data controllers. The commissioner is appointed by the government and is independent in the exercise of his/her functions. Individuals who feel their rights are being infringed can complain to the commissioner, who will investigate the matter and take whatever steps may be necessary to resolve it.[4] The DPD which defines personal data as information relating to an identified or identifiable natural person (Article 2(a) DPD).[5]

Similarly, the Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights. The ICO mandates the DPA, which is based around eight principles of information handling best practices (**figure 1**) that are considered in good order by the Information Commissioner's Office.

Figure 1—Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Source: Information Commissioner's Office (ICO), Data Protection Principles, *https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/*

To establish a comprehensive privacy program, the company in question has to adapt to internationally accepted principles of fair information practice as the basis for this policy. These principles are to be further aligned with concepts and requirements from the DPD and the US Department of Commerce's Safe

Harbor Privacy Principles. They also are recommended to follow the framework of the GAPP, which can be used as an operational framework to help multinational entities address privacy matters that takes into consideration local, national or international requirements.

A FRAMEWORK FOR ASSESSMENT: DPA AND GAPP

One of the mechanisms that can be utilized to satisfactorily map out the DPA principles to the enterprise's adapted privacy principles is to align the DPA with the AICPA GAPP. This is a foundational step to further the capability maturity model (CMM) of an enterprise from a data privacy compliance perspective. By going through the process of mapping out the DPA principles with the GAPP, the entity goes through the exercise of understanding which principles are pertinent, thus establishing current state versus future state. There are eight DPA principles that should be addressed in order to fulfill the ICO guidelines for managing personal data. **Figure 2** offers an example of the DPA principles that were mapped to the GAPP. This is a starting point for one to

Figure 2—Mapping DPA to GAPP

Data Protection Principle/Guideline Control	Work Program	Entity A	Entity B
1. Personal data shall be processed fairly and lawfully.			
• Only collect and use personal information where it has lawful grounds and legitimate business reasons to do so.	D.1.1.2 AICPA GAPP Alignment (Collection)	✓	x
• Be transparent in dealings with people as to what information about them it collects and how it will process their information.	D.1.1.2 AICPA GAPP Alignment (Collection)	✓	x
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.			
• If information is collected for a particular purpose, ensure that it will not be used for anything else until the individuals concerned have been informed and, where required, their permission obtained.	D.1.1.14 Data Privacy Program—DPA	✓	✓
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.			
• Do not ask for more information than needed for the purposes for which it is collected (even if the information would be useful to know).	D.1.1.15 Data Privacy Program—EUDD/DPA Alignment	✓	x
• Do not record information for the sake of it.	D.1.1.15 Data Privacy Program—EUDD/DPA Alignment	✓	x
4. Personal data shall be accurate and, where necessary, kept up to date.			
• Update records when informed by an individual that their details have changed.	D.1.1.5 AICPA GAPP Alignment (Monitoring and Enforcement)	x	✓
• Continuously review and assess the quality of information.	D.1.1.5 AICPA GAPP Alignment (Monitoring and Enforcement)	x	✓
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.			
• Comply with records retention policies and ensure the organization can justify why it need to retain each category of personal information.	D.1.1.15 Data Privacy Program—EUDD/DPA Alignment	x	x
• Ensure personal information is securely disposed of at the end of the appropriate period.	D.1.1.15 Data Privacy Program—EUDD/DPA Alignment	x	x
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.			
• Ensure the right to opt out of receiving marketing communications.	D.1.1.15 Data Privacy Program—EUDD/DPA Alignment	✓	✓
• Ensure the right to have inaccurate information corrected.	D.1.1.15 Data Privacy Program—EUDD/DPA Alignment	✓	✓
• Ensure the right of access to data subject information.	D.1.1.15 Data Privacy Program—EUDD/DPA Alignment	✓	✓

Figure 2—Mapping DPA to GAPP *(cont.)*			
Data Protection Principle/Guideline Control	**Work Program**	**Entity A**	**Entity B**
7. Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.			
• Train staff on their privacy obligations.	NA	x	x
• Ensure appropriate physical and technological security measures are in place to protect personal information whether it is on or off-site.	D.1.1.7 AICPA GAPP Alignment (Security)	✓	✓
• Enforce confidentiality and security policy compliance.	D.1.1.7 AICPA GAPP Alignment (Security)	✓	✓
• Ensure secure methods of transit are employed whenever personal information is transferred from one location to another.	D.1.1.7 AICPA GAPP Alignment (Security)	✓	✓
• Ensure that outsourced process suppliers have appropriate security measures in place and are contractually required to comply with privacy principles.	D.1.1.3 AICPA GAPP Alignment (Disclosure to Third-Parties)	✓	NA
• Ensure that any breaches are disclosed with respect to personal information wherever required by local legislation.	NA	✓	✓
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.			
• Ensure that any personal information for which the organization is responsible is adequately protected in the country of destination when transferred across border and during transit.	D.1.1.5 AICPA GAPP Alignment (Monitoring and Enforcement)	✓	✓
Source: Mohammed J. Khan. Reprinted with permission.			

begin to establish compliance with the DPA and the validation check of alignment with the GAPP.

The AICPA performed its own mapping of privacy concepts set out in domestic and international privacy regulations, laws and guidelines in relationship to the GAPP. **Figure 3** lists the 10 Generally Accepted Privacy Principles.[6]

All of these principles can then be mapped to the EU Directive seamlessly, which ensures buy-in of the GAPP among privacy professionals in Europe.[7]

Figure 3—Generally Accepted Privacy Principles

The following are the 10 *generally accepted privacy principles:*

1. **Management.** The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
3. **Choice and consent.** The entity collects personal information only for the purposes identified in the notice.
4. **Collection.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
5. **Use, retention and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual as provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality.** The entity maintains accurate, complete and relevant personal information for the purpose identified in the notice.
10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

Source: American Institute of Certified Public Accountants Inc., and Canadian Institute of Chartered Accountants. Reprinted with permission.

CONCLUSION

Multinational companies that operate in the EU, and specifically in the UK, need to abide by an increasingly complex and regulated privacy landscape. The establishment of a proper framework is essential to assess the maturity level of the enterprise's compliance as it pertains to protecting personal data of its customers, employees and partners. One of the best ways to conduct this is to establish the framework of the GAPP and tie it to the DPA. This will provide the enterprise with a sure way of mapping the frameworks and, more important, the transparency required to identify gaps, if any, that can be mitigated or addressed fully to comply with the privacy laws of the UK.

ENDNOTES

[1] American Institute of Certified Public Accountants (AICPA), Generally Accepted Privacy Principles (GAPP), *www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx*

[2] European Union (EU), Directive 95/46/EC, 1995, *http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf*

[3] UK Data Protection Act, UK, 1998, *www.legislation.gov.uk/UKPGA/1998/29/contents*

[4] Office of the Data Protection Commissioner, About Us, *www.dataprotection.ie/docs/ABOUT-US/1032.htm*

[5] Office of the Data Protection Commissioner, EU Directive 95/46/EC, The Data Protection Directive, *www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapter-1/92.htm*

[6] American Institute of Certified Public Accountants (AICPA), Generally Accepted Privacy Principles (GAPP), p. 14, *www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP_BUS_%200909.pdf*

[7] American Institute of Certified Public Accountants (AICPA), "Comparison of International Privacy Concepts," *www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/pages/internationalprivacyconcepts.aspx?action=print*

HelpSource Q&A

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

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

Ganapathi Subramaniam heads the information security function at Flipkart *(www.flipkart.com)*, India's leading e-commerce marketplace. An accomplished professional with 24 years of industry experience, Subramaniam's passion and profession has always been information security. Until recently, he was employed at Microsoft Corporation India as its chief security officer, performing the role of a security evangelist within its sales and marketing support group. He has previously worked at Accenture and big four firms such as Ernst & Young and PricewaterhouseCoopers. As a conference speaker and columnist, he has addressed numerous gatherings of chief information officers and chief information security officers worldwide.

Do you have something to say about this article?

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

Go directly to the article:

Q I run a newly established information security function in a European organization and work in an enterprise that is partially alien to controls. While there is fullest support from the top/senior leadership within the enterprise in terms of need for controls and their implementation, it does not seep into all levels below, and pockets are unfamiliar with security controls implementation. While such pockets may appear insignificant in terms of size, their support would make a material change.

How should I go about establishing the security function and building a culture that is supportive to controls implementation?

A Good question. This scenario is not alien and may sound familiar to a number of readers around the world, each having tackled it in his/her own way. I have also seen this question discussed at a number of conferences over the years.

The formula is simple: influencing without authority. There are many books on this topic, and my favorite one is by Robert Cialdini. As always, the following is an indicative list and not an exhaustive one:

> "The formula is simple: influencing without authority."

- Establish a security council consisting of key executives/ senior management from your organization whose roles can be defined as follows:
  - Approve the roles, responsibilities and accountabilities on information security and business continuity.
  - Approve the security road map aimed to reducing risk and helping operate in a risk-aware environment; the level of protection provided must be commensurate with the risk exposure.
  - Approve all information security policies and standards.
  - Approve all critical security exceptions or waivers to policies and standards.
  - Maintain risk and compliance oversight of the entire information security and business continuity program.
  - Provide sign-off on the open security risk.
  - Receive all security assessment reports/reviews.
  - Receive security metrics reports on security to ensure a holistic view.
  - Ensure security and continuity management move progressively and demonstrably toward achieving a mature and sustainable process.
  - Provide compliance oversight for the entire organization, function-specific and project-specific BCP development, and the testing process.
  - Monitor the implementation of tests as per the plan and schedule.
  - Review and approve the continuity strategy accepting residual risk.
  - Review reports on actual invocation of the plan and lessons learnt during crisis management.
- Categorize key individuals into multiple buckets—decision makers, influencers, sneezers (please refer to the book *Purple Cow*),[1] blockers/ aliens, friends/allies—and for each type have specific plans to win their support and trust. It may not be possible to achieve it in all cases. However, an influencing strategy suiting the types of individuals will help achieve our objectives.
- Ensure good negotiation. Know clearly that you may not be able to achieve your objectives on day one. Identify areas where you are willing to yield, as well as the nonnegotiable ones. For example, software license compliance may be a nonnegotiable item. Create a list of nonnegotiable controls and nice-to-have controls.
- Identify a list of allies within the organization who may be willing to help spread the message. Security must not be seen as the responsibility of only the security team.

- Tackle the blockers separately. Winning their trust and support is imperative to the success of the security team. Collaboration is a must. Talk the language of risk. If you cannot take everyone together with you, it may be difficult to roll out all the controls. Explain the impact to the business in the event of nonimplementation of security controls.
- Consider implementing detective or monitoring controls, if getting preventive controls implemented appears to be a challenge. For example, it may not be possible to implement Universal Serial Bus (USB) disablement for usage with removable media. Another option is to have a monitoring system that will alert you in the event of any attempt of data leakage/spillage.
- Remember that what worked at one organization may not work at another. Thus, try to put forward a road map aligned with your current organization's business agenda.
- Begin with policies, followed by infrastructure standards.
- Complete gap assessment using a standard controls framework such as COBIT® or ISO 27001:2013.
- Use all external drivers—industry regulators, external auditors and insurers—to drive your agenda.
- Roll out compliance and monitoring programs that include areas such as vendor security controls assessment.
- Create an incident management framework and implement it as a priority.
- Combine patch management with vulnerability assessments to contribute to the implementation of an appropriate controls framework.
- Have a clear metrics program and publish numbers. Numbers can provide the magic.
- Develop and roll out an awareness program.
- To repeat, speak the language of risk and business impact always. A number of controls can be seen as a theoretical need.

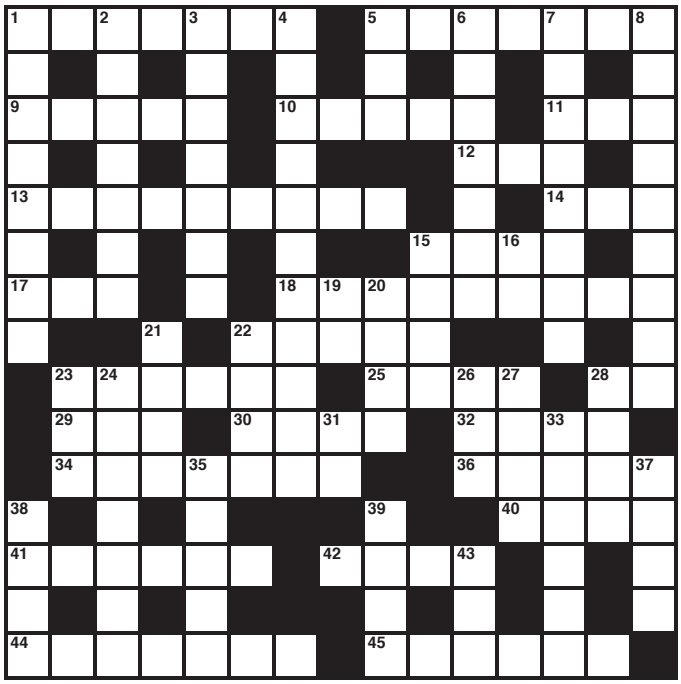
Q&A

ENDNOTES

[1] Godin, Seth; *Purple Cow: Transform Your Business by Being Remarkable*, Penguin Group, USA, 2003

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1 Goes down suddenly, as a system
5 Fixes to system bugs
9 Computers hooked up to a specific network
10 Early testing stage for software
11 ____top
12 End of the week
13 Vendors to consumers
14 Sun in Spanish
15 Economics Nobelist Friedman, familiarly
17 Originate (in)
18 One description for a good audit
22 Flourish
23 Made biased or distorted
25 ___ counter
28 Miss or Mrs.
29 Steeped beverage
30 Fixes firmly
32 Acronym for Appcito's service combining advanced load balancing and content-switching capabilities
34 One of the greatest theorists of programming, Edgar
36 Features on Windows 8 start screen
40 At an advanced stage, in a project
41 ____ management audits
42 Acronym for a major change in the use of communication devices in the workplace
44 Applies incorrectly
45 Puts completely inside another data file

DOWN

1 An audit will examine their security and effectiveness
2 Company whose IT processes are being examined and reviewed
3 Providing space for web sites on servers
4 Individual with a financial interest in a company or project
5 ___-ups (ads)
6 Visitor volume
7 Emphasizing the organic or functional relationship between the parts and the whole
8 They deliver services and goods
15 Concept that spreads fast online
16 Light, for short
19 SAP Business Objects (aka, software corporation)
20 Apple founder
21 Security breach
22 ____ practices
23 Standard, for short
24 Data input devices
26 Law
27 Locate exactly
28 Become acquainted
31 British "Thanks"
33 Defective, as code
35 Indications
37 ____ the deal
38 Goal of phishing
39 Eight bits
43 Nickname

(Answers on page 58)

CPE Quiz

Prepared by Sally Chan, CGEIT, CPA, CMA

Take the quiz online:

QUIZ #161

Based on Volume 2, 2015—Opportunities and Challenges of New Technology

Value—1 hour of CISA/CISM/CGEIT/CRISC continuing professional education (CPE) credit

TRUE OR FALSE

RAVAL ARTICLE

1. Technology-centric innovation involves technology as a lever to make a traditional business model more open source, virtual and efficient.
2. An ethically flawed idea may suffer from correctable deficiencies, but it could also be downright incurable.
3. In the postlaunch period, the role of IT innovation firms changes from that of an adversary to an ally.

GONZALEZ ARTICLE

4. Focusing too much on the data in IoT and not enough on the beliefs and behaviors of people attached to the "things" can create privacy and security risk issues.
5. There are no barriers that prevent mass prevalence of IoT as a part of smart buildings, at home or in an enterprise.
6. The single largest impediment for IoT will be an ineffective or nonexistent plan for deploying security updates will be. A solid security life cycle that considers security throughout design and development will have notably fewer security issues.
7. To achieve control in IoT and minimize the potential IoT risk, attention must be paid to minimize collection of personal data, minimize connecting data with individuals, and minimize and secure data retention.

BERATARBIDE AND KELSEY ARTICLE

8. E-health governance refers to applying IT within health care in harmony with the health care organization's (HCO's) strategies, goals and needs. Business-to-e-health strategic alignment is defined as the act of governing e-health, which involves decision making as well as e-health management.
9. E-health is considered key for sustainable health care, yet many e-health initiatives have failed, and HCOs commonly find themselves caught between the organizational pressures for delivering e-health and organizational resistance to new ways of functioning.
10. E-health governance is in its infancy across sectors and countries. The more mature e-health governance is, the better the strategic alignment between e-health and HCOs.

WLOSINSKI ARTICLE

11. A statistical analysis of cloud security incidents over a five-year period identified inadequate infrastructure design and planning to have the highest number of security incidents, while insecure interfaces and application programming interfaces (APIs) had the lowest.
12. To prevent misuse of the cloud, organizations should think like criminals to better know their methods. Steps taken by an attacker leading up to an attack can be analyzed and countermeasures implemented. Some of these steps include gathering data of device weaknesses and planting malware to allow access and to retrieve data of value from those devices.

ANDERSON ARTICLE

13. One mistake that information security managers seeking security solutions to fill a gap in their tools portfolio or replace an existing product make is to develop a set of selection criteria that mirrors a solution with which they are familiar. Insufficient product evaluation prior to purchase could potentially result in a solution with capabilities that are inconsistent with the organization's security needs.
14. The Goldilocks Principle states that a solution to something must fall within certain parameters rather than going to extremes in terms of offering too much functionality. The most successful solutions provide a "just right" balance in terms of benefits received, security needs met and resources required for support.
15. The benefits of using a SWOT analysis technique in solution evaluation include covering only issues that can positively be considered as a strength, weakness, opportunity or threat, and factoring in other issues and nuances with the potential to affect the success of a particular solution within a specific organization.
16. Often, the fault for less-than-successful technology investment is attributed the vendor, sales representative or product itself; prior management who made the acquisition; lack of senior management support; and/or the project team.

ISACA Journal

CPE Quiz

Based on Volume 2, 2015—Opportunities and Challenges of New Technology

Quiz #161 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC # _____

Quiz #161

True or False

RAVAL ARTICLE

1. _____
2. _____
3. _____

GONZALEZ ARTICLE

4. _____
5. _____
6. _____
7. _____

BERATARBIDE AND KELSEY ARTICLE

8. _____
9. _____
10. _____

WLOSINSKI ARTICLE

11. _____
12. _____

ANDERSON ARTICLE

13. _____
14. _____
15. _____
16. _____

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

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

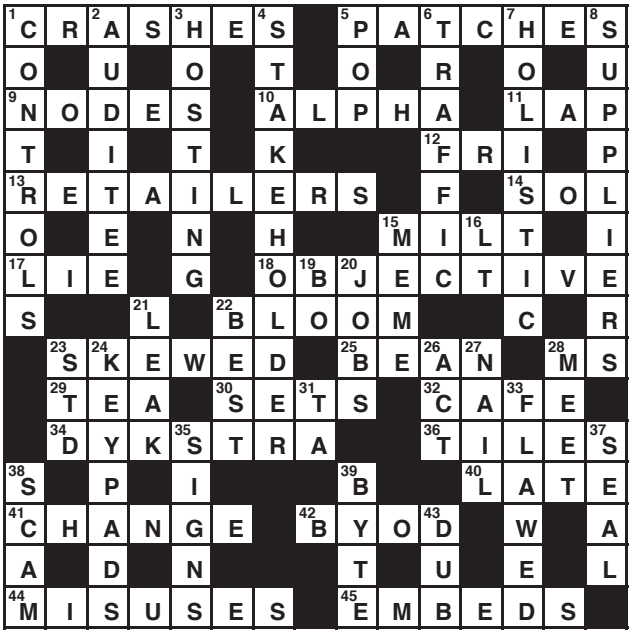
Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

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

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

Answers—Crossword by Myles Mellor

See page 56 for the puzzle.



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*	Back Cover

Leaders and Supporters

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

Subscription Rates:
US: one year (6 issues) $80.00
All international orders: one year (6 issues) $95.00. Remittance must be made in US funds.

ISSN 1944-1967

ISACA®
Trust in, and value from, information systems

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

www.isaca.org/bookstore

COBIT 5: THE LEADING FRAMEWORK FOR THE GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

FEATURED CATEGORY:
COBIT® 5 BOOKS BY ISACA®

- *COBIT 5*
- *COBIT 5: Implementation*
- *COBIT 5: Enabling Processes*
- *COBIT 5 for Assurance*
- *COBIT 5 for Information Security*
- *COBIT 5 for Risk*
- *COBIT 5 Bundle*

COBIT® 5
AN ISACA® FRAMEWORK

ANNOUNCING NEW ONLINE DATABASE SUBSCRIPTIONS FOR CISA AND CISM

NOW AVAILABLE IN ISACA'S BOOKSTORE—CISA AND CISM ONLINE DATABASE SUBSCRIPTIONS!

CISA®
Certified Information Systems Auditor®

CISM®
Certified Information Security Manager®

Need help preparing for your CISA or CISM Certification Exam?
ISACA study resources can help you prepare to finish strong.

Browse over 450 publications featuring the latest research and expert thinking on standards, best practices, emerging trends and more at ***www.isaca.org/bookstore***

FEATURED CATEGORY:

COBIT 5

COBIT 5

COBIT 5 is the only business framework for the governance and management of enterprise IT. This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, analytical tools and models to help increase the trust in, and value from, information systems. *COBIT 5* builds and expands on COBIT 4.1 by integrating other major frameworks, standards and resources.

Product Code: CB5
Member/Nonmember:
$35.00/$40.00

eBook Product Code: WCB5
Complimentary eBook available to Members.

COBIT 5: Implementation

This guide, along with *COBIT 5*, recognize that information and related information technologies are pervasive in enterprises and that it is impossible, nor good practice to separate business and IT-related activities. Proper governance of enterprise IT should be implemented as an integral part of enterprise management, covering the full end-to-end business and IT functional areas of responsibility.

Product Code: CB5IG
Member/Nonmember:
$35.00/$55.00

eBook Product Code: WCB5IG
Complimentary eBook available to Members.

COBIT 5: Enabling Processes

Product Code: CB5EP
Member/Nonmember:
$35.00/$55.00

eBook Product Code: WCB5EP
Complimentary eBook available to Members.

COBIT 5: Enabling Processes includes:

COBIT 5 Goals Cascade

Enterprises exist to create value for their stakeholders. Value creation means realizing benefits at an optimal resource cost while optimizing risk—a cornerstone objective of governance. The goals cascade is important, because it allows the definition of priorities for implementation, improvement and assurance of governance of enterprise IT based on (strategic) objectives of the enterprise and the related risk.

COBIT 5 Process Model

The COBIT 5 process model includes a number (37) of governance and management processes; this set of processes is the successor to the COBIT 4.1, Val IT and Risk IT processes, and includes all processes required for end-to-end treatment of all governance and management of enterprise IT.

Process Reference Model

This model is developed with best practices, standards and the opinion of experts. It is important to understand that the model and its contents are generic and not prescriptive, and it has to be adapted to suit the enterprise. Also, the guidance defines practices and activities at a relatively high level and does not describe how the process procedure is to be defined.

COBIT 5 for Assurance

COBIT 5 for Assurance provides a roadmap built from well-accepted assurance approaches that enable assurance professionals to effectively plan, scope and execute IT assurance initiatives, navigate increasing technology complexity, and demonstrate strategic value to IT and business stakeholders.

Product Code: CB5A
Member/Nonmember:
$35.00/$80.00

eBook Product Code: WCB5A
Member/Nonmember:
$35.00/$75.00

COBIT 5 for Risk

Effectively managing IT risk helps drive better business performance by linking information and technology risk to the achievement of strategic enterprise objectives.

Risk is generally defined as the combination of the probability of an event and its consequence. *COBIT 5 for Risk* defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

Product Code: CB5RK
Member/Nonmember:
$35.00/$80.00

eBook Product Code: WCB5RK
Member/Nonmember:
$35.00/$75.00

COBIT 5 for Information Security

COBIT 5 for Information Security aims to be an 'umbrella' framework to connect to other information security frameworks, good practices and standards. It describes the pervasiveness of information security throughout the enterprise and provides an overarching framework of enablers. The relevant information security frameworks, good practices and standards need to be adapted to suit specific requirements of the enterprise's specific environment. The reader can then decide, based on the specific needs of the enterprise, which framework or combination of frameworks is best to use, also taking into account the legacy situation in the enterprise, the availability of the framework and other factors. For this, the mapping of *COBIT 5 for Information Security* to related standards in appendix H will help find a suitable framework according to relevant needs.

Product Code: CB5IS
Member/Nonmember:
$35.00/$80.00

eBook Product Code: WCB5IS
Member/Nonmember:
$35.00/$75.00

COBIT 5 Bundle

Purchase the complete COBIT 5 Bundle and save!
The publications below are bundled together to provide a discount off the individual list prices. This set includes:

- COBIT 5
- COBIT 5 Implementation
- COBIT 5: Enabling Processes

Product Code: CB5S
Members SAVE $10—$95.00
Nonmembers SAVE $30—$120.00

eBook Product Code:WCB5S
Complimentary eBook available to Members.
Nonmembers—$80.00

NEW PUBLICATIONS

Announcing New Online Database Subscriptions for CISA and CSIM—Now Available in ISACA's Bookstore!

CISA Online Database—12 month subscription

Product Code: XMXCA15-12M
Member/Nonmember: $185.00/$225.00

CISM Online Database—12 month subscription

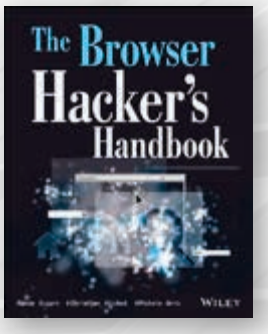
Product Code: XMXCM15-12M
Member/Nonmember: $185.00/$225.00

The *CISA®* and *CISM®* *Review Questions, Answers & Explanations Databases* are each a comprehensive pool of questions that combines the questions from their review manuals and their supplements.

Subscribe to the CISA or CISM exam online review course to:

- Have access to study at home, work or anywhere that best suits your needs
- Take sample exams with randomly selected questions and view the results by job practice domain, allowing for concentrated study in particular areas. Additionally, questions generated during a study session are sorted based on previous scoring history, allowing you to identify your strengths and weaknesses and focus your study efforts accordingly.
- And much more!

When you choose an online database, your subscription includes the exam preparation information from the *Review Questions, Answers & Explanations Manual* and *Supplement*.



The Browser Hacker's Handbook

by Wade Alcorn, Christian Frichot, Michele Orru

Product Code: 117WBH
Member/Nonmember: $44.00/$54.00

The web browser has become the most popular and widely used computer "program" in the world. As the gateway to the Internet, it is part of the storefront to any business that operates online, but it is also one of the most vulnerable entry points of any system. With attacks on the rise, companies are increasingly employing browser-hardening techniques to protect the unique vulnerabilities inherent in all currently used browsers. *The Browser Hacker's Handbook* thoroughly covers complex security issues and explores relevant topics.

Cloud Management and Security

by Imad M. Abbadi

Product Code: 118WCM
Member/Nonmember: $92.00/$102.00

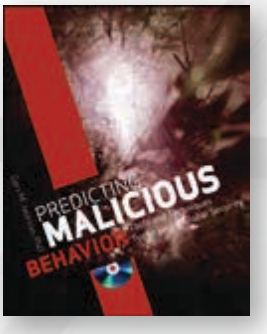
In this book, the author begins with an introduction to Cloud computing, presenting fundamental concepts such as analyzing Cloud definitions, Cloud evolution, Cloud services, Cloud deployment types and highlighting the main challenges. Following on from the introduction, the book is divided into three parts: Cloud management, Cloud security, and practical examples.

Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks

by MacDonnell Ulsch

Product Code: 108WCT
Member/Nonmember: $33.00/$43.00

Cyber Threat! How to Manage the Growing Risk of Cyber Attacks is an in-depth examination of the very real cyber security risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. Written by one of the nation's most highly respected cyber risk analysts, the book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences.



Predicting Malicious Behavior: Tools and Techniques for Ensuring Global Security

by Gary M. Jackson

Product Code: 116WPM
Member/Nonmember: $34.00/$44.00

This revolutionary book combines real-world security scenarios with actual tools to predict and prevent incidents of terrorism, network hacking, individual criminal behavior, and more. Written by an expert with intelligence officer experience, it explores the keys to understanding the dark side of human nature, various types of security threats (current and potential), and how to construct a methodology to predict and combat malicious behavior.

Browse over 450 publications featuring the latest research and expert thinking on standards, best practices, emerging trends and more at ***www.isaca.org/bookstore***

MEMBER GET A MEMBER

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.

MEMBER GET A MEMBER 2015 PROGRAM STARTS ON 1 AUGUST.

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

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

Be sure to go to *www.isaca.org/GetMembers* after August 1 to learn full details of this year's program.

INFLUENCE MORE

ISACA®

Trust in, and value from, information systems

* Rules and restrictions apply. Full rules will be available after 1 August 2015.

THERE'S NO SHORTAGE OF **CYBER SECURITY THREATS**

BUT THERE IS A **SHORTAGE OF IT SECURITY PROFESSIONALS**

DO YOU HAVE WHAT IT TAKES TO BE PART OF THE **SOLUTION**?

Cyber attacks are on the rise. Information security professionals are in high demand. Get up-to-date security skills with Capella University's master's or graduate certificate in Digital Forensics or Network Defense, aligned to the latest NSA focus areas.

The new graduate certificates can be completed in as little as 9 months, then applied toward your Master's in Information Assurance and Security (MS-IAS) to make an even bigger impact.

Plus, the knowledge you gained for your CISSP®, CEH®, or CNDA® certifications can help you earn credit toward your MS-IAS, saving you time and money.

ANSWER THE CALL. START TODAY TO LEARN MORE AND EARN MORE.

CAPELLA.EDU/ISACA OR **1.866.933.5836**

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

CAPELLA UNIVERSITY