Volume 6, 2015

ISACA® Journal

THE INTERNET OF THINGS

ADAPT. SURVIVE. THRIVE.

Featured articles:

The Criticality of Security in IoT

Back to the Future in Device Security

IoT—The Fate We Make Ourselves

And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG

NORTH AMERICA CACS

New Orleans, Louisiana | 2 – 4 May 2016

Make plans today to attend **North America CACS 2016** featuring world-class networking, customized learning opportunities and keynote speaker Tim Sanders.

SAVE THE DATE!

2–4 MAY 2016

Stay on top of information systems trends and opportunities. Join us at **North America CACS 2016** in **New Orleans, Louisiana**—the leading conference for audit, security and control professionals.

IN ADDITION TO EARNING UP TO 39 CPE HOURS:

- Gain tools and resources immediately applicable to your role and goals
- Choose from 60+ cutting-edge sessions and workshops
- Connect with highly respected IS/IT and business professionals

And don't miss special guest speaker Tim Sanders—Internet pioneer and *New York Times* best-selling author.

REGISTER EARLY AND SAVE US $200!*

Register at ***www.isaca.org/NACACSjv6***

*See website for pricing and registration details.

ISACA®

Trust in, and value from, information systems

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**?

Get up-to-date security skills with Capella University's Master's in Information Assurance and Security (MS-IAS), aligned to the latest NSA focus areas.

Earn up to three NSA Focus Area Certificates showcasing your mastery of skills in specific cybersecurity areas along the way to your MS-IAS.

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. **CAPELLA.EDU/ISACA** OR **1.866.933.5836**

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

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

Capella University

VOLUME 6, 2015

ISACA® Journal

Columns

Features

Plus

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

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 November and December.

Book Review: The Browser Hacker's Handbook
Reviewed by Ibe Etea, CISA, CRISC, CA, CFE, CIA, CRMA

Developing a Common Understanding of Cybersecurity
Deepak Rout, CISM, CRISC, CISSP

Book Review: Risk Assessment and Decision Analysis with Bayesian Networks
Reviewed by Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI

The Soft Skills Challenge, Part 3
Ed Gelbstein, Ph.D.

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

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

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

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

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

Cybersecurity for a "Simple" Auditor

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

A few issues back, I wrote about the US National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[1] In that article, I pointed out that the framework conflates information security and cybersecurity, which I believe should be differentiated. I received a very gratifying note regarding that article from Ian Sharland in South Africa, which said, in part, that he had "been struggling to articulate the differences—for our senior management—between our previous information security audit process (based on a combination of the COBIT®, ISO 27001 and ITIL frameworks/standards) and this cybersecurity audit process." Ian's message raised a question in my mind: What exactly is the cybersecurity audit process?[2] If, as I contend, cybersecurity is above and beyond information security, how then is the audit approach different?

LACK OF CYBERSECURITY STANDARDS

One difficulty in assessing cybersecurity preparedness is the lack of a standard to serve as the basis for an audit.[3] The NIST framework has become a *de facto* standard despite the fact that it is more than a little sketchy as to details. Though it is not a standard, there really is nothing else against which to measure cybersecurity. Moreover, the technology that must be the subject of a cybersecurity audit is poorly understood and is mutating rapidly. Auditors (and everyone else, for that matter) are hard-pressed to keep up.

Now, some auditors are learned and savvy in the ways of technology. I will leave it to them to teach us all the ways of finding the deep truths about cybersecurity. Right now, I would rather address myself to a "simple" auditor, one who is not so skilled in system internals and knows what not to ask.

A "simple" auditor should consider the fundamental difference between information security and cybersecurity: the nature of the threat. There is simply a distinction between protecting information against misuse of all sorts and an attack by a government, a terrorist group or a criminal enterprise that has immense resources of expertise, personnel and time—all directed at subverting one individual organization. To use a somewhat inapt analogy, I protect my car with a lock and insurance, but those are not the tools of choice if I see a gang armed with crowbars and chainsaws approaching my fender. This distinction, to my mind, is the very core of auditing an organization's preparations for defending itself against cyberattacks.

SIMPLE QUESTIONS

As is true in so many cases, the cybersecurity audit process begins with the objectives of an audit, which leads to the questions one chooses to ask. If a "simple" auditor only wants to know "Are we secure against cyberattacks?" then the answer should be written in stone: No organization should consider itself safe against cyberattackers. They are too powerful and pervasive for any complacency. If major television networks can be stricken,[4] if the largest banks can be hit,[5] if governments are not immune,[6] then the auditor's own organization is not secure either.

Still, "simple" auditors can ask subtle and meaningful questions, specifically focused on the data and software at risk of an attack. An audit process specific to cybersecurity might delve into the internals of database management systems and system software, requiring the considerable skills of a "tech-savvy" auditor. Or it might call for asking simple questions and applying basic arithmetic.

ARITHMETIC

If an auditor's concern is the theft of valuable information, the simple corrective is to make the data valueless, which is usually achieved through encryption. The "simple" auditor's question might be, "Of all our data, what percentage is encrypted?" If the answer is 100 percent, the follow-up question is whether the data are always encrypted—at rest, in transit and in use. If it cannot be shown that all data are secured all of the

time, the next steps are to determine what is not protected and under what circumstances. The audit finding would consist of a flat statement of the amount of unencrypted data susceptible to theft and a recitation of the potential value to an attacker in stealing each category of unprotected data.

Careful readers may note that data must be decrypted in order to be used and conclude that eternal encryption in use is, ultimately, a futile dream. There are vendors who think otherwise, but let us accept the concept that data will, at some time, be exposed within a computer's memory. Is that a fault attributable to the data or to the memory and the programs running in it? I say it is the latter. In-memory attacks are fairly devious, but the solutions are not. Rebooting gets rid of them and antimalware programs that scan memory can find them. So a "simple" auditor can ask, "How often is each system rebooted?" and "Does our antimalware software scan memory?"[7]

To the extent that software used for attacks is embedded in the programs themselves, the problem lies in a failure of malware protection or of change management. A "simple" auditor need not worry; many auditors (and security professionals) have wrestled with this problem and not solved it either. All a "simple" auditor needs to ask is whether anyone would be able to know whether a program had been subverted. An audit of the change management process would often provide a bounty of findings, but would not answer a "simple" auditor's question. The solution lies in having a version of a program known to be free from flaws (such as newly released code) and an audit trail of known changes. It is probably beyond the talents of a "simple" auditor to generate a hash total using a program as data and then to apply the known changes in order to see if the version running in production matches a recalculated hash total. But it is not beyond the skills of the people responsible for keeping the programs safe. An auditor need only find out if anyone is performing such a check. If not, the auditor can only conclude and report that no one knows for sure if the programs have been penetrated or not.

Finally, a "simple" auditor might want to find out if the environment in which data are processed can be secured. Ancient software running on hardware or operating systems that have passed their end of life are probably not reliable in that regard. Here again, a "simple" auditor need only obtain lists and count. How many programs have not been maintained for, say, five years or more? Which operating systems that are no longer supported are still in use? How much equipment in the data center is more than 10 years old? It is only arithmetic.

A "simple" auditor need not despair. In life, simple questions often lead to profound answers. If the questions are simple, but the answers are too complicated to understand, then who indeed is "technical"?

ENDNOTES

[1] Ross, S.; "Frameworkers of the World, Unite 2," *ISACA® Journal*, vol. 3, 2015

[2] I am not thinking exclusively of actions to be taken by members of an audit *function*. While surely auditors—internal or external—perform audits, independent assessments of the attainment of objectives, including control objectives, can be performed by any disinterested party.

[3] There are several excellent sources of information for auditors who would like to approach this subject, many of them from ISACA and the Institute of Internal Auditors. See particularly *Cybercrime Audit/Assurance Program*, ISACA, 2012, and *Cybersecurity: What the Board of Directors Needs to Ask*, ISACA and the Institute of Internal Auditors Research Foundation, 2014.

[4] *Le Monde*, Reuters, "TV5 Monde: les pirates n'ont pas diffusé de documents confidentiels de l'armée," *Le Monde*, 10 April 2015, *www.lemonde.fr/pixels/article/2015/04/10/tv5-monde-les-pirates-n-ont-pas-diffuse-de-documents-confidentiels-de-l-armee_4613876_4408996.html*

[5] Wilson, H.; "Millions Affected After Cyber Attack on HSBC," *The Telegraph*, 19 October 2012, *www.telegraph.co.uk/finance/newsbysector/banksandfinance/9621883/Millions-affected-after-cyber-attack-on-HSBC.html*

[6] Office of Personnel Management, "Information About the Recent Cybersecurity Incidents," USA, 23 June 2015, *www.opm.gov/news/latest-news/announcements/*

[7] Grimes, R. A.; "Should You Worry About Memory-only Malware?" *InfoWorld*, 4 February 2014, *www.infoworld.com/article/2608848/security/should-you-worry-about-memory-only-malware-.html*

Auditors and Large Software Projects, Part 3

Can Auditors Prevent Project Failure?

Ed Gelbstein, Ph.D., 1940–2015, worked in IS/IT in the private and public sectors in various countries for more than 50 years. Gelbstein 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. Thanks to his generous spirit and prolific writing, his column will continue to be published in the *ISACA Journal* posthumously.

This column (and the previous two, published in the *ISACA® Journal* volume 5[1]) focuses on a serious concern to business managers: What causes large software projects to have huge cost and timescale overruns and/or fail to meet expectations or, at worst, be abandoned before completion?

Part 1 of these series explored three areas that appear in the early stages of a project: The business case, the project risk analysis and the requirements definition. Part 2 explored three key management (and political) decisions: whether to buy or build software, establishing the project plan, and selecting the project manager.

This column focuses on auditing how the inevitable changes to the project are managed: Poor change control is a frequent cause of projects going wrong. COBIT® 5 devotes two sections (BAI06 and BAI07) to this topic.

CHANGE MANAGEMENT (ALSO REFERRED TO AS CHANGE CONTROL)

ISACA's Knowledge Center has an excellent article[2] on this topic that complements perfectly the change control process flow defined in the Information Technology Infrastructure Library version 3 (ITIL v3).[3] There are also several web sites that describe in detail the life cycle of changes.[4]

Some 40 years ago, while working in a critical information infrastructure operating 24/7/365, our director was a very capable man and also a bit of a dictator. Change control was mandatory and nonnegotiable, and a homemade workflow management system was used to support this process.

Years later and in other organizations, it became apparent that not everyone shared the view that poor change control leads to firefighting in operational activities and problems in software development. At that time, many internal auditors were not yet practicing risk-based audit and were unfamiliar with ITIL, which was introduced in the UK in the early 1990s.

Since the change management life cycle is straightforward, it is not difficult to buy or design a suitable application (there are several commercial offerings for the reader to explore). However, implementing such a system without a change management policy is pointless.

The challenge is getting people to comply with this policy for all changes to configurations, systems, application software, access rights and system privileges, and project plans. The usual reaction is to criticize, object and obstruct the initiative (despite briefings and explanations of the advantages of implementing this practice). Examples of objections include: "I have been doing this work for 20 years and I know what I am doing—I do not need more bureaucracy." Or, "UNIX programmers do not work like this."

The person with the 20 years of experience was invited to leave the organization (for other reasons). This led to the discovery that critical data center processes had been customized (2 million lines of partially documented code containing logical bombs to prevent their removal). Several times, the external auditors had highlighted the risk associated with this "indispensible individual," but management held this person in high esteem and had declined to act.

While removing this customization, the team understood the need for formalizing change managements and became its champion. Others had doubts until the day the global corporate network collapsed.

On a Monday, the day had started well, but by midmorning, the performance of the global network began to decline and then it died—nothing in and nothing out. A wide search for a possible cause was unsuccessful. Then a member of the team asked if anyone had been in the data center during the weekend. The data center's access control revealed that the networking lead engineer, who thought change control was a waste of time, had spent a morning there before leaving on a walking vacation in Norway.

Just as well, cellular telephony enabled us to contact him. He said he had an idea to optimize the network's router tables, and no, there was no record of it in the change control system because this was a simple change and there was no point in bureaucracy.

The network was reset to its original (documented) settings and everything was soon back to normal. After the networking engineer's return, we held a postmortem of the incident and reiterated how change control records would have saved the organization and its many users a lot of anxiety and aggravation. Shortly after this, the engineer decided to pursue his career elsewhere and there was no more argument about the mandatory nature of the change control system.

AUDITING CHANGE CONTROL PROCESSES

There is no point in attempting to duplicate the set of excellent documents of which these are just a small sample:

- *Change Control Audit Program and Internal Control Questionnaire*[5]
- *Change Management Audit/Assurance Program*[6]
- "Change Management"[7] guidelines from the Internal Audit Office, University of Queensland, Australia

Among other sources, there is a Change Management Body of Knowledge (CMBoK)[8] that has valuable guidelines for practitioners and auditors. CMBoK also covers organizational change and emergency changes; the latter appears rarely in projects, but is common in IT operations.

Here a somewhat different audit perspective on change management, in particular on capability areas and their maturity levels, is presented.

The model described here is a composite of several good practices and has six critical capability areas:

- **Leadership**—Sponsoring the institutionalization of change management; demonstrable senior management engagement in the application of this discipline; and defining business rules, policies and procedures, and ensuring compliance with them
- **Communications**—Establishing a culture that recognizes the value of change management, that the organization shares a common definition of what change management is, and that its use is regularly evaluated and improved
- **Application**—Making resources available for the practice of change management and defining those areas and/or functions where a common approach is mandatory, aiming for uniformity in practices and tools
- **Competencies**—Providing training and documentation, encouraging interchanges between experienced practitioners and learners, ensuring project teams collaborate and share change management knowledge
- **Authorities**—Change management policies and procedures define the approval mechanisms for proposed changes depending on the criticality, complexity and impact of the proposed change. This should also provide clear definitions of the minimum requirements for segregation of duties (SoD).
- **Standardization**—Aiming to have a standard approach to change management and a standard set of tools to support it, integrating the tools with project delivery processes, and ensuring that expertise and advice on change management can be readily accessed and shared

Each of these headings can be split into individual lines of audit and their maturity assessed and then summarized in a table similar to the one shown in **figure 1**. The goal is to reach levels 4 and 5.

Figure 1—Sample Maturity Table

Level 1: Nonexistent or *ad hoc*
Level 2: Change management is applied to isolated situations, but not with consistent practices.
Level 3: Change management is applied to multiple projects and/or operational activities. Good practices are identified and shared.
Level 4: Organizational standards for change management include common approaches and tools.
Level 5: Organizational competency—change management becomes part of the organization's way of doing things.

	Level 1	Level 2	Level 3	Level 4	Level 5
Leadership					
Communications					
Application					
Competencies					
Authorities					
Standardization					

Enjoying this article?

- Learn more about, discuss and collaborate on audit tools and techniques and change management in the Knowledge Center.

www.isaca.org/knowledgecenter

CONCLUSION

This column assumes that everyone shares the objective that projects should be completed on time and on budget and with functionality meeting expectations and causing no disruption.

However, despite progress in governance, risk management, project management and certifications, media constantly remind us that project overruns, operational disruptions and management frustration with IS/IT in their businesses still occur more frequently than one would wish.

Auditors who find that change management is not practiced as well as it ought to be should remind their auditees that those who go around looking for trouble usually find it. Thus, it is important to have the courage to raise the issue with senior management and the audit committee.

ENDNOTES

[1] Gelbstein, Ed; "Auditors and Large Software Projects, Part 1: Can Auditors Prevent Project Failure?," and "Auditors and Large Software Projects, Part 2: Can Auditors Prevent Project Failure?," *ISACA® Journal*, vol 5., 2015, *www.isaca.org/Journal/Pages/default.aspx*

[2] ISACA, *Change Management Audit/Assurance Program*, USA, 2001, *www.isaca.org/auditprograms*

[3] Axelos Ltd., ITIL v3, 2011, *www.itil-officialsite.com/*

[4] Doherty, Peter; Peter Waterhouse; *Change Management: A CA IT Service Management Process Map*, CA Inc., June 2006, *www.itsmcampus.com/ca_public/30264_change_mgmt_processmap.pdf*

[5] PRINCE2 Primer.com, Prince2 Video Primer, *www.prince2primer.com/change-control-procedures*

[6] *Op cit*, ISACA

[7] Internal Audit Office, "Change Management," University of Queensland, Australia, 2002, *www.uq.edu.au/internal_audit_office/STRATEGIC_PLAN_files/Guidelines-for-Change-Management.pdf*

[8] Change Management Institute, *The Effective Change Manager: The Change Management Body of Knowledge (CMBoK), https://www.change-management-institute.com/buycmbok*

Nickson Choo

Nickson Choo, CISA, CRISC, CFE, has more than 24 years of corporate and professional experience. He started his career in the internal audit function of a Fortune 1000 insurance company and has more than 12 years of insurance experience working in several life and general insurance companies in various operational positions. He was the president of the ISACA Malaysia Chapter in 2004 and 2006-2008. Choo currently serves on the board of governors of IIA Malaysia and was the chair of the ISACA Membership Growth & Retention Committee from 2012-2015.

Q: As a risk and governance professional, how do you believe your background in IT audit has supported and guided your career to date?

A: I believe my background in IT auditing gave me the foundation to help my clients identify process improvement opportunities and system controls expected within each system. In addition, being an IT auditor and knowing all the risk factors also helped me appreciate the nature of the client business better.

As I have progressed in my career in the risk advisory services, my background has allowed me to better advise and guide my clients toward achieving their business objectives while balancing the costs and benefits of good controls. I have learned that in this world where we are increasingly dependent on technologies to assist us, the principles I have learned from being an IT auditor have allowed me to better assess any given technologies.

Q: What do you see as the biggest risk factors being addressed by governance of enterprise IT (GEIT) professionals? How can businesses protect themselves?

A: One of the biggest risk factors we face is really from the cybersecurity realm. Companies are regularly reacting to threats and cyberattacks. This is especially true in Malaysia and surrounding regions where political sensitivity is at an all-time high within each country and even between countries.[1]

Other key threats include protection of business information as we have seen leakages of crucial and sensitive documents and communications being published online causing untold embarrassment and public relations nightmares for businesses. Increasingly, companies need guidance and assistance from IT professionals to be able to protect their businesses against such threats without disruption to their operations and business objectives.

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

A: My number-one piece of advice to anyone who wishes to pursue a similar career path is to join ISACA®. To be successful in this industry, you need to stay up to date on the latest in the industry and ISACA provides excellent resources in this area. In addition, ISACA certifications are sought after and provide that needed assurance of your skills and knowledge to employers and clients.

I have been a member of ISACA for more than 15 years, and the local chapter has provided me an excellent platform from which to network, interact and exchange ideas with my peers. The continuing professional educations programs in place have been key to developing and enhancing my skills and knowledge in IT audit, risk management and governance.

Q: Having begun your career in IS audit, how do you think the role of the IS auditor is changing or has changed? What would be your best piece of advice for IS auditors as they plan their career path and look at the future of IS auditing?

A: If you are starting off as an IS auditor, I would say that you have made the right choice. This profession is highly sought after and will continue to be in high demand as a result of society's and businesses' dependency on technology. An IS audit world will no longer be confined to just auditing a core business system, but will open up to include mobile devices, cloud-based systems, Internet devices and multiple storage sites. Undoubtedly, the required skill sets and expectations of an IS auditor will increase significantly but, of course, the rewards and remuneration will increase proportionately as well.

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

A: I guess the biggest workplace challenge I have faced is the lack of good IT audit resources. Although we have lots of IT graduates each year into the market place, they lack the required skill sets and knowledge required. ISACA is trying to accelerate this process by introducing a model syllabus, forming ISACA student groups and appointing academic advocates at selected universities. All of these efforts will help create graduates who are able to quickly integrate into businesses and help fill the shortage of IT audit resources.

ENDNOTE

[1] Yutim, Haider; "Indonesians Fury Over 'Fire Your Indonesian Maid' Ad," 4 February 2015, *http://english.astroawani.com/malaysia-news/indonesians-fury-over-fire-your-indonesian-maid-ad-53340*

Do you have something to say about this article?

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

Go directly to the article:

WHAT HAS BEEN, OR DO YOU ANTICIPATE BEING, THE BIGGEST COMPLIANCE CHALLENGE IN 2015? HOW WILL YOU FACE IT?

Cybersecurity. Every business must have a program in place to periodically assess its security posture and continue to invest and upgrade its hardware and technologies to reduce risk in this area.

WHAT IS YOUR FAVORITE BLOG?

Dilbert. It is awfully funny and sometimes seemingly meaningless, and yet it can mean so much.

WHAT IS ON YOUR DESK RIGHT NOW?

- 3 powerbanks (one can never get enough of them)
- An external hard disk drive (encrypted of course)
- My trusted iPhone
- A tray full of old IT-related magazines

HOW HAS SOCIAL MEDIA IMPACTED YOU PROFESSIONALLY?

LinkedIn has helped me to connect with other similar IT professionals, as well as identify and connect with existing and potential clients.

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

Join ISACA and keep yourself updated. The day you stop receiving updates on what is happening in the industry is the day you start becoming obsolete.

WHAT IS YOUR FAVORITE BENEFIT OF YOUR ISACA MEMBERSHIP?

The local chapter networking events. The ISACA Malaysia Chapter has some of the best and most fun networking events around.

WHAT DO YOU DO WHEN YOU ARE NOT AT WORK?

When I am not at work, I am kicking up dirt on a golf course somewhere and trying hard to be a better golfer.

Transparency and the IT Professional

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

The word "transparency" originated in the field of engineering. It has to do with the physical property that allows the transmission of light through a material, such as glass or plastic. It has become popular in many other disciplines since the mid-1980s. While the engineering definition of the term remains unchanged, there seems to be hardly any clarity in its meaning or usage in other disciplines.[1] It almost seems like the presence of transparency in all but the engineering field is suffering from opaqueness!

The distinction between transparency as a physical property and transparency as an information attribute is important here. The latter has a value connotation; its practice lies in economics, society, business, and politics in the form of the receivers' right to know, to be informed. "Respect for transparency is not simply value added to a corporation's line of goods and services, but a condition of a corporation's justifiable claim to create value rather than harm, wrong, or injustice in its dealings."[2] Thus, the entity responsible for transparency carries the duty of a moral agent to its stakeholders. As a means to an end, information transparency is "not an ethical principle in itself but a pro-ethical condition for enabling or impairing other ethical practices or principles."[3] Transparency is a means to achieve justice or well-being.[4]

The product of transparency is more like an X-ray output, where we are not attempting to look through the body, but rather look into the body in an indirect manner; that is, without accessing the body as such and instead, interpreting and evaluating images (e.g., text, graphs, pictures), such as the X-ray film, to make decisions (e.g., diagnose the health issue and prescribe treatment).[5] Information transparency requires that the content provided is understandable, adequate (granular) and reliable (trustworthy), for example. Finally, the recipients of information judge transparency; what matters is transparency as they perceive it to be. To the entity that strives to meet transparency requirements, what matters are the justifiable expectations of the receiver of the information. To continue with the example, the physician's information needs should be met from the X-ray film, not just the technician's standards for its production.

Thus, in nonengineering fields, the word has to do with (information) communication or information transparency. Since inaccessible stored data cannot be assigned any meaning by the receiver of information, information communication is an important context or a prerequisite condition to exhibit transparency; thus, terms such as "disclosure" or "communication" are used to describe an act of transparency. Since any communication involves the sender and the receiver, typically the sender is the entity responsible (often called "agent") and the recipients are its stakeholders, or the beneficiaries of the communication. Using provided information, the recipient either (1) confirms confidence in the state reported or (2) assigns it a level of trust and uses it for decision making. The former disclosure necessitates describing something in detail and the latter, offering reasons.[6]

FINANCIAL AND TECHNOLOGY TRANSPARENCY

In the fields of economics and finance, an important link between transparency and governance is established by regulators of financial markets, making public companies responsible for certain disclosures. For example, the US Sarbanes-Oxley Act of 2002 requires that both the chief executive officer (CEO) and the chief financial officer (CFO) of a registered company certify the state of internal controls and the accuracy of financial information communicated by management. The purpose is to reduce information asymmetry across the investor community and, thus, contain the problem of some benefitting from the privileged information (e.g., insider trading). Mandating transparency in this way requires content-related judgments (e.g., what information, when) to protect the recipients' rights to treat such information as reliable and timely.

It is important, however, to note that such mandates may not always produce consistent

results. For example, the US Securities and Exchange Commission (SEC) recently added as a requirement that any significant risk related to cybersecurity should be discussed in quarterly and annual filings by the company with the SEC. The result is a rather broad spectrum of disclosures, ranging from no disclosures to boilerplate statements to rather elaborate statements regarding the state of cybersecurity at the company.[7]

An argument can be made that the idea of transparency is technology neutral; it existed well before the emergence of technology, especially information technology. However, as an intermediary enabler, technology adoption changes the fabric of society and its interaction. Thus, since it impacts society, it has an impact not on the meaning of transparency, but certainly on how it will be delivered. Virtual reality (e.g., second life), artificial intelligence (e.g., robotics, drones, driverless cars), social networks (e.g., Facebook, Twitter, LinkedIn) and the Internet of Things (IoT)—have all contributed to rather challenging dilemmas. Privacy is just one example that pervades most of these scenarios.

Whereas the goal of transparency in financial markets' regulation is to facilitate informed decision making, a corresponding goal in the field of information and communication technology is primarily to breed confidence in the system. For example, the disclosure of cybersecurity risk presumably allows an investor to assess pertinent risk exposures impacting the decision to invest in a company. Content is important, but what defines content (i.e., the norms, standards, protocols, practices [policies]) is equally important. Thus, the disclosure requirements drive decisions regarding what is important to communicate (e.g., data capture, storage, protection, dissemination). For example, transparency-related issues of privacy of information do not specify content, but rather dictate privacy policy and system requirements that will achieve the goal of protection of privacy.

In sum, it appears that in dealing with transparency, economic systems present a strong bias in favor of reliable information that levels the playing field, while as an enabler, information technology is biased toward processes, platforms and applications that warrant the interested party's confidence (e.g., in matters of privacy) or that generate new contexts and challenges in the practice of transparency (e.g., social networks).

ACHIEVING TRANSPARENCY

In a study of nongovernmental organizations (NGOs) striving to achieve transparency through maximum disclosure via their web sites, various challenges surfaced. The researchers found that the web-enabled disclosure is limited by privacy and security concerns and by pressure from financial supporters and benefactors and potential NGO competitors who vie for grants and donations from the same or similar sources.[8] Balancing such conflicting demands could constrain transparency, although the technology (in this case, the web site) exists to cost-effectively maximize disclosures. What not to disclose, or how much to disclose, is a sensitive issue illustrated by the question: How much information should Apple have disclosed when it learned about Steve Jobs' illness? The privacy rights of the executive need to be balanced against the desire of the investors to know if there would be a leadership vacuum at Apple.

The bottom line in the practice of transparency is establishing trust of the receiver in the sender. A recent controversy that is brewing has to do with whether the US National Security Agency's (NSA) access to, and use of, people's phone call data violates the fundamental privacy rights of individuals. On this issue, to put their customers at ease, Apple and Google introduced new features in their smart phone software that prevents others from unlocking encrypted material, even if faced with a warrant.[9]

> "The bottom line in the practice of transparency is establishing trust of the receiver in the sender."

Such conflicts emerging these days have their roots in Internet-based data, communication and services. When Apple promises to make its phones so that the government cannot decrypt messages transmitted using its devices, one might applaud Apple for its courage to limit transparency and protect privacy. However, could the NSA add or extend its regulatory power to not allow phones to use encryption technologies that the agency could not decrypt?

To be transparent, how much data should an agent disclose? To gain trust, the agent might strive to disclose in great detail the pertinent information. However, the disclosure of sheer volumes of data does not transfer reliable information to the recipient.[10] For this to happen, the agent will often have to filter the data so that the disclosure is confined to what is relevant.[11] To display what is not relevant or not display what is relevant would compromise the objective; the former creates noise in the communication and the latter produces incomplete information.

Where necessary, the agent should filter data and transmit what is relevant, but data filtration to generate (relevant) information is no easy task.

Finally, Wikipedia provides an interesting context of how transparency issues dovetail with what technology delivers. While Wikipedia uses largely transparent writing and editing processes that potentially produce information that is reliable for the user, it remains silent on one aspect of these processes. This has to do with the nondisclosure of the identity of contributors, editors and administrators. This particular lack of transparency jeopardizes the (perceived) validity of the information being produced by Wikipedia.[12] No one discounts the huge value addition Wikipedia brings to society, but lingering doubts remain about the quality of its information.

WHEN NOT TO BE TRANSPARENT

Interestingly, not being transparent would most likely mean one is hiding something that others might think should be in plain sight. A primary defense for keeping a secret is likely to be the protection of something of value such as protection of assets (e.g., Coca-Cola's recipe) or human lives. The chameleon changes its color to camouflage itself. And even after decoding the Enigma messages, Alan Turing convinced the British army to not openly claim this knowledge, but rather create an artifact of otherwise believable evidence to act on the same targets that the decoded messages identified.[13] Not masking the truth would have resulted in winning the battles, but not the war, for the enemy would have changed the encryption key. But even here, Kerckhoff's principle says that every secret creates a potential failure point and, thus, "brittleness" in the system that could result in a major collapse of the organization.[14] Accordingly, in cryptography, the algorithm could be public knowledge, but the key, which can be changed without much cost, is not.

A key consideration here is the agent's (information provider's) assessment of the recipient's need to know, which, in turn, dictates what and how much information will be communicated. For example, a company's proprietary code does not need to be divulged; however, if it launches an open source code, potential beneficiaries depend heavily on complete transparency of the code and its revisions, for the end user must be able to view and alter the source code.[15]

Many businesses thrive on anonymity. Examples include the Swiss banks that promise to protect privacy of bank accounts, the Bitcoin ecosystem that believes in anonymity of the transacting party, and Ashley Madison—a company that runs a dating web site serving those looking for extramarital affairs, where secrecy of clients' personal information is critical to the site's success. Could such entities be forced to be "transparent" with regard to things they commit to keep anonymous? Perhaps not. However, some believe that such anonymity is unjustified and, therefore, want to champion the cause of harming them. For example, an intruder who hacked Ashley Madison's system claims to have personal information of their customers and intends to divulge it unless the site is shut down.[16] I believe this is not the case of a company not being transparent; rather, the challenge lies in whether people believe in the legitimacy of their business model and how they create value.

When not to be transparent? A minimum of three rules should be applied to decide what to disclose and how much to disclose at a given point in time. First, is the information proximately relevant to the recipient's interests in the agent? If the answer is yes, the company should proceed to the next question: How much granular information will be enough to honor the rights of the receiver? This may be a question of judgment; however, it needs to be addressed in some manner. Third, in putting out the details, are the rights of any other stakeholders compromised? If yes, what would be the best way to balance the conflict between what is appropriate to disclose and what needs to remain undisclosed? These suggest that the practice of transparency remains clouded despite efforts to lay out some structure and rules of conduct. It appears that judgment cannot be removed from decisions about being transparent. Stay tuned for the possibility of more clarity on transparency in the future.

ENDNOTES

[1] Michener, G.; K. Bersch; "Conceptualizing the Quality of Transparency," *1st Global Conference on Transparency*, 17-21 May 2011, Rutgers University, New Jersey, USA

[2] Elia, J.; "Transparency Rights, Technology, and Trust," *Ethics and Information Technology*, vol. 11, 2009, p. 145-153

[3] Turilli, M.; L. Floridi; "The Ethics of Information Transparency," *Ethics and Information Technology*, vol. 11, 2009, p. 105-112

[4] Menendez-Viso, A.; "Black and White Transparency: Contradictions of a Moral Metaphor," *Ethics and Information Technology*, vol. 11, 2009, p. 155-162

[5] *Op cit.*, Mendez-Viso, p. 160

[6] Pieters, W.; "Explanation and Trust: What to Tell the User in Security and AI?" *Ethics and Information Technology*, vol. 13, 2011, p. 53-64

[7] Morse, E. A.; V. Raval; J. R. Wingender Jr.; *Market Price Effects of Data Security Breaches*, working paper, 2015

[8] Vaccaro, A.; P. Madsen; "ICT and an NGO: Difficulties in Attempting to Be Extremely Transparent," *Ethics and Information Technology*, vol. 11, 2009, p. 221-231

[9] Yadron, D.; "Former Heads of Homeland Security, NSA Back Encryption," *The Wall Street Journal* Tech Blog, 29 July 2015, *http://blogs.wsj.com/digits/2015/07/29/former-heads-of-homeland-security-nsa-back-encryption/*

[10] In this sense, the Internet, by itself, is not transparent.

[11] See R. L. Ackoff's classic article, "Management Misinformation Systems," *Management Science*, 1967, p. 147-156.

[12] Santana, A.; D. J. Wood; "Transparency and Social Responsibility Issues for Wikipedia," *Ethics and Information Technology*, vol. 11, 2009, p. 133-144

[13] Hodges, A.; *Alan Turing: The Enigma*, Princeton University Press, USA, 2014

[14] Kerckhoff's principle, *www.crypto-it.net/eng/theory/kerckhoffs.html*

[15] Vuorinen, J.; "Ethical Codes in the Digital World: Comparisons of the Proprietary, the Open/Free and the Cracker System," *Ethics and Information Technology*, vol. 9, 2007, p. 27-38

[16] Yadron, D.; "Hackers Target Users of Infidelity Website Ashley Madison," *The Wall Street Journal*, 20 July 2015, *www.wsj.com/articles/affair-website-ashley-madison-hacked-1437402152*

Cloud Computing as an Enabler of New Business Models and Start-ups

Aligning On-demand SME Needs Through Cloud Computing

Angelique Schouten is cofounder and chief executive officer of Cloudtract, a free and simple contract management solution for small and medium-sized enterprises. Schouten has more than a decade of experience in cloud banking, software development, marketing and start-ups.

As a free and simple cloud-based contract management application for small and medium-sized enterprises (SMEs), Cloudtract supports businesses by aligning on-demand needs based on embracing cloud computing integration. Cloud computing's efficient systems and processes create the opportunity to drive innovation in businesses and support the optimization of operational flexibility and minimization of inexplicit costs that are critical enablers for attaining long-term business stability. But perhaps the biggest advantage of cloud services is the fact that their infrastructure is already in place, making cloud-based software instantly available and functional, remarkably shortening its setup life cycle in comparison to noncloud platforms. Cloud technology helps SMEs run and coordinate large external workforces, support operational management, and enable the building of new developments to ensure that they stay up to speed and futureproof within their markets. As industries are thriving using on-demand business models that require speed to market, agility and flexibility, SMEs are almost unequivocally directed to cloud technology implementations, which fit perfectly with the current behavioral profile of SME businesses. But how does this work in real-life situations?

> "As industries are thriving using on-demand business models that require speed to market, agility and flexibility, SMEs are almost unequivocally directed to cloud technology implementations."

TRYING TO REVIVE A STRUGGLING COMPANY

This all sounds quite logical and practical, but the immediate questions are how cloud computing can be implemented and what benefits can be materialized. Answering these questions will require stepping back in history a few years and looking at a practical case. A traditional middle-sized insurance company is struggling to hold onto its market share and seeking ways to reduce costs and reinvent itself. The company hired a new head of marketing and a new head of IT. Both new managers started by reviewing existing contracts with suppliers and deciding which contracts to prolong or cancel. It took these managers about eight weeks to locate all contracts, only to find that the company was wasting money on contracts for services that did not get used. Contracts, some dating back many years, were found all over the place in various folders and cabinets and on different desks.

The inventory led to a decision to cancel several contracts, including a €40,000 IT contract. The employee who was responsible for the contract was also responsible for securing a new contract with a different supplier; regrettably, he focused only on negotiating the new contract and forgot to cancel the old one by the deadline date, thus wasting €40,000. A mistake like this is unacceptable for all companies, large and small. So, the quest for a simple and safe contract management solution was undertaken. An analyses of existing systems showed that the market was overflowing with traditional software vendors offering over-engineered traditional enterprise resource planning (ERP) systems or expensive pay-per-use models. So what does an organization do in this cloud-based era? It designs and develops a suitable solution itself: Cloudtract.

€40,000 MISTAKE + CLOUD COMPUTING

When there is no sense of urgency, change is mostly far away. In the case of Cloudtract, a €40,000 mistake created the sense of urgency. In

Do you have something to say about this article?

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

Go directly to the article:

the "old" world, starting a new company would not be feasible due to the large hardware investments needed, especially if large volumes of data are the key business.

Cloudtract was founded based on the integration of cloud technology, considering its suitability to deliver computing resource advantages. As an online, cloud-based contract management solution for businesses, Cloudtract developed an application that fully enables scalability for a greater-proportioned user base. Features of the application allow businesses to set alerts for expiring contracts and store their contracts and other related documents in the cloud, allowing instant access and increased accessibility.

With scalability allowing an increase of computing power and data storage capacity, delivering a high-demand computing capacity and cost savings, businesses do not have to invest in physical space requirements and utility costs to set up traditional data center environments. Flexible and fast time-to-market benefits require the need for scalable computer resources and data storage server space.

The main benefits for starting up a new company that is fully cloud-based and has a virtual private cloud (VPC) at the heart of the company are:

- **Low and flexible cost operating model**—Cloud computing shifts from a fixed to a variable cost model and allows a pay-as-you-go model.
- **Scalability**—When data are at the heart of a company, growing quickly is essential. Cloud computing provides relatively low-cost, unlimited computing power to support this growth.
- **Availability**—Not only can the company focus on uptime with applications due to several cloud availability zones, it also enables the company to deploy new features more quickly, resulting in a shorter time to market.
- **Connectivity**—Cloud computing combined with web services enables the company to connect easily to third-party applications, which, in itself, increases market reach.
- **High security standards**— Because cloud computing is very focused on security, it upholds the highest security standards possible with accompanying accreditation and additional security and encryption layers.

CLOUD BENEFITS

The facilitation of data and data storage has become a commodity. As diversified demands result in the development of distinct specialized solutions that need to be quickly developed, tested and implemented, cloud technology delivers immediate provisioning of computing service needs and facilitates the on-demand economy requirements of businesses today. Given that cloud technology provides the perfect conditions for an extensive development, test, acceptance and production (DTAP) environment, finding qualified and experienced system operations (SysOps) staff to manage these environments seemed to be the only challenge.

Another important aspect in the development of the new company was the appeal for security of data. Using cloud-based infrastructures, the application is systemically required to comply with high security standards. Cloudtract operates in a VPC environment, which enables customizing network configurations and leveraging different levels of security.

As the scalability benefits and demands for data delivery opportunities for new business models regarding data and algorithms, the contract management tool is currently based on a freemium model, allowing the usability to continuously develop and offer additional features based on user input, market value, and interchangeable consumer needs and insight. Within an environment where businesses can access shared pools of configurable computing resources, drivers for potential new businesses can be identified through enhancing customer value propositions, increasing collaborations with

external partners, creating new delivery channels, creating competitive differentiation through specialization and vertical integration, and allowing flexible pricing models.

DATA SECURITY AND RISK COMPLIANCE CLOUD COMPUTING

With the expansion of cloud computing functionalities comes the need for effective security. Like controlling any other IT environments, the challenges of securing data, such as data loss, data leakage, service downtime, regulatory constraints, and risk of intellectual property theft, are amplified in the cloud model. For the service of monitoring and storing data to integrate with business administration of SMEs, cloud technology offers the best solution in which organizations/clients can store, retrieve and possibly modify data. To adopt the right cloud computing strategy as a business, drivers must be aligned with enterprise goals and objectives, and business and cultural factors must be favorable.

> "With the expansion of cloud computing functionalities comes the need for effective security."

In the case of Cloudtract, this means that data security is essential. On top of the VPC, encrypted disks are used by the cloud provider. All data are encrypted twice and procedural measures are taken to control the environments. When data security and availability of the data are important, choosing a cloud provider with several availability zones is crucial.

IMPORTANCE OF CLOUD PROVIDER

SMEs experience evolving priorities. The underlying infrastructure necessitates that security of an organization's cloud-based solution be based on a shared responsibility between it and the cloud provider that promises operability, risk transparency and audit governance. When structured on these basic foundations, the benefits of cloud technology will structurally comply with the purpose-driven integration for operational business procedures. Specific regulatory and business compliance requirements have to be made clear to users to specify the security of data. When starting a new company, criteria as a starting point for selecting a cloud provider include:

- Overall pricing
- Global presence and regional availability zones
- Security measures and standards
- Additional services and the development speed of these services

RESISTANCE IS FUTILE

The choice to enable cloud technology for conceptualizing a contract management solution makes sense due to how well cloud computing fits SME needs and the benefits it brings. The on-demand needs of the organization bolster arguments for cloud technology usage based on flexibility, availability, accessibility and data security.

The famous saying from *Star Trek*,[1] "Resistance is futile, you will be assimilated," might seem negative, but it is true here and cloud computing is an unstoppable, positive development. Cloud computing is here to stay and has become the new standard in doing business for large enterprises, SMEs and start-ups. It facilitates an entire new ecosystem of on-demand companies and redefines industry standards. The question is to what extent the owners of IT infrastructures are open to investigating the possibilities and tackling the challenges ahead.

ENDNOTES

[1] *Star Trek*, 1966-1969, is an American science fiction episodic television series created by Gene Roddenberry and owned by CBS and Paramount Pictures.

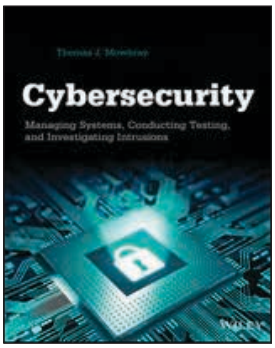
Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions

Reviewed by Andrew Richardson, CISA, CISM, CRISC, MBCS, MCMI, who is the group information security officer at AEGON UK. Richardson has more than 25 years of experience in IT, information security, audit and risk.

Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions is aimed at cybersecurity students and graduates, cybersecurity practitioners, enterprise architects, and information security professionals. Although it has a section covering security concepts, it is a practical guide for protecting networks, systems and data against cybersecurity threats.

The book is divided into three sections, comprising a total of 14 chapters. The three sections cover cybernetwork security concepts, hands-on cybernetwork security and cybernetwork application domains.

The first two chapters focus on anti-patterns, which are ineffective and potentially counterproductive common responses to recurring problems. The term, coined in 1995 by Andrew Koenig, was inspired by the book *Design Patterns*, in which the authors highlighted a number of design patterns in software development that they considered to be highly reliable and effective.



By Thomas J. Mowbray

By looking at cybersecurity anti-patterns, the book introduces the reader to a different way of thinking about cybersecurity. The book goes on to look at examples of anti-patterns, such as document-driven certification and accreditation, the use of information assurance standards with no proven benefits, and policy-driven security certifications that do not address threats. The book then focuses on the most common mistakes made in cybersecurity, describing how and why anti-patterns are created and how anti-patterns can be beneficial to the reader.

Cybersecurity has a different way of looking at the problems of cybersecurity, as most publications focus on best practices and what should be done. This publication looks at the anti-patterns that occur (e.g., no time for security) and describes the background, solutions, causes, symptoms and consequences, known exceptions, and the possible solutions to these problems. The end of part one of the book looks at enterprise security and using the Zachman Framework as a baseline reference model. Again, the focus is on anti-patterns and how they can be used.

Part two of the book deals with hands-on cybernetwork security in the form of network administration, the customization of backtrack and security tools, protocol analysis and network programming, vulnerability assessment and cybertesting, penetration testing, and the use of log analysis for cybernetwork defense. This covers elements such as managing administrator and root accounts, installing hardware, setting up networks, and reviewing a variety of other network administration tasks across Windows, Linux and VMWare. Part two of this book is a practical resource that provides the reader with detailed instructions that can be followed.

Part three covers the essentials for end-user cybersecurity awareness and education. It covers cybersecurity for end users, small businesses, large enterprises and health care organizations. The book concludes with a final chapter covering cyberwarfare.

The book is practical in its approach and does not just talk about theory. It provides practical examples of how to stay safe with email and tips on how small businesses that may not have cybersecurity experts on which to rely can put an enterprisewide cybersecurity plan into place.

Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions provides the reader with a well-rounded publication on cybersecurity that can be used to establish practical controls over all aspects of cybersecurity. This book would be a useful additional to any security professional's bookshelf.

EDITOR'S NOTE

Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

The Criticality of Security in the Internet of Things

Rebecca Herold, CISA, CISM, CIPM, CIPP/US, CIPT, CISSP, FLMI, is founder and chief executive officer of The Privacy Professor and cofounder and chief visionary officer of SIMBUS360. She has more than 25 years of information security, privacy and compliance experience; has published 17 books; and is an adjunct professor for the Norwich University (Northfield, Vermont, USA) Master of Science in Information Security and Assurance (MSISA) program.

For the past several years, a lot of research, writing and speaking has been focused on the Internet of Things (IoT) and the smart devices that are used within it. The technology is evolving faster than most can keep up with all the reports that are published. It is also a misnomer to keep referencing it as the IoT when, in progressively more instances, the Internet is not even involved. It is becoming more like the Network of All Things (NoAT), with more capabilities that are emerging for smart devices to communicate directly with each other in ways that go beyond the long-standing peer-to-peer (P2P) communications. And as these new technologies emerge, many are not being designed under any existing legal requirement to include security and privacy controls. For example, wearable fitness devices, home energy controllers, driverless and Internet-connected cars, smart watches, and many others seem to be designed with an ultimate goal of being newsworthy for how much data they can collect, analyze and share, without the auspices of virtually any regulatory authority to establish a minimum set of security and privacy controllers. Establishing security and privacy requirements for these growing numbers of personal smart devices is needed yesterday.

With all these new smart technologies and devices, most of them collecting, storing and communicating data without any action necessary by the individuals using them, it becomes more important than ever to build security and privacy controls into the devices.[1] While the technologies are new, the information security concepts that should be applied are not new; data security concepts that have been used for five to six decades or more can be applied within these gadgets, as can the comparably newer privacy control concepts.

In addition to the need for the engineers creating smart devices to build in data security and privacy controls, those businesses that have their employees using such gadgets, and businesses whose employees are using their own such gadgets while working, also need to establish parameters and rules around that use.

SMART DEVICES ARE INCREASINGLY BEING USED

How many of us are aware of any smart device development going on in our organizations? How many of us are aware of the smart devices that may soon be introduced within our environment or may already be in use? This is something on which all information security and privacy professionals and IT auditors, collectively referenced here as information assurance (IA) professionals, need to stay up to date. Here are just a few examples of some of the smart devices that have emerged over the past 15 years:

- **Mobile phones, which evolved into smart phones**—Smart phones were introduced in January 2007, with the introduction of the iPhone.[2] This was arguably the first type of widely used IoT device. Smart phones are now pervasive,[3] and the reach of data accessible from and to them is now significantly greater since they have applications (apps) and/or global positioning systems (GPS) installed. Do organizations know how many of their employees are using smart phones while also performing business activities? Employees could be bringing significant risk to the organization if their mobile devices are not properly controlled.
- **Medical devices**—Interest in these devices gained significance in 2007 when then-US Vice President Dick Cheney had his doctors disable the wireless connection to his pacemaker because he feared terrorists would hack into it and turn it off to kill him.[4] Many, and perhaps most, medical device manufacturers do not build any or, quite frankly, build negligible security and privacy controls into their devices.[5]
- **Smart meters and other smart devices within the smart grid**—One topic that comes up frequently in the group discussions of the US National Institute of Standards and Technology (NIST) Smart Grid Privacy Group[6] and the Smart Grid Interoperability Panel (SGIP)[7] (which the article's author has led since 2009) is how the smart devices being introduced into the smart grid will impact privacy,[8] particularly

those devices that are used by consumers and communicate directly with a wide number of smart device vendors without any regulations or industry standards.[9] It is likely that the evolution of smart meters and smart devices in this space will accelerate in the coming years, bringing with it privacy and security issues that have not yet been imagined.

- **Wearable fitness monitoring devices**—There are some wearables that are prescribed by health care providers[10] but do not fall under the traditional definition of a medical device that is regulated in the US by the Food and Drug Administration (FDA). There are also increasing numbers of fitness and health monitoring devices sold directly to consumers to help them keep track of exercising and specific types of health data, such as blood sugar levels and heart rate. The great success these wearables have had with helping their users to lose weight[11] is very seductive and leads those using them to become lax or nonchalant with regard to making sure they have appropriate security and privacy controls in place. Businesses are now even providing fitness monitoring devices to their employees to wear, with the businesses monitoring them to provide compensation incentives, which opens up a huge realm of privacy concerns.[12]
- **Smart home devices**—These include such devices as Amazon's Echo,[13] home security and baby monitors,[14] smart televisions (TVs),[15] and a wide range of home environment controllers.[16] These, too, are generally unregulated, and the data collected could be going to a very large number of third parties[17] of which the users have no knowledge. And, as the hack of the home security monitor that occurred in 2013[18] demonstrated, the need to build in security controls is great, and the possible privacy harms to those using the devices could be catastrophic, not to mention the fines and sanctions to the company providing the device.[19] In the US, lawmakers are looking to adopt new laws to secure these gadgets.[20] It is important for readers to know whether their countries are also considering such laws.
- **Smart cars**—Having computers perform various functions in cars is nothing new; the first computers were put into cars in the late 1970s to provide some engine controls.[21] However, beginning around 1995, it became common for cars to have a controller area network (CAN) to connect with and gather data from various types of sensors about different areas and parts of the car using wires and software protocols known collectively as the CANbus.[22] Today, microcomputers control a wide range of functions within automobiles such as braking, air bags, the horn, the locks and the ignition. They also track such things as location of the vehicle using GPS, the inflation of tires using sensors, the speed of the car at any given time and the path that is driven. These computers are wirelessly connected to more third parties than most drivers realize: Internet services providers (ISPs) enabling in-vehicle Internet access; OnStar and similar services that support emergency help; and, increasingly, auto insurance companies, individual US state transportation agencies, social media sites and a wide range of others.[23] And now there are confirmed instances of being able to hack into automobiles, such as when hackers demonstrated that they could take over a Jeep Cherokee, changing the cooling settings, the heating of the seats, the radio, the windshield wipers and disabling the accelerator.[24] US senators reacted quickly, proposing new legislation on the same day the news broke that would require the US National Highway Traffic Safety Administration (NHTSA) to set standards to ensure that all wireless access points of a vehicle are secured and built with technology to detect and stop a hack in real time. The proposed legislation also includes rules to force car companies to make customers aware of the data collected about them and their use of the car.[25] IA professionals need to stay on top of this to ensure that the automobiles they use for work have such connectivity appropriately secured.

> "Security is typically not even considered during the architecting and design of IoT devices."

SMART DEVICE MANUFACTURERS ARE NOT BUILDING IN SECURITY

Many of the hundreds of clients of information security and privacy services are start-ups, or small to mid-size technology companies, and many of them offer services and devices for the IoT. It is disappointing, and alarming in many ways, that most are not following long-standing systems engineering and programming design due diligence and testing rigor. One start-up technology company even explained they did not need change control procedures because they "use Agile Programming."[26]

In fact, security is typically not even considered during the architecting and design of IoT devices. At a discussion of the design of IoT devices at the 2015 US Consumer Electronics

Week show, a panel member stated that, "Security is not prevalent in the minds of the [IoT] architects."[27] But given that a Hewlett Packard 2014 IoT survey found that 70 percent of IoT devices were found to have significant security vulnerabilities,[28] this should not really be a surprise, should it?

The following discussion took place between a privacy professional and a medical device engineer after the engineer advised the privacy professional that the implantable device he engineered and maintains, which sustains the lives of hundreds of those using it, has absolutely no security controls built in.

Privacy professional: Are you not concerned that those using your medical device, with no access controls and no encryption and no antimalware, could be accessed inappropriately and bring harm to the patient wearing it?

Engineer: No. The data transmission and control are using short-range radio frequency identification (RFID). You would have to be right next to the patient to even access the device.

Privacy professional: But how is that near-vicinity access made?

Engineer: Using an app. It collects the data, changes controls, and a bunch of other stuff to maintain the device.

Privacy professional: How do you do maintenance on the devices then? Do you visit each patient? That seems time-consuming and nearly impossible considering all the patients who use your device.

Engineer: Oh, I can do that remotely. I go to a web site that communicates with the app to access the devices, based on the device number and/or patient name, depending upon how it is set up.

Privacy professional: So, I could access the device if I could get into the web site and find a device name or number.

Engineer: Yes, that is just what I said.

Privacy professional: So then I would not need to be right next to the patient to change the controls, would I?

A long, productive discussion followed.

FALSE ARGUMENTS AGAINST SECURITY AND PRIVACY CONTROLS

There are many other false arguments that can be heard, in person as well as in print and online, for why IoT device engineers and manufacturers cannot, should not and/or will not build in the necessary data security controls. Some of the most common false arguments include:

- **Nothing bad, related to security or privacy, can happen with the IoT device.** Wrong. Oftentimes, the engineers and manufacturers do not consider all the access paths that exist to the device. They often consider only the access point in the device itself. Once they thoughtfully consider all the ways in which access can be made, they should then understand the ways in which bad things can happen with regard to security, privacy and even safety.
- **Addressing security and privacy kills innovation.** Wrong. Actually, if privacy is purposefully addressed within new innovations, it expands and improves innovations. It does not inhibit them. The public is demanding that privacy be protected.[29] Privacy should be viewed as not just a differentiator or something to be done if legally required, but a standard requirement for any new technology or service involving personal data. It takes more innovation to create secure devices that mitigate privacy risk than it does to simply leave out such controls.[30]
- **Security is too expensive to build in.** Wrong. A medical device manufacturer once told this author how much he paid for marketing: "Somewhere in the mid-six-figures." When asked how much he spent on security, he replied, "As little as possible. If we stay below five figures we are happy." It is easy to see where his priorities lie, which is alarming considering an unsecured medical device can have dire health consequences for the patient using it.
- **Privacy cannot be built in.** Wrong. This is a widespread conundrum for IoT device engineers. And no wonder, considering privacy is a very fuzzy topic with a history of no specific actions provided for engineers to follow. This is changing. More instruction is being provided in various university[31] and professional classes, such as those provided at ISACA® conferences.[32] And more tools are being created, such as the upcoming *ISACA® Privacy Principles and Program Management Guide* (expected in early 2016).
- **Consumers do not care about privacy.** Wrong. Most people do care about privacy. A Pew research study reported that 91 percent of adults surveyed care about their privacy, but feel as though they have no control over how their personal information is collected and used by companies.[33] More consumers will be demanding that the devices they use have security and privacy controls built in.[34]

SMART DEVICES NEED TO HAVE SECURITY AND PRIVACY BUILT IN

IoT devices act as:

- Data collectors
- Data storage devices
- Data processors
- Data servers
- Access paths between devices

The risk associated with each device and all these different actions must be considered and appropriately addressed and mitigated.[35] The storage capabilities of the tiniest microchips are increasing by leaps and bounds and new storage warehouses are being built specifically for IoT devices.[36] All these data can provide insights into the individuals' lives who are using the devices. These data need to be protected and deleted when no longer necessary. And the data collected should be limited to only what is necessary to support the purpose of the device.[37] A large portion of smart devices are controlled by apps, which themselves typically have a multitude of security and privacy vulnerabilities. According to a 2015 study, 90 percent of mobile banking apps are vulnerable.[38] The banking industry is one of the most highly regulated and audited industries. If the apps it uses are this bad, think how much worse other apps are in industries with less, or no, regulation.

Additionally, the privacy harms that can result from the devices must also be considered and appropriately mitigated.[39]

Another problem is that architects who do try to build in security controls are constraining themselves to consider only existing and past types of security controls, which often do not lend themselves well to IoT devices. These new and different types of user interfaces require new solutions for the long-existing security concepts and risk that must be mitigated. For example, biometrics could be used in ways it currently is not. Location-based controls, which seem to have fallen out of favor as a viable security control in the past couple of decades, could also be used in a wide range of ways to provide security to smart devices.

Considerations for including security and privacy controls into IoT devices often stop at legal requirements. And considering there are few laws and regulations that are written in such a way that they would apply to IoT devices, this is another reason why those devices predominantly lack effective security and privacy controls.

The recent ISACA IoT survey[40] revealed that 49 percent of survey participants viewed wearables and other IoT devices as security threats to the workplace, and 25 percent were concerned with the privacy risk associated with them. However, 56 percent of those responding to the survey did not have policies and procedures covering the use of IoT devices. IA professionals need to address this.

WHAT TO DO GOING FORWARD?

In January 2014, an ISACA webinar titled "Where Do You Draw the Creepy Line?"[41] was attended by several thousand participants. It described the basic risk involved with IoT and with using big data analytics on all the data collected by the devices. Those basic risk factors and concerns are expanding.

As discussed during the webinar, actions need to be taken to address the risk associated with IoT. Here are some recommended actions:

- **Look forward.** Make sure someone in the organization is monitoring IoT developments, notices whenever a department or team within the business starts using them and when employees start bringing them into the business environment. One tool that should be of interest to IT personnel who are keeping an eye on this is Shodan, a search engine for IoT.[42]
- **Look at the emerging IoT standards.** There are many to consider, and many more in the works. Here are just a few:
  - Institute of Electrical and Electronics Engineers (IEEE): The Privacy and Security Architecture for Consumer Wireless Devices Working Group (COM/SDB/P1912 WG) initiative kicked off in July 2015.[43]

  - Open Web Application Security Project (OWASP): Internet of Things (IoT) Top 10 project, "designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies."[44]
  - NIST: The NIST Engineering Laboratory Cyber-Physical Systems (CPS) and Smart Grid Program Office is leading the Cyber-Physical Systems Public Working Group (CPS PWG) "to help define and shape key aspects of CPS to accelerate its development and implementation within multiple sectors of our economy." Through its five subgroups, the CPS PWG is preparing a CPS Framework.[45]
- **Address long-standing data security core concepts.** Make sure change controls, access controls, and other long-time information security practices are implemented not only within the IoT devices, but also in the rules for using IoT devices for business and within business environments. Build in controls from the beginning of device design and planning engineering.
- **Build in strong authentication.** Do not simply connect to specific IP addresses as a method of authentication. IP addresses can easily be spoofed. The risk of using IP addresses has already been demonstrated several times, such as for medical devices.[46] Always require default passwords to be changed before they are used for the first time.
- **Encrypt data.** Encrypt not only the wireless data transmissions, but also the data in storage. And, no, encryption does not take up that much of the IoT device resources to justify leaving it out.
- **Log access to the IoT device.** Log who accessed the device, what he/she did to the device and with the data, and when he/she did the accessing.
- **Embed antimalware within the device.** These smart devices are often more susceptible to malicious malware than other types of computing devices, as has been demonstrated by hacks into health care systems via unsecured medical devices using malware.[47]
- **Protect entry points.** Build in protection from port scans and other penetration tools.
- **Keep the devices updated.** Establish procedures to deploy firmware updates to fix discovered vulnerabilities. Yes, this can be accomplished.
- **Secure the IoT device perimeter.** This requires strongly securing the apps and clouds used in conjunction with the devices.
- **Watch third parties.** Establish oversight of third parties used to support the IoT devices and ecosystem.[48]
- **Consider privacy and safety harms.** IoT device makers must start looking at how their products could cause harm to those using them. Determine and mitigate the potential safety and privacy harm to those who will be using the devices.[49]
- **Establish IoT rules and boundaries.** For those businesses using smart devices, and where their employees are using IoT devices, establish policies and procedures that clearly describe the boundaries within which IoT devices can be used.[50] Organizations creating IoT devices need to create the rules for the necessary data security and privacy controls that must be built into the devices.

ENDNOTES

1 Brownlee, Lisa; "The $11 Trillion Internet of Things, Big Data and Pattern of Life (POL) Analytics," *Forbes*, 10 July 2015, *www.forbes.com/sites/lisabrownlee/2015/07/10/the-11-trillion-internet-of-things-big-data-and-pattern-of-life-pol-analytics/*

2 Arthur, Charles; "The History of Smartphones: Timeline," *The Guardian*, 24 January 2012, *www.theguardian.com/technology/2012/jan/24/smartphones-timeline*

3 In September 2014, the number of unique mobile users passed 3.6 billion, or 50 percent of the world's population. The number of mobile devices surpassed the world's population in December 2014. In 2015, for the first time, more than one quarter of the global population will use smart phones. By 2018, more than one-third of consumers worldwide, or 2.56 billion people, will use smart phones, according to eMarketer. That figure represents more than half of all mobile phone users. FIPP, *www.fipp.com/news/fippnews/is-the-importance-of-mobile-exaggerated*

4 Franzen, Carl; "Dick Cheney Had the Wireless Disabled on His Pacemaker to Avoid Risk of Terrorist Tampering," The Verge, 21 October 2013, *www.theverge.com/2013/10/21/4863872/dick-cheney-pacemaker-wireless-disabled-2007*

5 See: Herold, Rebecca; session at the 201410X Medical Device Conference, *https://www.youtube.com/watch?v=_aqOOPUwJhE*

[6] National Institute of Standards and Technology, NIST Smart Grid Collaboration Wiki for Smart Grid Interoperability Standards, USA, *http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGPrivacy*

[7] Smart Grid Interoperability Panel, Smart Grid Cybersecurity Committee, *www.sgip.org/SGCC*

[8] Smart Grid Interoperability Panel, *Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security*, September 2010, *www.nist.gov/smartgrid/upload/nistir-7628_total-2.pdf,* and NISTIR 7628 Revision 1, 2014, *http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf*

[9] Herold, R.; C. Hertzog; *Data Privacy for the Smart Grid*, CRC Press, 2015, *www.crcpress.com/Data-Privacy-for-the-Smart-Grid/Herold-Hertzog/9781466573376*

[10] *Corporate Wellness Magazine*, "Wearable Devices are Coming to a Doctor Near You," 3 April 2015, *www.corporatewellnessmagazine.com/technology/wearable-devices-coming-to-a-doctor-near-you/*

[11] Rosenbrock, K.; "Do Fitness Trackers Really Work for Weight Loss?" *The Active Times*, 19 March 2015, *www.theactivetimes.com/do-fitness-trackers-really-work-weight-loss*

[12] Young, E.; "Do You Want Your Company to Know How Fit You Are?" BBC News, 17 July 2015, *www.bbc.com/news/business-33261116*

[13] Your Security Resource, "How Private Is the New Amazon Echo?" *www.yoursecurityresource.com/expertqa/how-private-is-new-amazon-echo/index.html#.Va_rdPlViko*

[14] Associated Press, "Hackers Post Webcam, Security Camera, Baby Monitor Video Online," CBC News, November 2014, *www.cbc.ca/news/technology/hackers-post-webcam-security-camera-baby-monitor-video-online-1.2841770*

[15] Phillips, C.; "Privacy Fears Over Samsung's 'Orwellian' Smart TV," *Newsweek*, 9 February 2015, *www.newsweek.com/privacy-fears-over-samsungs-orwellian-smart-tv-305532*

[16] Christian, S.; "British Gas Works to Address New Security Threats and Conquer the Smart Home," Verimatrix, 30 June 2015, *www.verimatrix.com/blog/201506/british-gas-works-address-new-security-threats-and-conquer-smart-home*

[17] Howard, P.; "The Internet of Things Is Poised to Change Democracy Itself," Paxtechnica, 1 July 2015, *http://paxtechnica.org/?p=789*

[18] O'Brien, J.;"Police Warn Monitors Susceptible to Hackers After Middlesex Centre Incident," 23 July 2015, *www.lfpress.com/2015/07/23/police-warn-monitors-susceptible-to-hackers-after-middlesex-centre-incident*

[19] Federal Trade Commission,"Marketer of Internet-connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy," USA, 4 September 2013, *www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles*

[20] *Brooklyn Daily Eagle*, "Schumer Warns of Webcam, 'Smart' TV, Baby Monitor Hackers," December 2014, *www.brooklyneagle.com/articles/2014/12/1/schumer-warns-webcam-%E2%80%98smart%E2%80%99-tv-baby-monitor-hackers.*

[21] Chipsetc, "Computer Chips Used in Cars," *www.chipsetc.com/computer-chips-inside-the-car.html*

[22] *Popular Mechanics*, "How it Works: The Computer Inside Your Car," 21 February 2012, *www.popularmechanics.com/cars/how-to/a7386/how-it-works-the-computer-inside-your-car/*

[23] Massachusetts Department of Transportation, How E-ZPass Works, USA, *www.massdot.state.ma.us/highway/TrafficTravelResources/EZPassMAProgram/HowEZPassWorks.aspx*. Lanctot, R.; "Losing Facebook," 28 June 2015, *www.linkedin.com/pulse/losing-facebook-roger-c-lanctot*

[24] Greenberg, A.; "Hackers Remotely Kill a Jeep on the Highway—With Me in It," *Wired*, 21 July 2015, *www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/*

[25] Trujillo, M.; "Senators Seek Privacy, Anti-hacking Safeguards in Cars," *The Hill*, 21 July 2015, *http://thehill.com/policy/cybersecurity/248636-senators-want-privacy-hacking-safeguards-in-cars*

[26] Herold, R.; "Change Controls Are Still Necessary," *The Privacy Professor*, Dell Insight Partners, *http://privacyguidance.com/blog/change-controls-are-still-necessary/*

[27] CE Week New York 2015, "Tackling Connected Car Security and Privacy Concerns Highlights" panel discussion, *https://youtu.be/w8ShDE6RE6M*

[28] Hewlett-Packard Development Company, *Internet of Things Research Study*, USA, 2014, *www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf*

[29] Madden, M.; "Public Perceptions of Privacy and Security in the Post-Snowden Era," Pew Research Center, November 2014, *www.pewinternet.org/2014/11/12/public-privacy-perceptions/*

[30] Thierer, A.; "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation," Social Science Research Network, 18 February 2015, *http://ssrn.com/abstract=2494382*

[31] Carnegie Mellon University, "Engineering Privacy in Software," course description, Pittsburgh, Pennsylvania, USA, *www.cs.cmu.edu/~breaux/teaching-08605sp14.html*

[32] ISACA, EuroCACS/ISRM 2015, November 2015, *www.isaca.org/ecommerce/Pages/eurocacs-isrm.aspx*

[33] *Op cit*, Madden

[34] Hulme, G. V.; "Want Good IoT Security? It's Up to Each and Every One of Us," CSC Blogs, 23 July 2015, *http://blogs.csc.com/2015/07/23/want-good-iot-security-its-up-to-each-and-every-one-of-us/*

[35] Sarma, S.; "I Helped Invent the Internet of Things. Here's Why I'm Worried About How Secure It Is," *Politico*, June 2016, *www.politico.com/agenda/story/2015/06/internet-of-things-privacy-risks-security-000096?cmpid=sf*

[36] M2X, IoT Cloud-based Data Storage Service and Management Tool, AT&T, *https://m2x.att.com/*

[37] Herold, R.; "Data Collection Must be Limited for Internet of Things Privacy," *The Privacy Professor*, 30 January 2015, *http://privacyguidance.com/blog/data-collection-must-be-limited-for-internet-of-things-privacy/*

[38] Chettri, S.; "'90% of Mobile Banking Apps Are Vulnerable' Study," *Hindustan Times*, 19 April 2015, *www.hindustantimes.com/business-news/90-of-mobile-banking-apps-are-vulnerable/article1-1338449.aspx*

[39] Herold, R.; "Organizations Must Consider Privacy Harms," *The Privacy Professor*, 2015, *http://privacyguidance.com/blog/organizations-must-consider-privacy-harms/*

[40] ISACA, *Internet of Things: Risk and Value Considerations*, USA, 2015, *www.isaca.org/knowledge-center/research/researchdeliverables/pages/internet-of-things-risk-and-value-considerations.aspx*

[41] ISACA, "Where Do You Draw the Creepy Line? Privacy, Big Data Analytics and the Internet of Things," webinar, 9 January 2014, *www.isaca.org/Education/Online-Learning/Pages/Webinar-Where-do-you-draw-the-creepy-line-Privacy-big-data-analytics-and-the-Internet-of-things.aspx*

[42] Shodan, *www.shodan.io/*

[43] IEEE Standards Association, Privacy and Security Architecture for Consumer Wireless Devices Working Group (COM/SDB/P1912 WG), *http://grouper.ieee.org/groups/1912/meeting_information.html*

[44] Open Web Application Security Project, OWASP Internet of Things Top 10, *www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project*

[45] National Institute of Standards and Technology, Cyber-Physical Systems, USA, *www.nist.gov/cps/*

[46] Bonderud, D.; "Do No Harm? Medical Device Vulnerabilities Put Patients at Risk," The MSP Hub, 28 May 2015, *http://themsphub.com/do-no-harm-medical-device-vulnerabilities-put-patients-at-risk/*

[47] Jackson-Higgins, K.; "Hospital Medical Devices Used as Weapons in Cyberattacks," *Information Week Dark Reading*, 8 June 2015, *www.darkreading.com/vulnerabilities---threats/hospital-medical-devices-used-as-weapons-in-cyberattacks/d/d-id/1320751*

[48] Herold, R.; "Will Your Contractors Take Down Your Business?" *The Privacy Professor*, May 2015, *http://privacyguidance.com/blog/will-your-contractors-take-down-your-business/*

[49] Herold, R.; "Organizations Must Consider Privacy Harms," *The Privacy Professor*, 12 May 2015, *http://privacyguidance.com/blog/organizations-must-consider-privacy-harms/*

[50] Herold, R.; "How Businesses Can Reduce Wearables Security & Privacy Risks," *The Privacy Professor*, 12 March 2015, *http://privacyguidance.com/blog/how-businesses-can-reduce-wearables-security-privacy-risks/*

Back to the Future in Device Security

Leveraging FIPPs to Proactively Manage IoT Privacy and Security Risk

Doron Rotman, CIPP, is a managing director at KPMG LLP, the US national privacy service leader for KPMG and a member of KPMG international privacy leadership team. He has more than 30 years of experience, focused on providing privacy, security and information governance services.

Chris Kypreos, CIPP, is a senior associate at KPMG LLP, and a member of the International Association of Privacy Professionals (IAPP). Kypreos has helped develop and author several publications and has presented at industry events.

Sarah Pipes, CIPP, is a senior associate at KPMG LLP, and is currently on rotation at KPMG Belgium. Pipes is a member of the IAPP. She has helped develop and author several publications and spoken at several industry events.

Do you have something to say about this article?

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

Go directly to the article:

The Internet of Things (IoT) represents an unknown set of forces. However, one known is that IoT-connected devices will generate exponential levels of new data that will lead to powerful insights, drive new business and facilitate the development of innovative technologies. IoT also raises multiple data privacy and security concerns when new data sources combine with legacy sources to reveal new insights about individuals through predictive analytics that may be inconsistent with the original purposes for collection and use. Additionally, connecting new technologies with legacy systems can prove risky, as many new IoT device manufacturers lack software development and security experience.[1] These risk factors can increase a company's threat exposure and make the organization a ripe target for a breach.

Despite IoT's unknowns and the corresponding privacy and security risk, there are legacy tools available that privacy and security leaders can use to address these risk factors proactively. This article shows how frameworks based on the Fair Information Practice Principles (FIPPs)[2] are adaptable and practical tools to help embed privacy and security into new IoT devices.

EVALUATING PRIVACY AND SECURITY: A FRAMEWORK

Although IoT represents a state of change and advancement, a common set of principles can serve as the foundation for companies seeking to understand and manage privacy and security early in the design and development phases of new connected devices. One set of principles is FIPPs, which the US Department of Health, Education, and Welfare referenced in a 1973 report. The Organisation for Economic Co-operation and Development (OECD) revised the principles in 1980. Today, FIPPs serves as the basis for multiple codified privacy laws, regulations and standards throughout the world.[3]

Auch auf Deutsch verfügbar
www.isaca.org/currentissue

FIPPs-based standards continue to be useful for privacy and security professionals to evaluate and design their IoT programs and technologies because they are actionable and comprised of risk-based controls, and they are adaptable to the unique characteristics of a particular industry and an organization's business requirements.

Two FIPPs-based frameworks available are the Generally Accepted Privacy Principles (GAPP)[4] and the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.[5]

FRAMEWORK 1: GAPP

The GAPP framework was developed by a taskforce formed by the American Institute of Certified Public Accountants (AICPA) and CPA Canada. Its primary purpose is to assist management in creating an effective privacy program that addresses privacy obligations, risk and business opportunities. Therefore, the 10 principles and 73 control criteria within GAPP are designed to assist with the implementation and demonstration of better privacy practices. The framework additionally includes a maturity model that organizations can use to assess their overall maturity.

The 10 GAPP are:

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 describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
4. **Collection**—The entity collects personal information only for the purposes identified in the notice.
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 has 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 regulation 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 purposes 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.

These principles address not only strong privacy practices, but their implementation by the organization.

FRAMEWORK 2: NIST SP 800-53 APPENDIX J

NIST commissioned a Joint Task Force Transformation Initiative to publish SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations," which provides a catalog of security controls designed to support the security control selection for US federal information systems. Within this larger standard, the Appendix J Privacy Control Catalog was developed to provide a road map for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of personally identifiable information (PII), whether in paper or electronic form.[6] These controls are designed for use by chief privacy officers (CPOs) to support their organizations in complying with privacy components of applicable federal laws and other requirements. This is achieved in part through simplifying requirements into a single catalog through mapping overlapping controls found in various privacy and security requirements.

To achieve this, appendix J includes a structured set of controls across eight control families. These privacy control families are:

1. **Authority and Purpose**—This family ensures that organizations:
   - Identify the legal bases that authorize a particular PII collection or activity that impacts privacy
   - Specify in their notices the purpose(s) for which PII is collected
2. **Accountability, Audit and Risk Management**—This family enhances public confidence through effective controls for governance, monitoring, risk management and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.
3. **Data Quality and Integrity**—This family enhances public confidence that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.
4. **Data Minimization and Retention**—This family helps organizations implement the data minimization and retention requirements to collect, use and retain only PII that is relevant and necessary for the purpose for which it was originally

collected. Organizations retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a US National Archives and Records Administration (NARA)-approved record retention schedule.

5. **Individual Participation and Redress**—This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.
6. **Security**—This family supplements the security controls in appendix F to ensure that technical, physical and administrative safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.
7. **Transparency**—This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities.
8. **Use Limitation**—This family ensures that organizations only use PII either as specified in their public notices, in a manner compatible with those specified purposes or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.

GAPP and NIST SP 800-53 appendix J can trace their origins to FIPPs, and their flexibility and comprehensiveness have made them the predominant standards to evaluate privacy and security. Both standards are customizable, and organizations can leverage them to implement new organizational processes or as guidance to embed privacy and security controls into new IoT products and systems. Both are designed for management use and facilitate the implementation of privacy requirements rather than simply stating the end goal.

However, each framework also has unique strengths. NIST SP 800-53 appendix J is designed to facilitate compliance with numerous overlapping US federal laws, directives and orders, and, therefore, it is a legally driven framework. While appendix J is a useful tool for organizations across many industries, the primary audiences are those required to satisfy US federal requirements. Therefore, it is most useful for implementing IoT technologies in industries that must comply specifically with US law. Conversely, GAPP does not support compliance with any particular law, but rather international good practices. It is most useful for IoT technologies that will be implemented in a similar way internationally, with modest modifications to meet local requirements.

The two case studies that follow illustrate the effectiveness of the principles contained within each framework in designing cutting-edge IoT products.

USE CASE 1: SMART CAR—GAPP

The automotive industry views connected cars as the way of the future. The connected vehicle will incorporate technologies that enhance human safety, reduce traffic congestion, improve efficiency and vehicle performance, and provide valuable information services.[7] Moreover, analysts predict that the global market for connected vehicles will reach 220 million cars on the road by 2020.[8]

Although nearly all major automobile manufacturers and communication companies have entered the connected car market, evidence demonstrates that many companies continue to develop products with key privacy and security vulnerabilities. US Senator Ed Markey commissioned a report based on the responses of 16 major manufacturers that revealed a clear lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle or against those who may wish to collect and use personal driver information.[9]

Auto companies have demonstrated a commitment to privacy, and the Alliance of Automobile Manufacturers Inc. and Association of Global Automakers developed a self-regulatory framework, Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technology Services, to address these concerns. Each participating member will commit to compliance with the principles for new vehicles manufactured no later than model year 2017.[10] Although the principles provide guidance to members on how to satisfy the requirements, privacy leaders can leverage the GAPP framework's controls to support their compliance efforts and address future privacy and security risk in the planning and design phases.

Case Study Background

An auto manufacturer (the company) plans to develop software that they will install on their vehicles' built-in navigation system. The application will integrate via Bluetooth to an individual's mobile device to sync the user's contact addresses with the car's navigation system. The company can leverage the GAPP framework in the process of designing, developing and installing the application.

GAPP Management Principle

The company should assign a privacy product manager who will be an accountable party and will perform a privacy impact assessment at the project's outset to identify the associated risk based on the personal information collected, stored and transferred. The privacy manager will interact with various departments, including software development, legal and product supports, to understand business and regulatory requirements and monitor new obligations posed by changes in the business and legal environments.

GAPP Notice Principle

The company understands that notice is a foundational element in privacy laws and standards. The team is also aware that providing notice in the context of connected devices can be difficult when user interfaces are often nonexistent or limited. However, notice does become essential when data use is inconsistent with user expectations and in the cases of new purposes. The company can provide notice when a customer initially registers to use the application or identify alternate mechanisms to provide notice, including a web site that includes links to demonstrations and tutorials of the software's functionality.

GAPP Choice and Consent Principle

The company's software is functional because it integrates certain personal data elements with geo-location data. Similar to notice, the privacy manager understands the challenges in providing knowledgeable opt-in consent over limited interfaces. The company should consider providing various tiers of service to customers based on the level of consent provided. For example, drivers may elect to share the vehicle's current location with other members of their network to provide two-way visibility. Alternatively, the customer may prefer to consent only to the use of static address data entered into the device. By understanding the various use cases for the software, the company can offer granular choices that limit personal information usage without affecting functionality.

GAPP Collection Principle

The company understands that data collection becomes more critical in the IoT context, where most networked devices consistently collect and process data. Combining large data sets can offer powerful knowledge and analysis, but data usage may be inconsistent with the primary purposes of collection. The company should limit data collection to lawful methods and be transparent with customers as to how it collects and integrates personal information from third parties. Additionally, the company can reduce its potential risk for breach and associated liability by limiting data collection to only those elements that are essential for functionality. By incorporating data minimization controls into the application, the risk associated with notice, consent and retention becomes less magnified.

GAPP Use, Retention and Disposal Principle

The integration of the company's software with other devices and programs may enhance the customer experience, but the company should limit the use of data to primary business purposes or cases where the customer provided explicit consent. Additionally, the privacy manager should consult other stakeholders in the organization on business and legal retention requirements to enable those departments to create record-retention schedules. Then, the privacy manager should implement procedures to ensure the destruction of data upon expiration of record-retention dates. For example, the company could consider deleting all data stored by the software at the conclusion of each driving session and then reinitiate the connection when the driver starts the vehicle the next time. This will help reduce the risk of a data breach and can improve program functionality. The company should perform regular audits to test compliance with policies and procedures.

GAPP Access Principle

The company should recognize that allowing customers to access and update their data will result in a positive-sum experience. This improves accuracy and relevance of the data presented through the software to the customer. If the company

elects to store customer data, it may offer a secure web portal that customers can access to easily update and delete their information. By leveraging alternate technology, the company can work around limitations presented by IoT devices.

GAPP Disclosure to Third Parties Principle
The company may determine that the functionality of the software increases if there is integration with other third-party providers. By using GAPP, the company will better understand how to protect its customer information. The company will recognize that any new purposes for the data should require customer consent. Additionally, the privacy manager can work with legal counsel to ensure that appropriate provisions are included in third-party contracts based on the services provided.

GAPP Security for Privacy Principle
The company must understand the importance of application security in the design phase to protect customer data throughout the collection, storage and transfer phases of the life cycle. The privacy manager should work with the information security team to embed controls into the supporting IT infrastructure. The company should consider data encryption, both at rest and in transit, when information transmits from the device to the vehicle and from the vehicle to other third-party providers involved in the process. Additionally, the company can deploy industry-level access management solutions that limit access to personal information to only authorized and authenticated individuals.

GAPP Quality Principle
The company provides a service to its customers that relies on offering real-time data that are accurate and relevant. It is critical for the data collected to be normalized and consistent with the original entry status. Although the customer initially enters contact information into the mobile device, the company can ensure data quality by leveraging uniform protocols and controls.

GAPP Monitoring and Enforcement Principle
The company recognizes that good customer service requires offering mechanisms for the customer to engage the business. Although not unique to IoT, the company can establish a process to receive and respond to privacy and security inquiries and complaints. Additionally, the privacy manager should be responsible for ongoing monitoring of the environment for compliance and new business risk.

How to Apply GAPP
Most of these principles are applicable for IoT device manufacturers or software developers embedding privacy and security into the development process. However, GAPP facilitates flexibility: if specific principles, or even criteria within a principle, are not applicable to a particular development scenario, these can be documented and scoped out of the privacy assessment.

> "GAPP facilitates flexibility."

There is also flexibility in measuring of success in meeting the requirements laid forth by the GAPP principles. The AICPA and CPA Canada suggest the use of a Privacy Maturity Model based on the Capability Maturity Model (CMM). This model includes the following five levels: *ad hoc*, defined, repeatable, managed and optimized. The appropriate or desired state is determined by the organization, with acknowledgement that the highest level of maturity (optimized) may not be suitable for all or even many situations.

GAPP is a tool developed to help management create a practical and effective privacy program, and the 10 principles build to create a comprehensive management framework, addressing risk while enabling companies to retain their competitive advantage.

USE CASE 2: CONNECTED MEDICAL DEVICES—NIST SP 800-53

The connected medical device market is increasing rapidly, and analyst research predicts that the global remote patient monitoring devices market will grow to nearly US $1 billion by 2020.[11] As the number of wearable devices and monitoring technologies increases, concerns around the collection and storage of sensitive patient data will also continue to rise. As a result, the health care industry continues to be a vulnerable and attractive target for cyberattacks. In fact, recent research predicts that the health care field could face as much as US $5.6 billion annually in costs associated with data breaches.[12] US health care providers are subject to specific privacy and security requirements in accordance with the US Health Insurance Portability and Accountability Act

(HIPAA); therefore, it becomes critical that organizations safeguard their data and information systems to control access to systems, reduce privacy and security risk, and ensure data quality.[13] An organization can proactively leverage NIST SP 800-53 appendix J to help meet its compliance requirements under HIPAA and when evaluating new information management systems and other connected devices to ensure inclusion of appropriate privacy and security controls.

The following controls reflect the need to protect privacy throughout the information life cycle, from data collection to processing and maintenance through data sharing and destruction. The risk associated with each control area, therefore, is determined by the nature and processing of the personal data in question.

Case Study Background

In an effort to lower health care delivery costs and improve delivery quality, a veterans' affairs health care system (the organization) seeks to upgrade its health care information management (HIM) system to manage the exponential increase in data received from IoT medical devices. For example, at-home health monitoring devices provide transmissions of vital signs such as blood pressure and heart rate and can also measure symptoms related to diabetes, hypertension and asthma, among other diseases. Wearable devices can trigger an emergency response when necessary, while fitness bands provide information about exercise (e.g., steps taken, calories burned) throughout the day. The health care system's technology staff understands that there are various privacy and security requirements and prefers to scope mitigating controls during the planning and development phases.

Authority to Collect

The organization relies on collecting sensitive data elements to deliver quality and timely care to its patients. While reviewing the requirements relating to gathering information for the new HIM system, the technology staff should perform a privacy risk assessment to identify the risk associated with the collection of certain data and document the categories of elements in the privacy notice delivered to patients.

Accountability, Audit and Risk Management

The organization designates a privacy official to perform a privacy impact and risk assessment to identify the risk to personal information when deploying a new HIM system in the environment. This official and the technology staff understand that they should design systems with automated privacy controls that mitigate risk and reduce the likelihood of a breach. This step is critical, because the cost of redesigning privacy and security into the system after the fact is overly burdensome and expensive. By designing automated controls into the system, the organization understands that it can more effectively satisfy its monitoring and reporting requirements while increasing data security.

Data Quality and Integrity

The organization understands that maintaining accurate data in the health care context can be a matter of life and death. Doctors, nurses and medical professionals working with outdated data risk prescribing the wrong medications, which can potentially kill a patient. The privacy official should evaluate controls designed to ensure accuracy and validity of data upon entry into the HIM. Additionally, ensuring data quality becomes more critical as the system integrates with various connected devices storing and transmitting data in different formats.

> "Ensuring data quality becomes more critical as the system integrates with various connected devices."

Data Minimization and Retention

Although health care organizations have business justifications to collect most types of sensitive data, the organization understands it can reduce the risk of a breach by limiting collection of data to only that which is necessary and destroying sensitive data records upon expiration of the retention requirements. Additionally, the privacy official can coordinate with various departments to identify specific business requirements for extended data retention. Although the organization may retain certain data for testing purposes, the privacy official can explore de-identification and aggregation techniques to reduce privacy and security risk.

The organization's technology staff can help design controls to flag sensitive data elements and mask patient records to better support the data minimization and records disposal processes.

Individual Participation and Redress

Although health care providers can share protected health information (PHI) with limited restrictions for treatment, payment and operations reasons, the organization understands that patient consent and access are fundamental concepts in the decision-making process.[14] The organization builds trust with its patients when it provides them control over their information and allows them to update records to help improve data quality and accuracy. The privacy official should ensure that customer portals and other connected devices interfacing with the HIM provide access and certain control over the data records.

Security

To effectively secure personal information throughout the data life cycle, it is imperative that the organization document the various data flows. While designing the new HIM system, the privacy official should identify the different upstream and downstream systems and applications, the data elements contained in those systems, and the different data elements transferred from one system to another. Then, the privacy official can work with the organization's information security team to ensure that the different systems in the inventory receive the appropriate level of security based on the sensitivity of the data.

Transparency

The organization collects data from the connected devices that integrate with the HIM system. Therefore, the organization should provide notice to its patients on the types of information collected, processed, stored and transferred through these connected devices. If the wearable technology has limited interfaces, the privacy official should consider alternate methods to provide notice with these devices. For example, the organization may consider publishing its privacy notice on a web portal where patients access and input personal information.

Use Limitation

The organization understands the importance of patient trust in the doctor-patient relationship. The privacy official should incorporate controls and checks that limit the opportunity to access and use information for new and secondary purposes not accompanied by customer consent. However, HIPAA permits the sharing of certain records with other covered entities and business associates, incorporating audit log capabilities within the HIM system to help track data transactions to assist with the ongoing monitoring of data sharing and user access.

How to Apply Appendix J

This standard is designed to support effective compliance within the scope of privacy requirements by supporting compliance throughout the information governance cycle. While NIST SP 800-53 appendix J does not incorporate all US laws, especially those guiding particular data types such as health information, these additional laws can be incorporated easily at the appropriate stages of the existing framework. Appropriate compliance with controls also depends upon any additional requirements that may apply, and the organization may choose to implement optional "control enhancements" where there is a demonstrated need.

> "To address these issues and challenges, companies must incorporate privacy and security from the outset when looking to adopt, design and deploy new connected technologies."

NIST SP 800-53 appendix J is applicable to various use cases to assist in the build out of the organization's privacy program. The privacy official can leverage the control framework when establishing an overarching program governance structure and when seeking to deploy new IoT systems and applications in the environment. The organization can customize the controls based on operational needs, but it provides a series of guidelines to embed privacy into the environment.

CONCLUSION

IoT represents great and unpredictable change in the way data are collected, processed, stored and analyzed. New technologies will significantly improve the way companies operate their business and interact with customers and other organizations. In this sense, IoT symbolizes great promise, but it also poses risk to personal privacy and security, including

collecting and processing data for new purposes beyond their original intent and generating amplified risk associated with insecure devices and target-rich data sources. To address these issues and challenges, companies must incorporate privacy and security from the outset when looking to adopt, design and deploy new connected technologies.

FIPPs represent the foundational elements of many comprehensive risk- and control-based privacy frameworks. Organizations can leverage FIPPs-based frameworks, including GAPP and NIST SP 800-53 appendix J, to evaluate the privacy and security issues posed by new IoT devices, help their organizations design and integrate secure technologies, and reduce their overall risk levels. Although IoT is changing the way data are collected, processed and used, FIPPs contain relevant guidelines for companies to manage privacy and security proactively in the design of new IoT devices.

ENDNOTES

[1] *The Economist*, "Their Own Devices," 18 July 2015, *www.economist.com/news/science-and-technology/21657766-nascent-internet-things-security-last-thing-peoples*

[2] Department of Health, Education and Welfare, *Records Computers and the Rights of Citizens*, USA, July 1973

[3] Gellman, R., "Fair Information Practices: A Basic History," 31 December 2008, *http://bobgellman.com/rg-docs/rg-FIPShistory.pdf*

[4] American Institute of Certified Public Accountants and CPA Canada, "Generally Accepted Privacy Principles," March 2011, *www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx*

[5] National Institute of Standards and Technology, Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, USA, 30 April 2013, Appendix J

[6] *Ibid.*, p. J-1

[7] Auto Alliance, "Auto Issues—Automakers Believe that Strong Consumer Data Privacy Protections are Essential to Maintaining the Trust of Our Customers," 13 November 2014, *www.autoalliance.org/index.cfm?objectid=46DD7290-68FD-11E4-866D000C296BA163*

[8] Greenough, J.; "The 'Connected Car' Is Creating a Massive New Business Opportunity for Auto, Tech, and Telecom Companies," *Business Insider*, 19 February 2015, *www.businessinsider.com/connected-car-statistics-manufacturers-2015-2*. Note that the definition of "connected cars" used in this study is: "built with the necessary hardware to connect to the Internet."

[9] Markey, E., "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk," February 2015, *www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf*

[10] *Op cit*, Auto Alliance

[11] Transparency Market Research, "Remote Patient Monitoring Devices Market—Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2014–2020," June 2015, *www.pharmiweb.com/pressreleases/pressrel.asp?ROW_ID=117619#.VahJ0vlVgli#ixzz3g6TRMnS2*

[12] Ponemon Institute, "Fourth Annual Benchmark Study on Patient Privacy & Data Security," 12 March 2014, *www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security*

[13] Congress, Health Insurance Portability and Accountability Act of 1996, (Pub. L. 104–191), USA, 21 August 1996

[14] Department of Health and Human Services, "Uses and Disclosures for Treatment, Payment, and Health Care Operations," 45 CFR 164.506, USA, 3 April 2003, *www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/sharingfortpo.pdf*

Internet of Things—The Fate We Make for Ourselves

Jim Seaman, CISM, CRISC, has enjoyed an extremely interesting and rewarding career within the security industry spanning almost 26 years. His career was forged in the application and enforcement of robust security and compliance legislation in the Royal Air Force Police over 22 years in the areas of physical security, counterterrorism and security intelligence. Since 2002, he has specialised in the field of information security management and investigations and cybersecurity. Over the last four years he has employed his skill sets, knowledge and experiences in the corporate sector across various industry sectors including financial, retail, oil and gas, UK government, travel, insurance, e-commerce and telecommunications.

The fantasy once associated with science fiction films is becoming increasingly similar to modern life.

The first *Terminator* movie introduced some cybersecurity concepts. In addition to introducing the topics of social engineering, vulnerability management and computer malware, the latest film in the saga has introduced the topic of the Internet of Things (IoT). These movies reflect the significant improvements in technologies used by businesses. As a result, there are some lessons that can be learned from looking at the *Terminator* movies, one of which is to have a proactive, rather than reactive, approach to security.

Back in the factual world, an exciting example of some of the latest development work can be seen in the research being carried out at Newcastle University (United Kingdom),[1] including:

- Ambulances interconnected to the traffic lights enabling more efficient and faster journeys[2]
- Touch- and temperature-sensitive bionic limbs[3]

Most IT security or information security professionals face the constant battle of explaining to their executives why it is important to spend sufficient money, time and resources on such things as securing systems and networks, vulnerability management, penetration testing, antivirus software, social engineering and security incident response. Security professionals also must try to maintain an understanding of and manage the new and emerging technologies being introduced to support an organisation's efficiencies.

What type of dynamic, real-world technology advancements are happening? Presently, scientists are reporting the advancement and development of the following exciting technologies:[4]

- **Emergent artificial intelligence (AI)**—AI is the development of machines that can learn, adapt and respond to their environments. These machines are also known as 'Intelligent Machines'.
- **Sense-and-avoid drones**—Remote-piloted drones that can fly themselves, without any remote assistance from a pilot sitting in a bunker somewhere piloting the drone via a joystick and monitor

All of a sudden, the far-fetched components of the *Terminator* movies do not appear to be so far-fetched after all. Add IoT into the equation, and the potential dangers become a great deal more serious.

Kevin Ashton, cofounder of the Auto-ID Center at the Massachusetts Institute of Technology (MIT) (Cambridge, Massachusetts, USA), is associated with coining the phrase 'Internet of Things (IoT)' while delivering a speech at Procter & Gamble.[5] 'If we had computers that knew everything there was to know about things—using data gathered without any help from us—we would be able to track and count everything and greatly reduce waste, loss and cost', he said. 'We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best'.[6]

The advancement of technologies means that the devices capable of interconnecting to share data have reduced in size and increased in capacity, ranging from the 3 gigabyte (GB) random access memory (RAM), 128 megabyte (MB) smart phone to a 768 GB RAM, 21 terabyte (TB) computer, or any physical item capable of being fitted with a microchip (even people, as is reported as being carried out by a Swedish company).[7]

Such devices are only going to improve their ability to interconnect and share data without the need for human interaction or control. There is also an increasing number of systems being insecurely developed. The volume of interconnected devices is predicted to be between 50 and 75 billion[8] by 2020 and 70 percent of the world is expected to be using smart phones.[9] Both businesses and individuals rely on such data-sharing devices. But lack of control and appreciation for ensuring that such devices are adequately protected, through technical controls, user education and policies, can result in significant IoT insecurity.

Although it is unlikely that there will be a global machine uprising, there are some lessons to be learned from science fiction long before it ever gets close to being a fact, especially given the strong benefits that are being speculated from incorporating AI technology into IoT devices. Acting now can reduce the impact from IoT-originated data breaches.

It has never been more important for organisations across the globe to work together to ensure that future advancements in technology are carried out safely and securely. The potential seriousness of the risk associated with IoT breaches is highlighted in US automaker Chrysler's recent recall of more than 1.4 million vehicles[10] after significant vulnerabilities were identified within the Uconnect system, an Internet-connected computer that controls such things as the onboard navigation, telephone and Wi-Fi hot spot systems. During a controlled experiment, attackers were able to hack into a Jeep Cherokee travelling at 70 mph. The attackers took control of the entertainment, air conditioning and acceleration systems, whilst highlighting that they even had the capability of tracking a vehicle via the global positioning system (GPS) and disabling the brakes.

> "It has never been more important for organisations across the globe to work together to ensure that future advancements in technology are carried out safely and securely."

Given such alarming developments, IoT data security/safety must be put at the forefront in business environments. Some of the recommended measures should include:

- **Businesses recognising the importance for securing data devices, baselining themselves with suitable industry standards**—These standards may include COBIT® 5, ISO/IEC 27001:2013, the US National Institute of Standards and Technology's (NIST) Cybersecurity Framework or NIST SP 800-53, to name a few. Businesses should also connect with reputable security services providers (e.g., consultancy, penetration testing, web application testing).

  The adoption of a suitable security standard provides a consistent benchmark that ensures that all systems, people and processes are the same (i.e., standard), which promotes improved safety and security. This concept is extremely important in support of the development of the IoT world, in which multiple interconnecting systems share significant amounts of data, as this process ensures that these connections are carried out safely and securely.

  It is useful to reference the series of articles written by the Council on Cyber Security,[11] providing further detailed advice on securing the IoT through the application of the Critical Security Controls for Cyber Defense[12]—in essence a robust foundation upon which to forge the basis of a compliance program.
- **Vendors developing secure systems**—Because of the urgency from vendors to develop and sell these new and emerging technologies, there has been little or no effort applied to ensuring that the systems were built securely. As the technology has advanced, the potential danger associated with these advanced data processing technologies has significantly increased. For example, take the latest smart phones. These phones have the capability of acting in the capacity of a temporary mobile portable desktop, accessing sensitive emails or downloading copies of sensitive documents. Yet how many of these devices have the capability to install a personal firewall, antimalware programs or operating system updates?

  All of these vulnerabilities are at the forefront of a hacker's arsenal for attack. Given that it is highly likely that these devices will be included in 2020's predicted 50-75 billion connected devices, it is extremely important that data and system security be placed at the forefront of any future technological advances.

  In addition, it is important that vendors realise the importance of ensuring that the psychological perspectives associated with the older generations' use of technologies[13] are factored into the design of such systems to provide ease of use and effective and integrated security measures.
- **End users receiving security awareness training about the safe and secure use of the devices**—The significant threats to data resources come from the end-user perspective, in which users carry out actions that undermine or bypass the security measures employed to protect both the device and the data within it. Ensuring that all end users are fully aware of the correct usage of devices becomes increasingly important when such devices are interconnecting, as in the world of IoT.

It is important to remember that as technologies advance to meet IoT capabilities, human beings may not be able to respond as quickly to the new technologies, and more seasoned members of staff may need additional training in the correct and effective use of these devices.

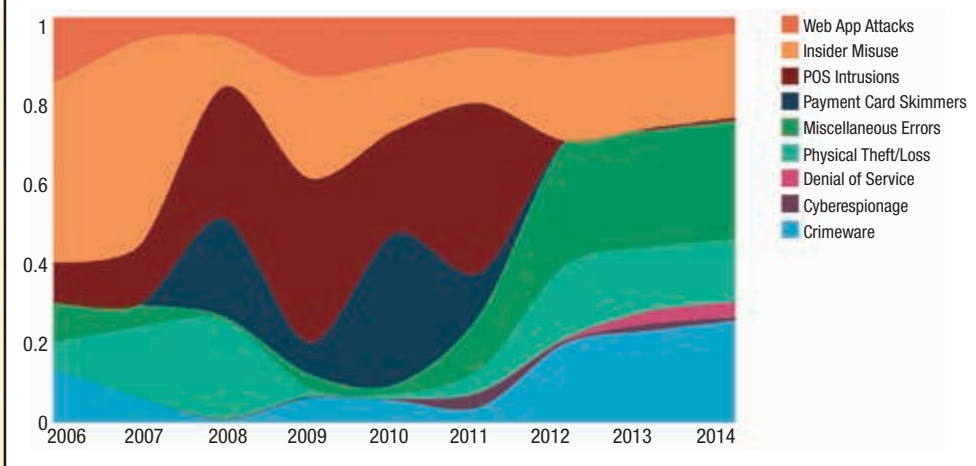
- **Security professionals maintaining their professional knowledge and awareness of emerging technologies and threats**—This can include membership in professional bodies, formalised professional development programmes or other similar efforts. The appointment of suitably trained and experienced professionals within an organisation is critical to helping reduce the risk associated with the introduction of new technologies. They act as the linchpin between decision makers and end users, ensuring effective mentoring, risk identification and communication. To make this an effective service, it is essential that these specialist appointments maintain their professional knowledge so they can efficiently respond to the challenges associated with the dynamic world of new technologies.
- **Global governments recognising the need to ensure data and device security by introducing appropriate legislation and awareness campaigns**—Unfortunately, today's world appears to be one of reaction and, as a result, the majority of organisations only react to technology-related issues in response to data breaches. There are limited legal requirements for businesses to ensure that technologies, usage and data are secure. With the introduction of more IoT technologies, it has never been more important for global governments to recognise the need to enforce the sensible use of such technologies, through the introduction of appropriate legislation. Without such legislation, there is nothing to incentivise businesses to operate their technologies responsibly.

Much of the same happened with the advancement of the motor industry. In 1769, the first steam-powered vehicle was invented. However, in the United Kingdom, the requirement to have a license to drive was not introduced until 1903. By the early 1930s, there were more than 2.3 million motor vehicles on UK roads, and there were about 7,000 motor vehicle-related deaths each year. This caused the UK government to react with the introduction of the Road Traffic Act and the Highway Code.[14] Lessons should be learned from the technological advancements in the motor industry so that similar mistakes do not occur with the technological advancements of the IoT.

All of the aforementioned measures will help to reduce the potential for IoT-associated data losses and minimise the potential for exploitation by an attacker. The following studies and reports show the existing vulnerabilities and sources of attack against existing technologies. They also demonstrate the importance and need for secure dynamic technologies and investment in the development of information systems (IS) security professionals and systems testing professionals, without which the potential benefits provided by the emerging IoT technologies will be undermined by reactive responses, resulting in some serious areas for concern in the future.

Figure 1 shows that the most significant threats are presented against external-facing web applications and from the insider misuse perspectives. Consequently, this demonstrates the need for ensuring systems are continually tested against exploitable vulnerabilities (before an unknown hostile exploits these vulnerabilities) and robust policies and procedures are in place to help reduce the threats presented from the insider (whether from a deliberate or accidental action).

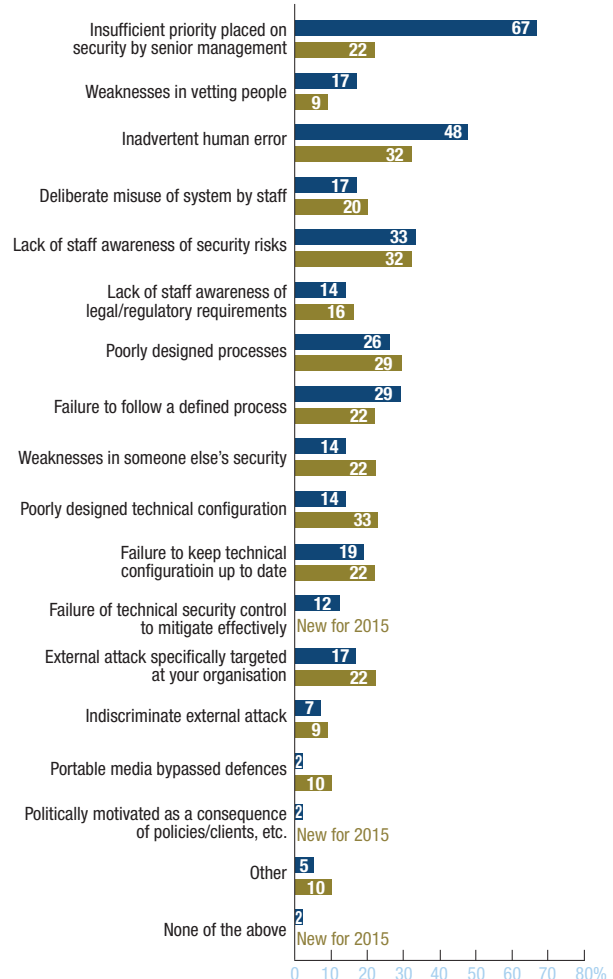
Figure 1—Frequency of Incident Classification Patterns Over Time Across Security



Source: *Verizon, 2015 Data Breach Investigations Report.* Reprinted with permission.

Figure 2 provides an overview of the contributing factors that were seen to be behind the causes of a security incident. This clearly demonstrates that good security principles start with senior management endorsing and supporting good security practices.

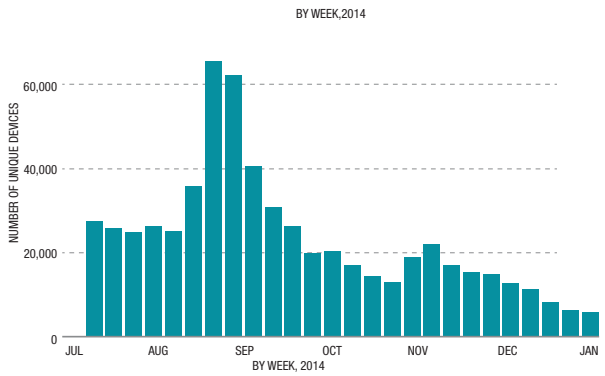
Figure 2—Contributing Factors



Source: Pricewaterhouse Coopers, *Global State of Information Security Survey: 2015 Results By Industry*. Reprinted with permission.

The development of the IoT world will increasingly involve the use of mobile devices and, as a consequence, developers, vendors and end users need to be fully aware of the high risk of malware threats that could cause a breach, especially given the theme of IoT where millions of devices will be interconnecting and sharing data. **Figure 3** shows that even in the relatively immature mobile environment, a significant number of devices are getting infected—recorded as peaking at more than 60,000 devices during September and October 2014.

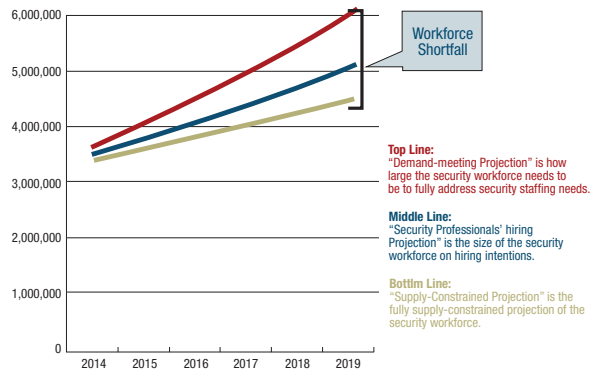
Figure 3—Number of Detected Mobile Malware Infections



Source: *Verizon, 2015 Data Breach Investigations Report*. Reprinted with permission.

Figure 4 is the most disturbing of all the statistics discovered, given the rapidly evolving technology industries and the business reliance on such technologies. This technological evolution does not appear to be matched with the appointment of suitably trained and experienced information security professionals to proactively engage with businesses to mitigate the threats highlighted in **figures 2** and **3**.

Figure 4—Projected Information Security Workers Globally



Source: Frost & Sullivan, *The 2015 (ISC)² Global Information Security Workforce Study*. Reprinted with permission.

CONCLUSION

If these trends continue in the same vein, there is substantial risk of technology advancing at a rate that creates billions of interconnected data-sharing devices (including intelligent machines/AI) with minimal security considerations being applied.

As a result, much like the *Terminator* movies, the development of the security industry can be likened to that of John Connor's resistance. The future of a safe and secure technological world will rely on an under-resourced and outnumbered band of security professionals providing a reactive service, responding to increasing numbers of breaches.

If the world does not recognise these issues and act quickly to address them, we run the risk of fact becoming stranger than fiction. To quote the *Terminator*, 'The future is not set. There is no fate but what we make for ourselves'.

ENDNOTES

[1] School of Electronic and Electrical Engineering, Communications, Sensors, Signal & Information Processing Research Group (ComS2IP), Newcastle University, United Kingdom, *www.ncl.ac.uk/eee/research/groups/coms2ip/*

[2] Knapton, S.; 'Gadget Which Turns All Traffic Lights Green Trialled in UK', *The Telegraph*, 3 April 2015, *www.telegraph.co.uk/news/science/11512274/Gadget-which-turns-all-traffic-lights-green-trialled-in-UK.html*

[3] School of Electronic and Electrical Engineering, 'Bionic hand that is 'sensitive' to touch and temperature', Press Release, 24 February 2015, Newcastle University, United Kingdom, *www.ncl.ac.uk/eee/about/news/item/bionic-hand-that-is-sensitive-to-touch-and-temperature-copy*

[4] Meyerson, Bernard; 'Top 10 Emerging Technologies of 2015', World Economic Forum, 4 March 2015, *https://agenda.weforum.org/2015/03/top-10-emerging-technologies-of-2015-2/*

[5] Postcapes, 'A Brief History of the Internet of Things', *http://postscapes.com/internet-of-things-history*

[6] 'Internet of Things', Techopedia, *www.techopedia.com/definition/28247/internet-of-things-iot*

[7] BBC News, 'Chip and Skin: The Office That Microchips Its Staff', 29 January 2015, *www.bbc.co.uk/news/technology-31037989*

[8] Danova, Tony; 'Morgan Stanley: 75 Billion Devices Will Be Connected to the Internet of Things by 2020', *Business Insider*, 2 October 2013, *www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10?IR=T*

[9] Ericsson Mobility Report, '70% of the World Using Smartphones by 2020', *FutureTimeline.net*, 26 June 2015, *www.futuretimeline.net/blog/2015/06/26.htm#.VaasPWdFAfg*

[10] Fernandez, A.; 'Fiat Chrysler Recall Highlights Potential Need for Regulatory Changes', Gordon & Rees, 30 July 2015, *www.privacydatabreach.com/category/internet-of-things/*

[11] Council on Cyber Security, 'A Look at Applying the 20 Critical Security Controls to the Internet of Things, Part 1', 4 November 2014, *www.counciloncybersecurity.org/articles/a-look-at-applying-the-20-critical-security-controls-to-the-internet-of-things-iot-part-1/*; 'A Look at Applying the 20 Critical Security Controls to the Internet of Things (IoT), Part 2—Technology', 25 November 2014, *www.counciloncybersecurity.org/articles/a-look-at-applying-the-20-critical-security-controls-to-the-internet-of-things-iot-part-2/*; 'IoT and the Critical Security Controls, Part 3—Technology', 13 January 2015, *www.counciloncybersecurity.org/articles/iot-and-the-critical-security-controls-part-3/*; 'Internet of Things and the Critical Security Controls, Part 4—Technology', 20 February 2015, *www.counciloncybersecurity.org/articles/internet-of-things-and-the-critical-security-controls-part-4/*

[12] Council on Cyber Security, 'The Critical Security Controls for Cyber Defense', version 5.1, *https://ccsfiles.blob.core.windows.net/web-site/file/bb820ab03db7430abac40451ba4d3bb7/CSC-MASTER-VER5.1-10.7.2014.pdf?sv=2012-02-12&st=2015-08-24T20%3A16%3A59Z&se=2015-08-24T20%3A18%3A59Z&sr=b&sp=r&sig=4tbWY9lIpBZNEbdSQl1cMJu24QWLJ3WpOo1gH%2BWKFkk%3D*

[13] Rogers, Wendy A.; Arthur D. Fisk; 'Toward a Psychological Science of Advanced Technology Design for Older Adults', *The Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, 65B(6), November 2010, p. 645–653, *www.ncbi.nlm.nih.gov/pmc/articles/PMC2954331/*

[14] Driver & Vehicle Standards Agency, 'History of road safety, The Highway Code and the driving test', updated 26 March 2015, United Kingdom, *www.gov.uk/government/publications/history-of-road-safety-and-the-driving-test/history-of-road-safety-the-highway-code-and-the-driving-test*

Revising Cybersecurity Skills for Enterprises

Ivo Ivanovs works at EY EMEIA Information Security Advisory Centre, specializing in information security and data protection for companies in Eastern Europe. Ivanovs is also vice president of the ISACA Latvia Chapter.

Sintija Deruma, Education Chair of the ISACA Latvia Chapter, leads the BA School of Business and Finance's (Riga, Latvia) new master's degree program in cybersecurity management, the first such program in Latvia. This full-time master's program concentrates on the cybersecurity management domain and combines core cybersecurity management skills with a master's of business administration and Certified Information Security Management (CISM)-related curriculum tasks.

Cyberspace is a virtual environment. Today, it does not matter which device is used for connecting to the Internet. Millions of users are there—in that virtual place—conducting day-to-day activities such as communicating, shopping, paying bills, searching for information, reading news, doing business, and controlling or managing something.

Cybersecurity is the ability to protect or defend the use of cyberspace from cyberattacks[1] and is defined as the protection of information assets by addressing threats to information processed, stored and transported by internetworked information systems.[2]

MAIN CHALLENGES FOR CYBERSECURITY

The main challenges faced by governments attempting to enhance their cybersecurity capability and, by doing so, ensuring reliable and properly protected information resources are:

- The increased importance of the national coordination of information and communications technology (ICT)
- Cooperation between the public and private sectors
- International cooperation
- Reinforced incident response
- Effective crime control
- Critical infrastructure protection

The development of democracy and social networks has expanded the virtual environment and turned it into an effective collaborative platform for municipalities, governments and politicians, as well as criminals who do not respect national borders. These criminals are called by different names, based on their motivations and competencies, including terrorists, hackers and other attackers.

The positive impact of this virtual world on democratic processes, driven by active participation of the population, is indisputable. It includes education possibilities and information exchange using cyberspace. However, the dark side of it cannot be ignored. Data thieves are professional criminals deliberately trying to steal resources and information utilizing lack of competence by users and sometimes even those who should protect the users.

The UK report *Cyber Security Skills: Business Perspectives and Government's Next Steps*[3] makes clear that having the skills and capabilities to manage cyberrisk effectively can reduce the financial cost to a business from cybercrime, and it can also increase consumer confidence, providing that business with a competitive edge. As businesses increasingly take steps to protect themselves from cyberattacks, demand for cybersecurity products and services will continue to increase, providing growth opportunities for the organizations that supply them. A highly skilled workforce will enable cybersuppliers to derive maximum benefit from these opportunities.

Cyberthreats have the power to drive up costs and affect revenue for companies, making them similar to any other financial risk. What organizations need are practical tools to mitigate this risk.[4] Larry Clinton, Internet Security Alliance (ISA) president, said, "We need to connect the dots between the operational issues and the strategic issues which is what businesses focus on."[5]

PEOPLE AND SKILLS—PREPARING FOR CYBERSECURITY

Cybersecurity is a long-term trend in which information assurance, risk approach by default, and privacy by design indicate the evolution of information security and give broader understanding of cyberspace.[6]

Cybersecurity skills are key elements of an organization's preparedness to address cyberrisk.

Thus, in the field of cybersecurity, ability, knowledge and skills are essential for business survival in the virtual world and in the economy of tomorrow.

The recently released study, *State of Cybersecurity: Implications for 2015*[7] by ISACA® and RSA, reveals that 82 percent of organizations expect to experience a cyberattack in 2015, yet more than one in three (35 percent) are unable to fill open cybersecurity positions.[8]

The lack of cybersecurity professionals is a vulnerability in the three lines of defense.

The three lines of defense concept means collaboration and better understanding of how to

manage risk to an acceptable level. The first line of defense is responsible for day-to-day activities—monitoring and protecting information assets. The second line of defense is responsible for governing those tasks and ensuring that information assets have applicable monitoring, reporting and tracking; and the third line of defense is responsible for ensuring compliance.

In this case, soft skills for risk managers; auditors; process, information and system owners, including information security managers, are needed to resolve problems more creatively to assure the confidentiality, integrity, availability and accountability of an organization's information assets.

Cybersecurity will continue to pose a serious risk, of which top management needs to be aware, measure and supervise continuously. This process should be a part of the company's strategy, and top management plays a strategic role in implementing the cybersecurity culture.

The motivation of hackers ranges from individuals testing their skills to break into the US National Aeronautics and Space Administration (NASA) systems to well-organized criminal enterprises hacking for profit to intrusions sponsored by foreign intelligence services.[9]

The comparably small size of certain governments, for example, Latvia, to other European Union (EU) member-states combined with the small size of the companies operating in these smaller countries are two of the main challenges to developing and maintaining skilled cybersecurity resources to fight cybercrime, which, in fact, can be a well-organized, multinational business with strategy, processes and quality management, a dynamic infrastructure, robust cash flow, and highly-skilled professionals.

This situation is worsened by the job market in which leading security services companies aggressively cherry-pick cybersecurity specialists by offering lucrative compensation packages along with intensive training for skills development. Cybersecurity employees with years of faithful employment at small, regional banks, universities and state governments get employment offers they simply cannot refuse. Panic ensues at many organizations when they lose security professionals who, more or less, owned the organization's informal incident detection and response processes.[10]

A better understanding cyberecosystem elements, their relationships and main performance drivers makes it possible to plan and develop effective cybersecurity readiness, even within the limited resources and capabilities of small enterprises.

Cyberdefense requires short-term and long-term solutions for cybersecurity professionals in obtaining knowledge in different dimensions, including:

- Cybersecurity for computing professionals (e.g., computer science, software engineering)
- Cybersecurity for society (policy creators and decision-makers)
- Cyberdefense for operations

To strengthen the security of information resources, proactive behavior is no longer sufficient to safeguard the critical resources in the organization. Organizations need to go further; they need to reengineer the behavior, attitudes and knowledge of all stakeholders, including those outside the organization (e.g., customers, suppliers). It is obvious that all kinds of Internet users, regardless of their age, business area and confidence, should expand their knowledge.

> "Proactive behavior is no longer sufficient to safeguard the critical resources in the organization."

This leads to the conclusion that the main drivers toward reasonable cybersecurity are human resources—the capabilities for which can be developed as follows:

- Establish new professions
- Develop education curriculum
- Reengineer security awareness programs
- Reengineer mind-sets

The mind-set of the cybersecurity professional is a very important factor in preventing, detecting and mitigating security breaches. Developing this way of thinking must be part of recruiting and educating cybersecurity professionals,[11] recalling the similarity with opposite forces in which the mind-set of the hacker is the main advantage in distinguishing the good and not-so-good hacker.

The core competencies cybersecurity managers must possess include:

- Plan, organize, direct, control and evaluate the operations of cybersecurity management systems, formulating strategies, policies and plans, and security architecture taking into account the legal and ethical issues of cybersecurity.
- Plan, organize, control and continually evaluate risk management procedures.

- Direct and advise staff engaged in providing holistic information security management integration and establish security awareness training.
- Direct and control corporate governance and regulatory compliance procedures, incident handling, and management.
- Plan, administer and control security requirements for projects, contracts, equipment, services, inventory skills and competencies for related professionals.
- Accept the responsibility for processes associated with business contingency and disaster recovery planning.
- Prepare reports and briefs for management committees evaluating the cybersecurity ecosystem.

The Skills Framework for the Information Age (SFIA)[12] is a logical, two-dimensional skills framework defined by areas of work on one axis and levels of responsibility on the other. It has been proven to be an effective resource that benefits businesses by facilitating all aspects of the management of capability in corporate and educational environments.[13] Further, the US National Initiative for Cybersecurity Education (NICE) provides a common understanding of and lexicon for cybersecurity work, defined as the capabilities critical for successful job performance across cyberroles and the behaviors that exemplify the progressive levels of proficiency associated with these competencies.[14]

PEOPLE, NOT TECHNOLOGY, ARE KEY ELEMENTS OF CYBERSECURITY

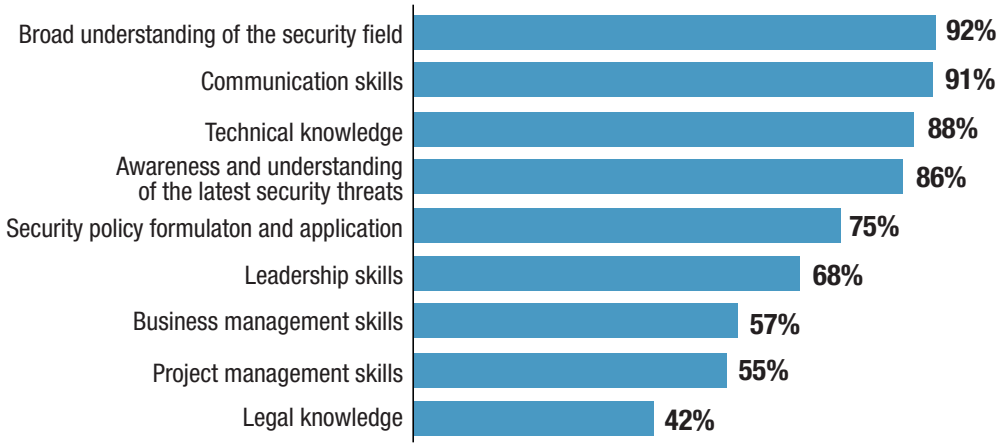
The 2013 (ISC)² Global Information Security Workforce Study[15] was conducted in 2012 through a web-based survey. The study's objective was to gauge the opinions of information security professionals regarding trends and issues affecting their profession and careers. Designed to capture expansive viewpoints and produce statistically significant results, a total of 12,396 surveys of qualified information security professionals were collected.

With security staff viewed as critical in importance, it is equally important to understand the acuteness of need, organizations' ability to fund staff expansion and improvement, and the sought-after attributes of information security professionals. When examining the sought-after attributes of information security professionals, it is not just the skills that are important. Confirmation of those skills and professionals' engagement in peer groups are also essential.

The 2013 (ISC)² Global Information Security Workforce Study respondents ranked success factors of professionals in order of importance as shown in **figure 1**.

Across the entire survey, broad understanding of the security field was on top in terms of importance, followed by communication skills; technical knowledge, awareness and understanding of the latest security threats round out the top four. While skill and knowledge building must never slow down—attackers, hackers and other cyberthreat actors certainly will not—information security professionals must also translate their risk management expertise into organization-wide leadership.

Figure 1—Success Factors of Information Security Professionals (Important and Very Important)



Source: *The 2013 (ISC)² Global Information Security Workforce Study*[16]

CONCLUSION

When taking into account the aforementioned frameworks and the demand in the market for new cybersecurity professionals, it can be concluded that good technical knowledge of cybersecurity alone is not enough to establish effective cybersecurity and broader understanding of the business and human management principles. Strategic skills are equally important, especially in smaller organizations that cannot afford narrow specialization of their resources.

ENDNOTES

[1] National Institute of Standards and Technology, NIST IR 7298 Revision 2, Glossary of Key Information Security Terms, USA, 2013

[2] ISACA, *Cybersecurity Fundamentals Glossary*, USA, 2014, *www.isaca.org/Knowledge-Center/Documents/Glossary/Cybersecurity_Fundamentals_glossary.pdf*

[3] Department for Business, Innovation and Skills, *Cyber Security Skills: Business Perspective and Government's Next Steps*, United Kingdom, March 2014, *www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf*

[4] Ayers, E.; "Public-private Push to Improve Boards' Cyber Readiness," Cyber Risk Network, 2014, *www.cyberrisknetwork.com*

[5] *Ibid.*

[6] Deruma, S.; *Problems and Solutions of Information Security Management in Latvia*, SHS Web of Conferences, vol. 10, 2014, *www.shs-conferences.org/articles/shsconf/pdf/2014/07/shsconf_shw2012_00007.pdf*

[7] ISACA and RSA Conference, *State of Cybersecurity: Implications for 2015*, 2015, *www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2015.aspx*

[8] *Ibid.*

[9] Martin, P. K; "Hackers Had 'Full Functional Control' of NASA Computers," BBC News, 8 March 2012, *www.bbc.com/news/technology-17231695*

[10] Oltsik, J.; "Cybersecurity Skills Shortage Panic in 2015?" *Networkworld*, 9 December 2014, *www.networkworld.com*

[11] McGettrick, A.; *Toward Curricular Guidelines for Cybersecurity, Report of a Workshop on Cybersecurity Education and Training*, Association for Compuitng Machinery, 30 August 2013, *www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf*

[12] SFIA Foundation, Skills Framework for the Information Age, UK, *www.sfia-online.org/*

[13] *Ibid.*

[14] National Initiative for Cybersecurity Education, USA, *http://csrc.nist.gov/nice/*

[15] Frost & Sullivan, *The 2013 (ISC)² Global Information Security Workforce Study*, USA, 2012, *www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf*

[16] *Ibid.*

Feature

A Business-integrated Approach to Incident Response

Hari Mukundhan, CISA, CISSP, has more than 13 years of extensive information security, IT audit, IT operations, and project and program management experience across a wide range of clients and businesses. He is currently a cybersecurity program manager in a leading private organization. He can be reached at *harimukundhan@yahoo.com.*

With the significant increase in the rate of cybersecurity incidents worldwide, the financial impacts due to these incidents have also soared. From 2013 to 2014, the total number of security incidents has increased by 48 percent to 42.8 million incidents, and the number of companies reporting losses of US $20 million or more has almost doubled over the same period.[1] In addition, the number of aggressive business disruption attacks that impact the network core is expected to increase significantly over the next three years.[2] Recent high-profile attacks on various large retail and financial organizations are cases in point.

A Poneman Institute study revealed that only 14 percent of companies surveyed said that their executive management takes part in the incident response process, and "as a consequence of this lack of involvement and awareness, incident managers may not only find it difficult to prioritize incident handling, but may also find it difficult to obtain the resources from business leadership to invest in the skills and technologies necessary to deal with future security incidents,"[3] which are expected to increase significantly. Therefore, incident handling as a function requires strong integration with operational risk management processes in a more systematic manner, so that the impact to business can be better understood and the prioritization of incidents can be more accurate.

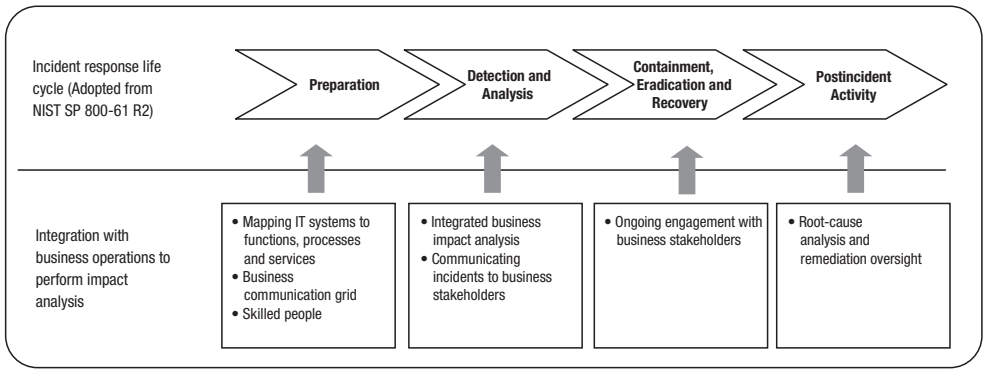
AN INTEGRATED APPROACH TO INCIDENT HANDLING

The US National Institute of Standards and Technology (NIST) "Computer Security Incident Handling Guide"[4] has been leveraged to emphasize the potential integration points between the security incident management process and operational risk management process and to provide a framework for incident managers and business managers to engage each other effectively. This article reviews each phase of the NIST process flow guide, identifies the integration points with business stakeholders and provides guidelines on how to operationalize those in a practical way (**figure 1**).

INCIDENT PREPARATION PHASE

The IT system infrastructure should be mapped to the business processes it supports, the governing functions and, ultimately, the client services delivered. This helps the incident managers estimate the overall business impact rapidly once they are reasonably confident about the accuracy of the incident precursor and indicators, which typically affect the infrastructure components (e.g., UNIX hosts, file transfer servers). Identifying the potential areas of impact is probably one of the most important and challenging parts of the incident response process.[5] But maintaining an evergreen map of how the system functions, processes and is

Figure 1—Incident Response Life Cycle and Business Integration



Source: Hari Mukundhan. Reprinted with permission.

Do you have something to say about this article?

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

Go directly to the article:

serviced provides organizations a significant advantage when they race against time to recover and respond to an incident.

In large organizations, documenting every process can be a time-consuming and costly exercise, but it does not need to start from scratch. There are some existing documents that could potentially be used to build the map, for example:

- US Sarbanes-Oxley Act of 2002-related process walk-through documents and test sheets can provide information on the process and supporting systems.
- Business impact analysis (BIA) and recovery time objective (RTO) documents can provide insights, albeit at a high level in many cases, on the functions, processes and services that may experience outages and estimates on how long systems may be unavailable.
- Risk and control assessment programs typically strive to map the business components to the systems to identify the operational risk to business due to the identified system risk factors.

An unfolding security incident, depending upon its scope, could create confusion and panic to both staff and customers. To proactively mitigate such confusion, incident managers should provide clear, precise, relevant and targeted information to various audiences. For the business stakeholders, the message should be as nontechnical as possible and must point to potential business impacts so that stakeholders can calibrate the responses on their side. The incident manager role in the information security organization has the best vantage point to provide such information. The incident manager should be prepared up front with the communication grid, i.e., what information should be communicated to which business stakeholders and during which life cycle stage of the incident. Appropriate templates, email distribution lists and call trees should be created up front in partnership with the business. Where possible, a dry run should be performed to fine tune the effectiveness of the communication channels and vehicles. **Figure 2** is an example of a communication grid.

As with many things, people make the difference between a good process and a great process. Staffing the incident management process with the right people with the right skill sets, especially at the integration points with business, helps in navigating the response to a more successful outcome. Ideally, such staff should have a good mix of technical, business and communication skills and be equally comfortable dealing with the technical teams and the business teams.

DETECTION AND ANALYSIS

Risk is typically a function of the adverse impact that arises if the circumstance or event occurs and the likelihood of occurrence.[6] Therefore, if the impact to business is unclear, the risk due to the incident is also unclear. This situation can potentially lead to incident response teams incorrectly prioritizing incidents. That is, it may outwardly appear that one incident is more critical than another, but, in fact, this may not be the case. For example, an externally facing web site that is being impacted by a denial-of-service (DoS) attack may appear more critical than the unavailability of a single sign-on (SSO) server that services many internal applications. But in the case of a web site with a commonly used SSO server, for example, its unavailability could cripple business operations. Obviously, in such a case, the SSO server incident needs to be prioritized ahead of the DoS attack incident. Because of situations such as this, quickly understanding the business impact in partnership with business managers is vital. The following are some of the business impacts that require analysis:

> "If the impact to business is unclear, the risk due to the incident is also unclear."

- **Financial impact**—Both a financial loss and an inappropriate financial gain to an organization due to an incident should be considered when determining the financial impact. Based on the capital requirements and the risk appetite, organizations should identify a threshold value beyond which a formal chief financial or risk office review is required. An inappropriate financial gain is still considered a financial impact that requires investigation, analysis and eventually corrective action. For example, a man-in-the-middle attack on an end-of-day net transaction file sent by a client may show that the client owes money to the firm rather than the other way around.
- **Legal and regulatory impact**—The impacts regarding legal concerns, such as contractual issues, regulatory fines and penalties, and breach of service level agreements (SLAs), must also be considered. Given the heightened regulatory environment after the global financial crisis, the potential impact to statutory and regulatory requirements needs to be given special attention.

Figure 2—Example of a Communication Grid

Information required for the communication grid:

1. Identify relevant stakeholders associated to various key processes and systems in the organization.
2. Pre-establish communication channels and contact details:
   a. Identify audio and video conference numbers. Preferably, maintain a separate conference line for senior management.
   b. Create email distribution lists.
   c. Create call tree(s) to broadcast message to business users.
   d. Where possible, obtain dedicated rooms with both video and audio conferencing facilities.
   e. Maintain key stakeholder official contact information.
3. Create email, call tree, etc., communication templates.
4. Create a communication grid to determine 'what should be communicated to whom' with clarity on what MUST (mandatory) vs. what SHOULD (recommended) be communicated to whom. In other words, mandatory vs. recommended.

Key Incident Management Actions	Relevant Stakeholders					Communication Channel
	Technology and IT Security Managers	Business Manager	Senior Management	Functional Heads (Business and Administrative)	Business Users	
Complete initial notification of potential business-impacting incidents.	Must	Must	–	Should	–	Email distribution list
Evaluate business impact on a continuous basis.	Should	Must	–	Should	–	A/V conference/contact list/ In-person
Perform periodic executive updates.	–	–	Must	Should	–	Senior management A/V conference lines
Communicate business impact.	Should	Must	Must	Must	Should	Email distribution list
Evaluate and finalize containment, eradication and recovery options.	Must	Must	Should	Should	–	Email distribution list
Communicate actions and relevant information around the finalized option.	Must	Must	Must	Must	Must	Call tree
Perform periodic recovery updates.	Must	Must	Must	Must	Must	Call tree

Source: Hari Mukundhan. Reprinted with permission.

- **Operational impact**—A partial or full inability to run the day-to-day business operations of an organization needs to be considered. Depending on the type and scope of the incident, an impact to business operations may or may not impact customer service. It may or may not impact finances. It can be organizationwide or can be limited to a certain section. However, a sustained impact to operations typically leads to a cascading financial, regulatory and/or reputational impact.
- **Reputational impact**—Reputational impact occurs when negative publicity regarding an institution's business practices leads to loss of revenue or litigation.[7]

Typical incident documentation tends to delve deep into the technical details related to the incident (e.g., the IP addresses impacted, details of the system log files, the network layer in which the incident occurred). However, as noted in the incident preparation stage, the incident manager should keep the message nontechnical and focus on the potential impacts to the business in a plain and simplistic fashion. The communication templates created during the incident preparation stage can be utilized to get the key messages out as soon as possible via email distribution lists, call trees or conference calls.

The following are some of the key aspects to be taken into consideration while documenting and communicating the incident:

- Determine the incident types and the severity level at which business engagement is required. Note that not every incident warrants a business engagement. Also take into consideration the sensitivity of the information before sharing.

- Develop templates and guidance to create a high-level, nontechnical executive summary articulating the scope and depth of the incident. Target this toward the executive business leaders.
- Develop templates and guidance to create a detailed, nontechnical write-up articulating the impact to IT systems and, thereby, the potential processes and services that could be impacted. Such communication is typically targeted toward the function heads, managers and staff.
- Maintain email distribution lists, call trees and other possible communication channels that can be used for communication during the incident.
- As required, train incident managers on the important aspects of business communication.

CONTAINMENT, ERADICATION AND RECOVERY

For incidents that have a business impact, the incident manager and the business manager have to work closely to ensure that business response is timely and adequately calibrated. If the incident and the business impact is an evolving one, the incident manager may have to invite the business manager to brief, periodic touch-point meetings to appraise the current state of the incident's scope and depth and how it is being contained and eradicated. The business manager, depending upon the evolving state of the incident and its containment or eradication success rate, would, in turn, be expected to constantly reassess the impact and respond accordingly. For example, if a network worm has brought down only a small number of desktops used by operations staff and the incident response teams are able to successfully contain, eradicate and restore services quickly, then the impact to customers may not be significant and the business may have to simply wait for the rest of the desktops to be up and running. On the other hand, if the network damage is spreading fast and is outpacing the incident response team, the business managers may have to consider other options, such as activating a disaster recovery site, transferring work to a different location or shifting to a manual option.

Periodic engagement with the business manager during this phase has the following advantages:

- Provides a constant feedback mechanism to the incident managers on the priority level of an incident
- Provides feedback on the effectiveness of the business continuity plan, thereby improving the resilience of the organization and its functions
- Assists in proactively managing news media, social media, regulators, vendors and other third parties

- Manages client expectations accordingly
- Prepares the business proactively for legal and other contractual impacts
- On a long-term basis, aligns the cybersecurity agenda with the business strategy

POSTINCIDENT ACTIVITY

The postincident activity section of the NIST guide[8] provides excellent insights on how to arrive at lessons learned and how to improve the incident response process in general. Performing a root-cause analysis for impactful incidents and following it up with remediation measures is important. In simple terms, the incident manager should be able to document the relationship between the incident's root causes and the business impact and how the incident was contained, eradicated and recovered. A joint lessons-learned session should, at a minimum, focus on the following:

- Identify accountable parties to the incident root cause and assign ownership to remediate.
- Determine if the incident has recurred along with a recurring financial impact. If the probability of the incident occurring in the future is also high, consider whether additional capital needs to be allocated to cover for future potential losses.
- Update the system's function-process-service map and other documentation, if required.
- Determine whether the business impact was calculated accurately and what needs to be done to improve the calculation.
- If the disaster recovery site was activated, check whether the recovery plan requires an update. Interface with business continuity managers to carry forward the update.
- Constant oversight should be provided by business managers to ensure that root-cause owners are remediating the root causes on time and business management is kept updated.

CONCLUSION

To help keep the cybersecurity agenda consistently aligned with business priorities and to provide a practical and effective mechanism for prioritizing incidents, an integrated approach to incident management is vital. Response and recovery can be more targeted and more efficient. Additionally, incident managers may find themselves in a better position to obtain resources to invest in skills and technologies that are required to deal with future incidents.

ENDNOTES

[1] PricewaterhouseCoopers, "Global State of Information Security Survey: Key Findings and Trends," 2015, *www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml*

[2] Gartner, "Gartner Says By 2018, 40 Percent of Large Enterprises Will Have Formal Plans to Address Aggressive Cybersecurity Business Disruption Attacks," 24 February 2015, *www.gartner.com/newsroom/id/2990717*

[3] Ponemon Institute, "Cyber Security Incident Response: Are We as Prepared as We Think?" January 2014, *www.lancope.com/sites/default/files/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf*

[4] Cichonski, P.; T. Millar; T. Grance; K. Scarfone; "Computer Security Incident Handling Guide," NIST Special Publication 800-61, August 2012, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf*

[5] *Op cit*, Cichonski

[6] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," NIST Special Publication 800-30, USA, September 2012, *http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf*

[7] Federal Financial Institutions Examination Council, *IT Examination HandBook*, InfoBase, USA *http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/retail-payment-systems-risk-management/reputation-risk.aspx*

[8] *Op cit*, Cichonski

Real-life Risk Theory

Mette Brottmann is a senior risk analyst and controller in a bank.

Klaus Agnoletti is a senior security specialist at an outsourcing vendor.

Morten Als Pedersen is responsible for IT security at a university.

Ronnie Lykke Madsen is chief information security officer at an audit company.

Michael Rosendal Krumbak is an IT security specialist at a pharmaceuticals company.

Thor Ahrends, CISA, CISM, CRISC, is an IT security consultant, IT auditor and senior manager at an audit company. He has worked as an IT security consultant and IT auditor at several recognised companies.

Most IT professionals know the theory and importance of addressing and mitigating risk. Daily resource limitations and task prioritisation, however, do not always allow for best practice approaches to be taken.

ERFA (erfaringsudveksling) is a Danish concept that means "knowledge sharing." A group of Danish security experts meets four times annually to discuss new threats, technologies and issues experienced. The group members include IT security experts working in, for example, big and medium-sized banks, consulting firms, manufacturing companies and universities. All discussions are treated confidentially. The authors of this article are some of the members of this group. The participants have discussed day-to-day issues and lessons learned have been collected in this article.

The basic idea behind the approach outlined herein is to define some basic tasks that can be used as eye-openers to drive the business case for further risk work. This article outlines real-life approaches to risk work used by members of the ISACA® Denmark Chapter's RiskERFA group (the group).

Working with risk is needed to balance IT security controls. How is it possible to determine the protection level of IT assets if these are not categorised and associated with a financial value? Risk-based controls are growing in importance, and no one can disagree that the business side must be involved and stakeholders must commit.

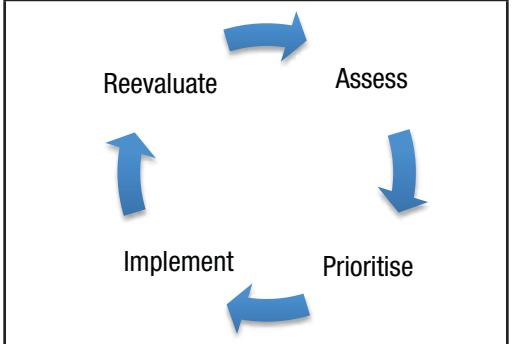
During discussions, the group realised that the COBIT® 4.1 Capability Maturity Model level 5 sometimes is out of reach in daily tasks and procedures. Complex procedures and strict requirements for documentation may collide with requirements for lean business operation.

Topics of discussion that contributed to this realisation included:

- At a large, 40-year-old Danish company with a tradition of *ad hoc* procedures, limited documentation and an unstructured risk management process made it difficult for the IT department to identify critical processes. Instead, the IT security department, supported by IT operations personnel, identified the 21 most important IT services that are now the basis for developing general information security management system (ISMS) processes.
- Using different cases, the group also discussed how the risk of IT projects can be assessed informally simply by asking the project owners, 'What is the worst thing that could happen with this new service'? Through these discussions, the risk is clarified on a common basis and risk/impact may informally be classified.
- Risk regarding personal data and privacy are always on the agenda. The coming European Union Data Protection Regulation will only emphasize privacy risk. To quantify not only direct risk, but also indirect risk (e.g., reputational risk), it might be relevant to reach out to departments (e.g., communications, human resources).

Rather than aiming only at a high maturity level, it is possible to significantly improve the basis for decision making by performing some simple initial steps. This also stimulates the process of increasing the maturity level by asking relevant questions to the relevant actors participating in the risk work, thereby raising awareness and attracting management support for implementing a more formalised ISMS.[1] The process is a continual improvement circle, as illustrated in **figure 1**.

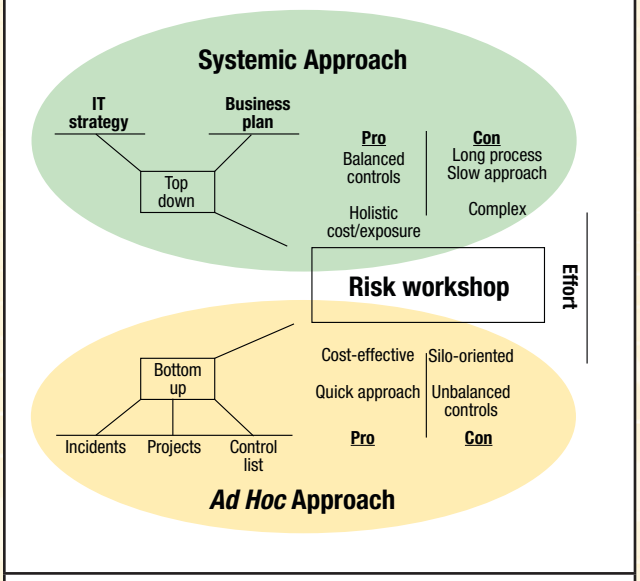
Figure 1—ISO Plan-do-check-act Approach



Source: The Danish RiskERFA (Brottmann, Agnoletti, Pedersen, Madsen, Krumbak and Ahrends). Reprinted with permission.

Figure 2 was agreed upon by all group members. The risk approach can be top down or bottom up. Sometimes both approaches are used at the same time within the company. Different projects and organisational units may benefit from using different approaches. This is also a way of risk orienting the risk approach. The work is best organised in a structured risk workshop with participation from both the line of business and IT security professionals.

Figure 2—Risk Workshop Model



Source: The Danish RiskERFA (Brottmann, Agnoletti, Pedersen, Madsen, Krumbak and Ahrends). Reprinted with permission.

Determining the methodology to use should be a conscious decision based on the following points:

- Business requirements, legislative compliance and contractual requirements
- Urgency of timely clarification
- Complexity of the area in question
- Internal process flow complexity and conflicting interests
- System implementation and technology legacy

Some industries (e.g., pharmaceuticals, banking) have strict compliance requirements covering risk mitigation and risk reporting. Compliance requires a formalised approach, but the bottom-up method can also be used in these cases as long as the outcome is communicated in a formalised risk report, issues are identified and continuous improvements are initiated if needed.

Any risk activity must be anchored with a business owner (system or project owner). Anchoring should be determined by who will suffer the most if something breaks (both in the short and medium term).

Alignment with business policies and strategic initiatives must be ensured by the IT facilitator as part of the risk workshop.

The bottom-up approach for specific projects and/or compliance-driven adjustments is most often the reality. Anchoring is, therefore, essential; otherwise, the initiatives lose value. The bottom-up approach requires coordinating multiple diverse risk activities.

In contrast, the top-down approach requires a complete overview of assets, which is hard to establish in a large organisation. Complex challenges must be addressed, and a top-down approach requires some form of formalised role managing of the risk work. The outcome is highly dependent on the required organisational muscles and implemented governance framework. There is no right or wrong approach. The proper approach is most often a combination of the two approaches.

The following pragmatic suggestions are based on actual findings within the group:

- **Workshop**—Input must be gathered from both subject matter experts (SMEs) and groups with more generic knowledge (line of business). Only by combining the two can the decision makers acquire the necessary information. From a risk-view maturity level, three out of five is, in many cases, sufficient (using the COBIT® Capability Maturity Model scale).
- **Simplification**—A fast-track approach could be to ask business areas to identify the top-five pain points/risk factors for each business area and start the risk work within this scope. This may be done by interviewing the individual responsible for the relevant business areas. Another way of rating could be to prioritise high-revenue areas or high-damage areas.
- **Mapping**—The IT facilitator then needs to identify the infrastructure/systems required to support the areas identified by business.
- **Scoring**—The focus should be on simple and tangible deliveries, with simple scoring on a scale of one to five. Use a simple chart illustration to show deviations from the defined baseline.

- **Enforcement**—Recommendations or requirements are not effective without necessary anchoring. The risk owner must have both the power to make decisions and resources to enforce implementation processes, projects and systems.
- **Learnings**—Actual incidents should be evaluated, the realised cost should be compared to the expected cost and the model should gradually be improved. The outcome of this work will be a prioritised improvement list and potentially a business case with embedded cost calculations.
- **Continuous**—With constant measuring, mitigation and response, the risk assessment can accommodate changes in use and threat exposure. This result can be trusted as a decision tool. The assessment should be followed by implementation of prioritised risk controls.

Currently the method described is being further developed in real-world cases among the members of the RiskERFA. Future lessons learned will be shared in a subsequent article.

Enjoying this article?

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

www.isaca.org/topic-risk-management

AUTHOR'S NOTE

The article is a product of contributions from all RiskERFA group members, including, but not limited to those listed on authors of this article.

ENDNOTES

[1] International Organizations for Standardization, ISO 27001, *www.iso.org/iso/home/standards/management-standards/iso27001.htm,* or ISO 27002, *www.iso.org/iso/catalogue_detail?csnumber=54533*

Feature

Risk and Ethics in Cyberspace

Wanbil W. Lee, DBA, is principal director of Wanbil & Associates; president of The Computer Ethics Society; adviser at the Centre for e-Commerce and Internet Law, Vienna; member of the International Expert Network, Nous Global, UK; and adjunct professor at several universities. He has devoted more than five decades to the field of computing, spanning the banking, government and academic sectors, mainly in Australia and Hong Kong. His teaching and research interests focus on ethical computing and information security. Lee also speaks to a wide range of audiences in Asia, Europe and Australia. He is a member of several learned societies and sits on committees/boards of some of those bodies, advisory committees of the Hong Kong government and editorial boards.

Of all the human inventions since the dawn of civilization, the computer is the only one that extends our intellectual power. All others extend our physical power. The upside is that the computer can bring joy; the downside, misery. There is no problem with joy, but that is not the case with misery. How to minimize the vulnerability, eliminate the threat or mitigate the risk associated with the problem is the question.

IT professionals have been relying on all sorts of countermeasures, including the familiar technical access control mechanisms (such as firewalls, cryptographic algorithms and antivirus software [AVS]), computer law and computer audit, yet organizations still suffer negative consequences. Why is this so? There is something wrong somewhere, but what is it and where does the fault occur? Perhaps our understanding of risk needs be updated; education across science and technology needs be improved; effective decision models need be implemented as the ones currently in use are less than effective; and the Internet community needs to give ethical consideration to developing and using information and communications technology (ICT) products and services.[1]

SHIFTING THE UNDERSTANDING OF RISK TO MINIMIZE MISINTERPRETATION

Security problems—whether of a technical or nontechnical nature—are rooted in human error, to which no one is immune. Wherever and whenever there is vulnerability, there is threat ready to exploit it. Risk will result when threat is actually carried out.

To mitigate risk (that is, the damage, loss or destruction of what one wants to protect), one must deal with vulnerability and identify threat. It can be said that risk is a function of vulnerability and threat [r = f (v, t], and exposure to risk is a function of probability (the likelihood that risk occurs) and damage (of technical, financial and ethical nature) [r = f (p, d)].

It has been argued recently that people have long been influenced by the misinterpretation of risk,[2] that risk is taken as a technical concern and measured in economic and legal terms, but it is, in fact, a managerial concern as well and should be evaluated in socio-technical as well as legal-financial terms. This is a mistake and the technical, economic and social aspects should be recognized in order to gain a holistic view.

To make the point, here are several cases for illustration.

Case 1

When planning to replace a corporate legacy system with a web-based facility, concentrating on potential economic efficiency such as improved speed, elimination of redundancy or even reduced head counts means missing such adverse consequences as end-user dissatisfaction and deterioration in morale (due to the disturbance to inertia).

Case 2

Evaluating information governance of a computer-based system, but failing to include an audit of or a check for ethical issues, runs the risk of a deficient information security management review.

Case 3

Assessing softlifting[3] by focusing on the economic and legal impact, such as infringement of copyright law, and leaving out the social impact, such as personal use of sensitive proprietary information, will result in a risk of an incomplete assessment.

Hence, it is important to recast our mind-set and shift our understanding of risk in order to manage risk exposure.

IMPROVING EDUCATION ACROSS SCIENCE AND TECHNOLOGY

Cybercrimes are proliferating and reaching every corner of the world with no sign of slowing down despite the extant preventive measures that comprise technical access control mechanisms and computer laws. Cybercriminals are well educated and equipped with specialized

knowledge and skills, but they apparently lack a spirit of care for moral justifications. This could be attributed to a flaw in science and technology[4] education that has rendered the teaching/training of science and technology an act of indoctrination with lopsided learning objectives and syllabi dominated by hard, specialized knowledge and skills only. The resultant graduate scientists and technologists become obsessed with short-term technical excellence and economic gain.

The flaw is that the adopted curricula tilt toward technical and economic efficiency vs. long-term, human-centered social acceptability and cultivate a sense of egoistic financial gains, but neglect moral implications. Soft knowledge and skills should be an integral part of the curriculum proper, as they are needed to nurture an awareness of altruistic consequences.

To investigate the impact of education on human behavior in general, and knowledge of computer ethics and students' attitudes in particular, a seven-year (2006 to 2012) exploratory study, consisting of an annual survey, was undertaken.[5] The empirical data showed that less than 10 percent of the students surveyed claimed that they were aware of computer ethics, more than 60 percent were not sure if they carried out their work ethically, and approximately 30 percent thought that they carried out their work ethically. By deducing from these data, it was concluded that ethics education has a positive impact on the students; that is, knowledge of ethics arguably has an effect of lowering the rate of abuse, and computer science curriculum can be improved by including a module on computer ethics and social responsibility.

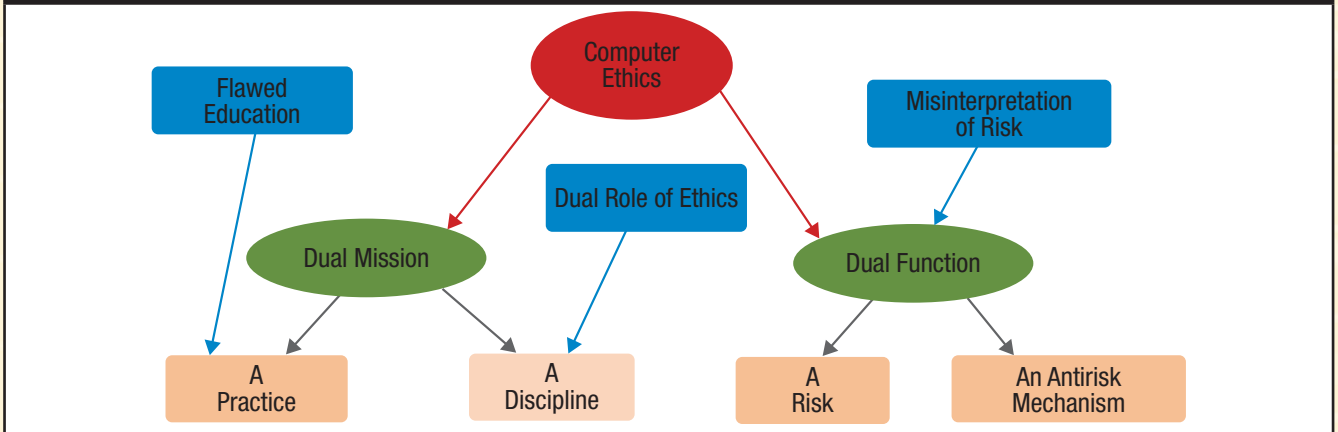
IMPLEMENTING EFFECTIVE DECISION-MAKING MODELS IN CYBERSPACE

Under the dual influences of the misinterpretation of risk and flawed education on science and technology, decision makers invariably focus on the technical, economic and legal variables only, with ethical considerations left out. The resultant decision analysis—composed of cost-benefit and risk analyses—is deficient. To address the deficiency, or to assess social acceptability and detect the possible adverse impact of ethical consequences, the Ethical Movement in Cyberspace (Ethical Movement), which is advocated by the Computer Ethics Society (*iEthics*),[6] alerts us to a new type of risk (ethical risk), a new category of anti-risk mechanism and a new tool for ethical analysis (Ethical Matrix). It also suggests adding ethical analysis to the decision-making tool kit and to use the Ethical Matrix method for ethical analysis.

COMPUTER ETHICS

Computer ethics is generally considered a static and passive domain concerned with the social and ethical impact of the computer. Generally speaking, it addresses ethics in cyberspace and is concerned with the ethical dilemmas encountered in the use and development of computer-based application systems. Of course, it is formally defined, and among its many descriptions is Moor's often-quoted classic definition.[7] The Ethical Movement proposes that computer ethics is not only static, but also dynamic and positive, and represented by a double duality model, depicted in **figure 1**.[8]

Figure 1—Conceptual Graph of Double Duality



Source: Wanbil Lee. Reprinted with permission.

COMPUTER ETHICS AS A DIFFERENT TYPE OF RISK

As alluded to earlier, using the computer in contradiction to ethical principles constitutes a different type of risk *vis-à-vis* risk of a technical, legal or financial nature because risk is a technical and managerial concern and it should be measured in financial, legal and moral terms with equal priority.

COMPUTER ETHICS AS A KIND OF ANTIRISK MECHANISM

Checking for potential ethical impact (in addition to technical and economic efficiency) adds a step, or steps, to the other established antirisk routine countermeasures (including cost-benefit analysis and risk analysis). For example, going through the process of applying the Ethical Matrix method for ethical analysis will force decision makers to consider adverse consequences and may reveal such risk areas as low user morale and dissatisfaction or potentially undesirable consequences of a social or moral nature that would otherwise be missed in the typical antirisk checks and audits. It will also raise technical and economic efficiency issues such as improved speed, elimination of redundancy or reduced head counts. This makes computer ethics a different kind of antirisk mechanism *vis-à-vis* the extant risk countermeasures.[9]

These extant countermeasures are being rendered impotent by emerging complex and sophisticated applications and technologies such as the Internet of Things (IoT), big data and cloud computing, and by the ever-lurking perpetrators who are always ready to crack any new countermeasures soon after they are developed and released.[10] Antirisk development is becoming more difficult. New antirisk mechanisms are, thus, called for to strengthen the weakened existing mechanisms.

The Internet community is a powerful group in contemporary society as it handles and has under its control a powerful commodity: information. That commodity has an immense impact on our technical, economic, legal and mental well-being. This group has the responsibility to resolve these issues and should realize that although ethics is the same in cyberspace as in the physical world, its implication is different. To fill this gap, the Ethical Movement has come up with a new meaning for computer ethics as a risk and an antirisk mechanism. Moving from concept to practice, it has been proposed that this antirisk mechanism be adopted as an alternative anticrime mechanism and as a new approach to evaluating trust.[11]

THE ETHICAL MATRIX

The Ethical Matrix is a conceptual tool originally designed for making decisions about ethical acceptability of technologies in the field of food and agriculture,[12] and the project "Bioethical Analysis in Technology Assessment: Application to the Use of Bovine Somatotrophin and Automated Milking Systems"[13] is an early application of the ethical matrix. The aim is to analyze the ethical impacts of injecting subcutaneous *bovine somatotrophin* (bST), a commercially produced hormone, into dairy cattle in order to increase the milk yields to respond to two concerns: 1) Diminishing well-being of the cattle because higher metabolic demands may lead to increased rates of illness, and 2) Threat to the consumers' health because of an increase in the milk concentration of insulin-like growth factor 1 (IGF-1).

In general, the matrix is made up of as many rows and columns as the particular case needs. A row is allocated to a stakeholder (an interest group of people, including clients, employers and probably the general public), a column is assigned a "value" representing respect to ethical principles and the cells contain the concerns of the stakeholders (the main criterion that should be met with respect to a particular principle). The method can be applied in two or three steps as follows:

1. Identify and determine the stakeholders, the values representing the respective ethical principles, and concerns of each stakeholder with respect to the ethical principles.
2. Assess/quantify the perceived relative impacts by the identified concerns of the particular interest group with respect to the ethical principles.
3. Debate, deliberate, discuss and decide.

Specifically in the test case, four stakeholders were identified (thus, four rows) humans (food consumers and producers) and nonhumans (farm animals and biota)—and three values were found relevant (thus, three columns):

- Well-being (representing utilitarian values, i.e., "maximizing the good for the maximum number of people")

- Autonomy (representing deontological values or "treating everyone as ends, not means"—in essence, the Golden Rule)
- Fairness/justice (representing justice in the categorical imperative sense or corresponding to Rawls' notion of "justice as fairness" [one person's benefit or gain is consistent with that of others, and fair equality of opportunity, but tolerable of social and economic inequalities for those that would benefit the least advantaged members of society]).

A generic example of an ethical matrix and an illustration of the ethical matrix used in the project can be found in the *Ethical Matirx Manual.*

It is noteworthy that sometimes the matrix is used for identifying ethical issues only (i.e., step 1 alone). The deliberations and discussions taken to arrive at those issues may contribute helpful hints to the final decision. Further, with appropriate adjustment, the matrix can be adopted for other fields and has been used in other situations. For example, the method was applied to perform an ethical analysis of postimplementation concerns arising from a project for an organization that was replacing its existing offline help-desk platform with an online monitoring system at a high-tech facilities distributor. The concerns thereof are of an ethical nature and include the staff's concern over personal privacy invasion at work; the firm's problem with potential damage to corporate image, personnel welfare and staff morale; and the professionalism and deontological issues for the chief information officer (CIO) and the technical team.[14]

The result of the first-cut analysis is shown in **figure 2**. Subsequent steps, including quantifying the concerns, evaluating the relative strength or weakness of each concern, and making the recommendation, are not included here in the interest of space. Analysts should note that the underpinning principles mentioned earlier should be consulted in carrying out these steps.

Finally, it is worth noting that the columns and rows may be swapped with each other, giving an alternative structure.[15]

ETHICAL CONSIDERATIONS FOR THE INTERNET COMMUNITY

ICT professionals of various ranks, including CIOs, tend to offer support when asked for an opinion on the importance of computer ethics, but when pressed for elaboration as to what computer ethics is or why it is important, many may respond in silence. To proceed, a real appreciation of basic ethical principles is needed.

To start, one can look to the Edward Snowden episode. He "blew the whistle." Some respect him, calling him a hero; others disapprove of his actions, calling him a traitor. Is he defensible on ethical grounds?

One might have heard these arguments: "Snowden is not the only one. There are plenty of other whistle-blowers," or "If Tom, Dick and Harry can do it, why not Edward Snowden?" These arguments are based on the concept of relativism.[16]

Hence, if one person thinks it is right to say Snowden is a hero, but another individual does not think so, the argument is pointless, as it allows two people to decide right and wrong for themselves. In the end, no moral distinction between the opinions of the two individuals can be made. Certainly, the debate does not tell us whether Snowden's actions are morally right or wrong.

But Snowden is no ordinary worker; he is a professional, one who engages in a job that handles a highly sophisticated commodity—confidential information. He was an employee of the US National Security Agency (NSA). In this capacity, Snowden appears to be wrong and disloyal to his employer in stealing and disclosing confidential information without authority. However, while, as a professional, Snowden is expected to respect professionalism and observe his professional code of conduct, as a person, he has a duty to

Figure 2—The First-cut Results

Stakeholder \ Values	Well-being	Autonomy	Justice/Fairness
Firm	Personnel welfare, corporate image	Personnel protection	Staff morale
Staff	Personal privacy	Freedom of personal movement	Exploitation by minority
Executive vice president	Job security	Firm's welfare	Entitlement of support resources
CIO	Corporate policy regarding system utility	Professionalism	Distribution of computer resources

Source: Wanbil Lee. Reprinted with permission.

himself and his moral convictions. This duty-based argument is based on the theory of deontology.[17]

So, as an employee, Snowden failed because he was disloyal and leaked confidential information. But, as a professional, he was right in exposing the stealth act because he was acting in accordance with professional conduct. While helpful in defending duty-bound actions, this principle is inherently troublesome because the actor owes responsibility to the multitude of stakeholders, and each of the stakeholders has its own aims that may be conflicting with one another.

Next, think of the impact or the consequences of Snowden's actions. The consequences may be beneficial or harmful. Snowden might have done "good" for the victims in particular and the world at large and "bad" for NSA and the US government. This results-based argument, known as consequentialism or utilitarianism,[18] certainly supplements the duty-based argument, but it leads to questions such as, "How good? How bad? And for whom?"

The consequentialist argument is not sufficient and raises questions about for whom or for how many the result is good. This argument needs to be supplemented with a utilitarian view. A utilitarian argument may be useful to suggest the issue of for whom or what purpose the good result is beneficial or the bad result harmful, but it raises further questions that include, among others, quantifying and comparing the results.

As can be seen, even after taking into consideration the so-called Golden and Silver rules, categorical imperative and social contract theories,[21] none of these principles alone can help resolve ethical dilemmas. Balancing the respect for each principle with the needs of the different stakeholders is necessary to reduce conflicts and arrive at a technically efficient, economically sound, legally viable and socially acceptable solution. A mix of some or all of these principles is needed. The Ethical Matrix could be the answer.

It is important for the Internet community to be equipped with knowledge of computer ethics, especially its role as a different type of risk and an alternative type of antirisk mechanism, and to give ethical consideration to the design and implementation of ICT products and services. Only then can one hope to be truthful to oneself and trusted by all other stakeholders.

CONCLUSION

Computer ethics is unlikely to become less important over time. Instead, it is poised to become an increasingly important aspect for those who create applications and solutions and those who use them. While the ramifications of every ethical decision are broad and diverse, a few basic good practices can be defined:

- Know your risk and what it should be.
- Be educated in science and technology. Ensure that your education includes ethics, an oversight in current curricula that needs to improve.
- Know your decision model, including the shortcomings of those in current use and the updated versions.
- Know your ethics. Understand the common ethical theories that underpin computer ethics so you can make up your mind when faced with a case like that of Edward Snowden.
- Know computer ethics, its new meaning and new functions so that you can convince yourself and others to give ethical consideration to the design, development and use of ICT products and services.

ENDNOTES

[1] Lee, W. W.; *e-Crime & understanding Risk & Ethics in Cyberspace*, Inaugural e-Crime Congress, Hong Kong, 11 June 2015

[2] Lee, W. W.; "Ethical Computing," *Encyclopedia of Information Science and Technology, 3rd Edition*, 2015, p. 2,991-2,999

[3] "Softlifting" is the software equivalent of shoplifting, which is basically not intended for financial gain and is often mistakenly believed by many to be legal. It occurs, for example, when a person copies a friend's software or brings a copy of software home from work for personal use. Though commonly considered a category of computer crime, softlifting falls more properly within the area of intellectual property law. Under the US Copyright Act of 1976, it is illegal to make or distribute copies of copyrighted material without authorization. Also, the Act provides a variety of remedies to compensate the plaintiff and punish the offender.

[4] *Op cit.*, Lee, 2015

[5] Lee, W. W.; K. C. C. Chan; "Computer Ethics: A Potent Weapon for Information Security Management," *ISACA® Journal*, vol. 6, 2008, *www.isaca.org*

[6] The Computer Ethics Society (iEthics), *www.iEthicsSoc.org*

[7] Moor, James H.; *Metaphilosophy*, Blackwell Publishing Ltd, 1985, p. 266-275. "Computer ethics is the analysis of the nature and social impact of information and communication technology, and the corresponding formulation and justification of policies for the ethical use of such technology."

[8] Lee, W. W.; *Ethical, Legal & Social Issues*, Postgraduate Diploma in eHealth Informatics, lecture notes, University of Hong Kong, 2014-15

[9] The extant countermeasures can be grouped in the following four categories: technical access control, computer law, risk analysis and computer audit.

[10] Lee, W. W.; *Information Security Management: Semi-intelligent Risk-analytic Audit*, VDM Verlag, January 2010

[11] Lee, W. W.; *Ethical Movement: An Alternative Anti-crime Mechanism in Cyberspace*, 16th Info-Security Conference, Hong Kong, 29 May 2015

[12] Mepham, B.; M. Kaiser; E. Thorstensen; S. Tomkins; K. Millar; *Ethical Matrix Manual*, LEI, The Hague, 2006, *http://mycourses.flyuvu.com/external_media/class_files/410G/ET2%20manual%20(Binnenwerk%2045p).pdf*, 2006

[13] *Ibid*.

[14] Lee, W. W.; "Why Computer Ethics Matters to Computer Auditing," *ISACA® Journal*, vol. 2, 2014, *www.isaca.org/journal/*

[15] Lee, W. W.; "Pitfalls & Ethical Issues in Internet & Social Media," Tea Gathering Seminar, organized by the Hong Kong Institution of Engineers for the Veneree Club, 18 September 2013.

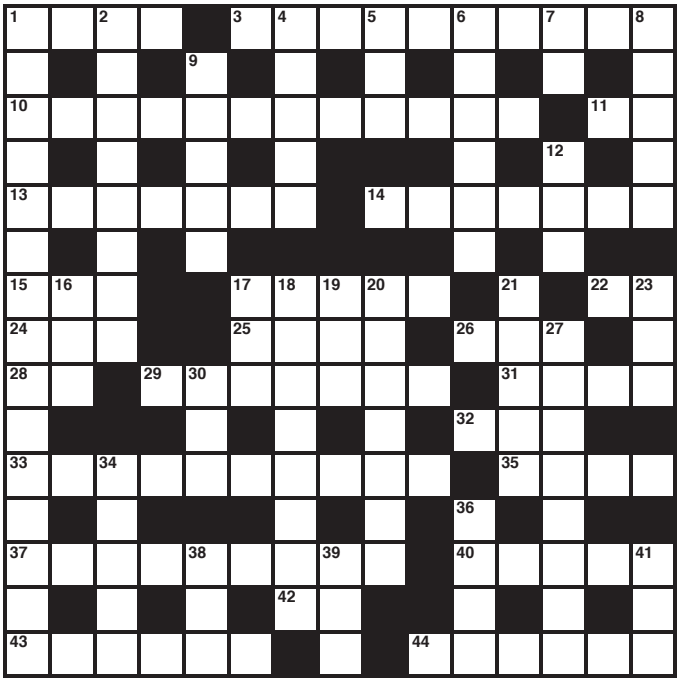
[16] *Ibid*.

[17] *Ibid*.

[18] *Ibid*.

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1. Institution that issued "Framework for Improving Critical Infrastructure Cybersecurity," abbr.
3. Best defense against cyberattacks
10. Corporately, a means to achieve justice and well-being
11. ___-sect
13. Compensate
14. Disclose
15. Old scanning device, abbr.
17. Cloud____ free and effective contract management solution
22. Information systems, for short
24. Passing phase
25. Famous astronaut first name
26. Crystallize
28. Promotion
29. Type of software that detects and defends against malicious programming
31. Data____
32. Defraud
33. Practicing politically motivated technology operations
35. Slant
37. In an early stage of development
40. Conduct a formal review of the operations of a company to find flaws and improve processes and structure
42. Head __ head
43. Main character in "The Imitation Game"
44. Poor ____ control is a frequent cause of projects going wrong

DOWN

1. Type of risk one is dealing with, 4 words
2. Basis for comparison
4. Approaches
5. Map abbr.
6. Predicament
7. Internet address
8. Too trusting
9. In accordance with, 2 words
12. Key above caps lock
16. Computer design abbreviation
17. Explosive initials
18. ____ the wheel
19. Goal
20. Of recognized authority and excellence
21. Visual sales pitches
23. Small- and medium-sized enterprises, abbr.
27. Social media site enabling better networking
30. Sandra Bullock film, "The ___"
34. Word that comes before attack and security
36. ___ tag
38. Tokyo currency
39. Positive or negative item
41. Connection

(Answers on page 58)

CPE Quiz

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

Take the quiz online:

QUIZ #163

Based on Volume 4, 2015—Regulations & Compliance

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

TRUE OR FALSE

PATEL ARTICLE

1. There has been a noticeable jump in those organizations that attribute security incidents to current service providers and contractors and former partners.
2. Large-scale heists of consumer data were reported in South Korea, where 18 million payment card accounts were exposed in a security breach. In Verden, Germany, city officials announced the theft of 105 million email addresses, passwords and other information.
3. A vendor risk management program should obtain executive guidance from the compliance function to provide regulatory and other compliance requirements and the IT risk and control function to determine the risk and the risk level.

BANU AND CHITRA ARTICLE

4. The explosive increase of information online leads to some search problems—specifically, search engines usually return too few unrelated results on a given query.
5. The Deep Web Data Extraction (DWDE) framework seeks to provide accurate results to users based on their URL or domain search.
6. Precision is the number of false positives divided by the total number of positives, providing the percentage of true positives. Recall is the number of false positives divided by the number of true negatives and false positives, providing the percentage of positives that are found.
7. 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

SUBRAMANIAN ARTICLE

8. IoT comprises devices and sensors interacting and communicating with other machines, objects and environments.
9. There are two classes of devices based on the capability and processing power: 1) The smallest devices have 8-bit system-on-a-chip (SoC) controllers, 2) The top level of devices is based on Atheros or ARM chips with 32-bit architecture.
10. 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.
11. There are multiple technologies/protocols that the devices are connected to in the external world. Some of the most widely used include: TCP, IP, UDP, Telnet and FTP.
12. Physical security is no longer the first and foremost task for any information systems audit. Auditors need not concern themselves with mundane physical security of the systems configuration.
13. 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.

KHAN ARTICLE

14. Companies that operate in the EU are required to follow basic principles that are set forth by the EU's data protection commissioner.
15. The Data Protection Office (DPO) is currently the UK's independent body set up to uphold information rights.

ISACA Journal
CPE Quiz
Based on Volume 4, 2015—Regulations & Compliance

Quiz #163 Answer Form

(Please print or type)

Name _____

_____

Address_____

_____

_____

CISA, CISM, CGEIT or CRISC #_____

Quiz #163

True or False

PATEL ARTICLE

1._____

2._____

3._____

BANU AND CHITRA ARTICLE

4._____

5._____

6._____

7._____

SUBRAMANIAN ARTICLE

8._____

9._____

10._____

11._____

12._____

13._____

KHAN ARTICLE

14._____

15._____

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.

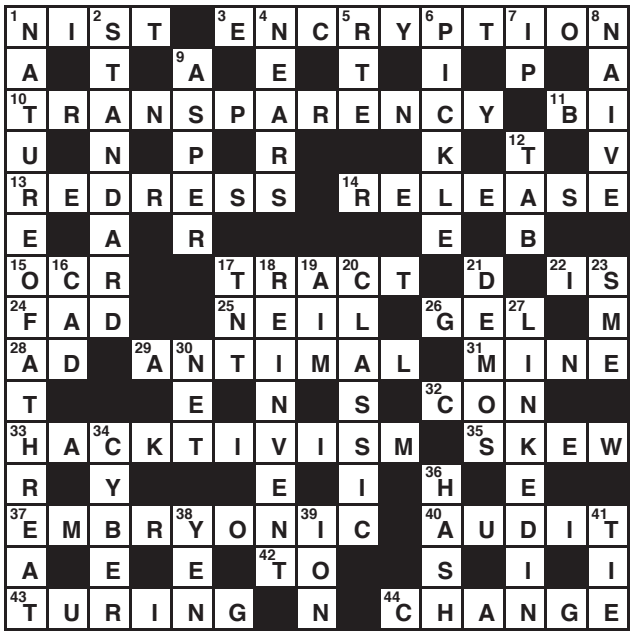
Outside the US, ISACA will pay the postage to return your graded quiz. You need only to include an envelope with your address.

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 guidance 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 judgment 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 became 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

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

COMING IN JANUARY 2016!

NEW! UPDATED CERTIFICATION PREPARATION MATERIALS

GET PREPPED FOR EXAM AND CAREER SUCCESS

CISA® Review Manual 26th Edition
Enjoy a complete refresh and updated content that aligns with the new job practice, which will be tested in early June 2016.

CISA® Review Questions, Answers & Explanations 11th Edition and Database
1,000 practice questions to hone your skills. All items have been reviewed and aligned to the new job practice and the 2015 supplement has been integrated.

CGEIT® Review Manual 7th Edition
The new layout features a switch from double-column to single-column layout for improved flow of content.

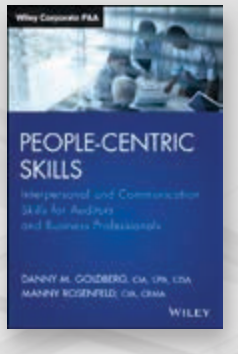
CISM® Review Questions, Answers & Explanations 8th Edition and Database
Features 950 Questions, with the integration of the 2014 and 2015 supplements. All explanations now follow the same A-D format.

CRISC™ Review Questions, Answers & Explanations 4th Edition and Database
Practice with 500 questions with the addition of the 2015 supplement.

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 BOOKS

People-Centric Skills: Interpersonal and Communication Skills for Auditors and Business Professionals

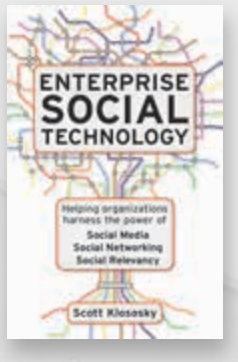


by Danny M. Goldberg and Manny Rosenfeld

Product Code: 1WPC
Member/Nonmember: $30.00/$40.00

A comprehensive guide to the "soft skills" that make technical professionals more effective. *People-Centric Skills* aim to improve all aspects of personal interactions, relationship development, and communication. These skills are as essential to success as are technical capabilities. This is the story of a leading internal audit department taking that next step to becoming a world-class audit organization in a fictional company. The foundation of that next step is developing their People-Centric Skills. The book demonstrates the impact that interpersonal and communication skills—whether good or bad—have on an auditor's effectiveness, job, and career.

Enterprise Social Technology: Helping Organizations Harness the power of Social Media, Social Networking, Social Relevancy



by Scott Klososky

Product Code: 1GLB
Member/Nonmember: $13.00/$23.00

Every leader has heard of the business benefits of social technology, yet many still struggle to understand how to get the most out of the technological tools at their disposal— asking questions like "What should I be doing on Facebook?" and "How can Twitter help my company?"

Enterprise Social Technology demystifies this much-hyped subject, and gives readers a levelheaded, growth-focused approach to how they can put all kinds of social technology—not just the big, well-known platforms—to work for their companies.

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 who invented the technology, 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.

The companion CD demonstrates available detection and prediction systems and presents a walkthrough on how to conduct a predictive analysis that highlights proactive security measures.

2 EASY WAYS TO ORDER:

1. Online—Access ISACA's bookstore online anytime 24/7 at ***www.isaca.org/bookstore***

2. Phone—Contact us by phone M–F between 8:00AM – 5:00PM Central Time (CT) at 847.660.5650

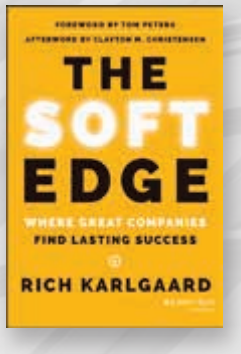
Empowering Green Initiatives with IT: A Strategy and Implementation Guide

by Carl H. Speshock

Product Code: 89WEG
Member/Nonmember:
$50.00/$60.00

Empowering Green Initiatives with IT provides organizations with strategy, planning, implementation and assessment guidance for their green initiatives. It discusses the many benefits of green initiatives with the assistance, integration and collaboration of the IT department and vendors, i.e., custom and vendor application development and reporting tools, green IT examples, and business intelligence dashboards that can perform analytical and predictive analysis of green-related business data.

The Soft Edge: Where Great Companies Find Lasting Success

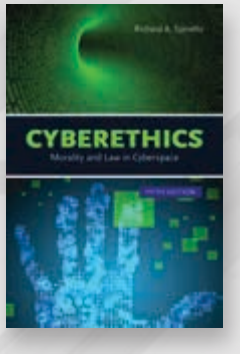


by Rich Karlgaard

Product Code: 119WSE
Member/Nonmember:
$18.00/$28.00

High performance has always required shrewd strategy and superb execution. These factors remain critical, especially given today's unprecedented business climate. But Rich Karlgaard—Forbes publisher, entrepreneur, investor, and board director—takes a surprising turn and argues that there is now a third element that's required for competitive advantage. It fosters innovation, it accelerates strategy and execution, and it cannot be copied or bought. It is found in a perhaps surprising place—your company's values.

Cyberethics—Morality and Law in Cyberspace, Fifth Edition



by Richard Spinello

Product Code: 5JBC
Member/Nonmember:
$107.00/$117.00

The Internet and widespread use of blogging, email, social media and e-commerce have foregrounded new, complex moral issues and dilemmas. Likewise, modern technologies and social networks have brought numerous challenges to legal systems, which have difficulty keeping up with borderless global information technologies.

The fully revised and updated Fifth Edition of *Cyberethics: Morality and Law in Cyberspace* offers an in-depth and comprehensive examination of the social costs and moral issues emerging from ever-expanding use of the Internet and new information technologies. Focusing heavily on content control, free speech, intellectual property, and security, *Cyberethics: Morality and Law in Cyberspace* provides legal and philosophical discussions of these critical issues.

FEATURED CATEGORY:

CYBER SECURITY

CSX™ CYBERSECURITY NEXUS

CSX Cybersecurity Fundamentals Study Guide

Product Code: CSXG1
Member/Nonmember: $45.00/$55.00

eBook Product Code: WCSXG1
Member/Nonmember: $45.00/$55.00

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

Implementing the NIST Cybersecurity Framework

Product Code: CSNIST
Member/Nonmember: $35.00/$60.00

eBook Product Code: WCSNIST
Member/Nonmember: Free/$60.00

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

Securing Mobile Devices

Product Code: CB5SMD1
Member/Nonmember: $35.00/$75.00

eBook Product Code: WCB5SMD1
Member/Nonmember: Free/$75.00

Securing Mobile Devices should be read in the context of the existing publications COBIT 5 Information Security, Business Model for Information Security (BMIS) and COBIT 5 itself.

This publication is intended for several audiences who use mobile devises directly or indirectly. These include end users, IT administrators, information security managers, service providers for mobile devices and IT auditors.

The main purpose of applying COBIT 5 to mobile device security is to establish a uniform management framework and to give guidance on planning, implementing and maintaining comprehensive security for mobile devices in the context of enterprises.

Transforming Cybersecurity

Product Code: CB5TC1
Member/Nonmember: $35.00/$60.00

eBook Product Code: WCB5TC1
Member/Nonmember: Free/$60.00

The cost and frequency of cyber security incidents are on the rise, is your enterprise keeping pace?

The numbers of threats, risk scenarios and vulnerabilities have grown exponentially. Cyber security has evolved as a new field of interest, gaining political and societal attention. Given this magnitude, the future tasks and responsibilities associated with cyber security will be essential to organizational survival and profitability.

This publication applies the COBIT 5 framework and its component publications to transforming cyber security in a systemic way.

2 EASY WAYS TO ORDER:

1. Online—Access ISACA's bookstore online anytime 24/7 at ***www.isaca.org/bookstore***

2. Phone—Contact us by phone M–F between 8:00AM – 5:00PM Central Time (CT) at 847.660.5650

CREATE VALUE FOR YOURSELF AND YOUR ENTERPRISE—START BY OBTAINING A CERTIFICATION FROM ISACA!

"EMPLOYERS SEE MY **ISACA CERTIFICATIONS**. THEY KNOW I WILL BE A **VALUABLE RESOURCE**."

— MARCUS CHAMBERS, CISM, CGEIT
CONSULTANT
LONDON, UNITED KINGDOM
ISACA MEMBER SINCE 2012

Becoming ISACA-certified showcases your knowledge and expertise. Give yourself an edge and gain the recognition you deserve with ISACA certifications—register for an upcoming exam soon!

Register at *www.isaca.org/2016exams-Jv6*

MORE EFFECTIVE

UPCOMING CERTIFICATION EXAM

11 June 2016

Registration Opens Soon!

Take the first step towards gaining the recognition you deserve with an ISACA certification!!

CISA® Certified Information Systems Auditor®

CISM® Certified Information Security Manager®

CGEIT® Certified in the Governance of Enterprise IT®

CRISC™ Certified in Risk and Information Systems Control™

ISACA®
Trust in, and value from, information systems

www.isaca.org/2016exams-Jv6


CSX
CYBERSECURITY NEXUS
ADVANCE YOUR CYBER SKILLS AND CAREER
Train for the new performance-based CSX Practitioner Certification. Acquire hands-on instruction in a cyber-lab environment—available through CSX certification training partners. Embrace skills aligned with globally recognized NIST Cyber Security Framework domains. Gain the certification that affirms your readiness to be an in-demand first responder in the global cyber security workforce.
Start now at: ***www.isaca.org/CSXP***
ISACA