Volume 3, 2016

ISACA Journal

Data Privacy

The Complexity Is in the Details

Encryption in the Hands of End Users

Protecting Information—Practical Strategies for CIOs and CISOs

www.isaca.org

ISACA®

Trust in, and value from, information systems

SHOWCASE WHAT SETS YOU APART, INSTANTLY—START BY REGISTERING FOR AN ISACA® CERTIFICATION EXAM TODAY!

"PROFESSIONALS NEED ISACA CERTIFICATIONS. WHEN YOU HAVE ONE, THE FUTURE IS VERY EXCITING."

— IVAN ANYA, CISA, CGEIT, CRISC
MANAGING DIRECTOR/CEO, BUSINESS INTELLIGENCE TECHNOLOGIES, LTD
LAGOS, NIGERIA
ISACA MEMBER SINCE 2013

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 today!

Register at *www.isaca.org/2016exams-Jv3*

ACCOMPLISH MORE

UPCOMING CERTIFICATION EXAM

10 September 2016*

Early Registration Deadline: 15 June 2016 | Final Registration Deadline: 22 July 2016

* CISA and CISM only

Take the first step towards gaining the recognition you deserve—register early for a September CISA® or CISM® exam today and save US $50!

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*

Save US $75 automatically when you register online!

www.isaca.org/2016exams-Jv3


HISCOX
business insurance®
“My business runs on big ideas. And a tiny budget.”
Get a fast, free quote at Hiscox.com/bigideas or call our licensed insurance agents at 866-507-0461 Mon–Fri, 8:00am–10:00pm ET. Your policy could start as low as $22.50/mo.
#encouragecourage.
© 2016 Hiscox Inc. All rights reserved.

ISACA Journal

FEATURES

PLUS

Online-exclusive Features

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

Online Features

The following is a sample of the upcoming features planned for May and June 2016.

Application of Situation Awareness in Incident Response
By Teju Oyewole, CISA, CISM, CRISC, COBIT Assessor, CISSP, CSOE, ISO 27001 LA, ITIL, MBCS, PMP

Auditing IS/IT Risk Management, Part 3
By Ed Gelbstein, Ph.D.

Security in an Age of Distraction
By Kerry A. Anderson, CISA, CISM, CGEIT, CRISC, CCSK, CFE, CISSP, CSSLP, ISSAP, ISSMP

Discuss topics in the ISACA Knowledge Center: *www.isaca.org/knowledgecenter*
Follow ISACA on Twitter: *http://twitter.com/isacanews*; Hashtag: #ISACA
Join ISACA LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

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

Read more from these Journal authors...

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

ISACA®
Trust in, and value from, information systems

3701 Algonquin Road,
Suite 1010
Rolling Meadows, Illinois
60008 USA
Telephone +1.847.253.1545
Fax +1.847.253.1443
www.isaca.org

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).

Specializations include Digital Forensics, Network Defense, and Health Care Security.

Along the way to your MS-IAS, earn up to 3 NSA focus area digital badges showcasing your mastery of skills in specific cybersecurity areas.

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.
HIGHER LEARNING COMMISSION: https://www.hlcommission.org, 800.621.7440
CAPELLA UNIVERSITY: Capella Tower, 225 South Sixth Street, Ninth Floor, Minneapolis MN 55402, 1.888.CAPELLA (227.3552)

Capella University

information security matters

Challengeable Truths

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 click on the Comments link to share your thoughts.

It seems to me that everything I knew in my youth to be true has been overturned, refuted, disavowed or revised.[1] I have taken some of this rather hard, especially the news about Santa Claus. On the other hand, the process of learning to see the world in a different way has been a constant source of intellectual excitement my entire life. In information security, I have seen a vast revolution, from the days of "It cannot be done" to today's "It must be done." My enthusiasm about our profession has not only not abated, but it has increased enormously in the years—still just a few years—that the reality of the threat of cyberattacks has been recognized.

There were certain tenets that I absorbed as I learned my craft:

- Information resources are to be used by those authorized to do so.
- Encryption is the most effective way to protect information from misuse.

- Authenticated identity is the basis for access control.

These and many other verities are part of the tribal wisdom of the InfoSec clan; who am I to challenge them? Yet, since governments, criminal gangs and terrorists have taken to attacking the security of information systems, targeting individuals, corporations and governments, I have been forced to consider revising, if not abandoning, all that I have known to be true.

Authorization, Encryption and Identity

Is authorized use an immutable principle? This is a subject of hot dispute between the EU and the US. The European Court of Justice ruled in October 2015 that information owned by citizens in the EU was not safe from the unauthorized, prying eyes of security organizations in the US, especially the US National Security Agency (NSA). While the NSA has not officially said so, it would seem that its leaders feel that safety from terrorism overrides concerns about authorized use. Without expressing my opinion on the matter, I believe that information security professionals need either to relinquish the principle that only authorized use is permissible or defend it. It is no longer an unchallengeable truth.[2]

Much the same can be said about encryption. Is it a truly effective means of security if the bad guys can use it to subvert security itself? Many police agencies think it is not, while many in the information security field reject the argument for providing "back doors" to encryption schemes. I happen to think that back doors make it easier for crooks to outsmart the cops, but still the point of view of the US Federal Bureau of Investigation (FBI) and the intelligence community cannot just be dismissed out of hand.[3]

Access rights and privileges are accorded to individuals, presumably based on their job requirements. Increasingly, cyberattacks are being perpetrated not by the intrusion of malware, but by theft and misuse of the credentials of authorized users, especially those with privileged access. As noted by the US Federal Financial Institutions

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.*

Examination Council, "These attacks include theft of users' credentials—such as passwords, user names and e-mail addresses—and other forms of identification that customers, employees and third parties use to authenticate themselves to systems. Attacks also include theft of system credentials such as certificates."[4] In short, authenticated identity cannot always be trusted.

No Cyberrisk Assessments

All the foregoing is leading up to my assault on two chapters from the Book of Conventional Wisdom, beginning with: Risk assessments should *not* be performed as a component of cybersecurity.

Oh, yes, there are other books that insist on risk assessments, not least of which is the US National Institute of Standards and Technology (NIST) Cybersecurity Framework.[5] All the techniques that are discussed for performing a risk assessment are based on probability and the assumption that risk equals probability multiplied by impact.[6] This simplistic formula has been totally demolished by Nassim Nicholas Taleb's masterful book, *The Black Swan: The Impact of the Highly Improbable*.[7]

The argument for probability breaks down because it is highly improbable that any given organization will be struck by a cyberattacker today. Even over the span of 365 days, the probability would still be minute, so the annualized risk using the traditional formula is extremely low. Therefore, for many organizations, the result of performing a risk assessment would be to conclude that cyberattacks are not a threat to them and so nothing need be done.[8]

The determinant is not the probability of the threat of a cyberattack, but its credibility. If a threat is credible, management must do something about it, even if it is only informed acceptance of risk. Sadly, cyberattacks are a credible threat to all organizations. In this era, no one in the management of even a moderately large enterprise can say, "Oh, sure, we might be attacked, but oh, heck, let's take our chances."[9]

So if a risk assessment must be performed, here is my suggested process for doing so:

A. Are cyberattacks a credible risk? (Yes/No)

B. If yes, implement sufficient security controls.

C. If no, repeat step A.

System Crashes

Another revision of belief brought about by the advent of cyberthreats is: Treat all system failures as though they were caused by cyberattacks.

As long as there has been information technology, there have been system crashes. I am sure that Alan Turing[10] hung his head over his vacuum tubes wondering what went wrong. But even in wartime, I doubt that Turing ever thought that the cause of the failure was enemy attack. Even today, when a system goes belly-up, almost everyone thinks "bug" before they say, "Oh my, this must be a cyberattack."

> **"Organizations should react as though they were attacked until this can be disproven."**

This sort of thinking must stop. Instead of assuming that something benign has happened until it can be proven that the cause of a failure was a cyberattack, organizations should react as though they were attacked until this can be disproven. Yes, there will be many false alarms, but these should not add greatly to the mean time to repair. Whatever the cause, technicians must locate the flaw that caused the failure, but if they do not bring a mind-set that anticipates malign causation, it is less likely that they will see it even if it is there. The amount of time that it takes to eliminate a cyberattack as a cause of downtime is minimal compared with the time it takes to reverse the damage an actual attack might cause. (Perhaps military forces do assume they are under attack when systems go down. If it is permitted, I would like to hear from someone who can describe military thinking in this regard.)

Imperfect Assumptions

In the past few years, I have been addressing various aspects of cyberrisk more than any other topic. In part, this is because it is the greatest challenge of our time in the information security domain. World peace and climate change are weightier challenges, but we security professionals do not have much to contribute to resolving those. Cybersecurity, as I have previously said in this space, is above and beyond information security.[11]

> **"We should be open to revising what we think is true."**

Targeted attacks by powerful enemies are forcing us to reconsider almost everything we thought we knew about protecting information resources. The whole point of what I have written here is that we should be open to revising what we think is true because the bad guys are so good at finding the flaws in our shared, but imperfect assumptions.

Enjoying this article?

- **Learn more about, discuss and collaborate on cybersecurity in the Knowledge Center.** *www.isaca.org/topic-cybersecurity*

Endnotes

1 I have paraphrased—or frankly, stolen—this line from the play *Da* by the Irish playwright Hugh Leonard.

2 Farrell, Harry; "Safe Harbor and the NSA," *Washington Monthly*, 17 December, 2015, *www.washingtonmonthly.com/ten-miles-square/2015/12/safe_harbor_and_the_nsa059016.php#*

3 Sanger, David E.; "New Technologies Give Government Ample Means to Track Suspects, Study Finds," *The New York Times*, 31 January 2016, *www.nytimes.com/2016/02/01/us/politics/new-technologies-give-government-ample-means-to-track-suspects-study-finds.html*

4 Department of the Treasury, "Cyber Attacks Compromising Credentials Joint Statement," Office of the Comptroller of the Currency, 30 March 2015, USA, *www.occ.treas.gov/news-issuances/bulletins/2015/bulletin-2015-19.html*

5 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, 12 February 2014, USA, p. 22-23, *www.nist.gov/cyberframework/*

6 Ross, S.; "Effective Techniques for Continuity Risk Management, Measurement," *TechTarget*, 2009, *http://searchcompliance.techtarget.com/tip/Effective-techniques-for-continuity-risk-management-measurement*

7 Taleb, N. N.; *The Black Swan: The Impact of the Highly Improbable*, Random House, USA, 2007

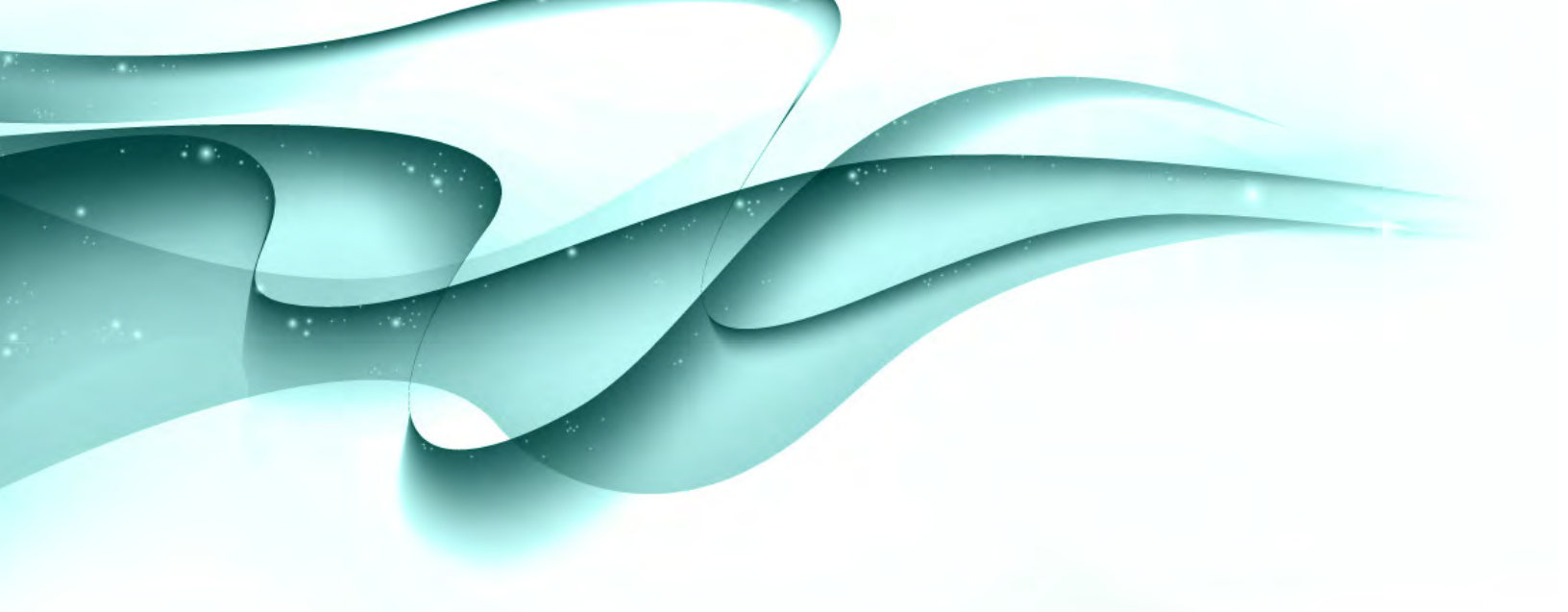
8 *Ibid.*, p. 40

9 Gustke, F.; "No Business Too Small to Be Hacked," *The New York Times*, 13 January 2016, *www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.html?_r=0*

10 Alan Turing, 1912-1954, was one of the 20th century's great geniuses. He conceptualized the computer as we know it in the 1930s and, during World War II, automated the breaking of the German Enigma code.

11 Ross, S.; "Frameworkers of the World, Unite, Part 2," *ISACA® Journal*, vol. 3, 2015, *www.isaca.org/Journal/archives/Pages/default.aspx*


CSX™
CYBERSECURITY NEXUS
INTRODUCING CSX PRACTITIONER BOOT CAMP
Accelerate your cyber security training with our new 5-day, intensive CSX Practitioner Boot Camp. Build and practice tougher technical skills and concepts in an adaptive, performance-based cyber laboratory environment. You'll come out knowing how to apply industry-leading methods within real-world scenarios — growing your technical ability and helping you advance your career in cyber.
Start now at: ***www.isaca.org/CSXPBootcampJournal***
ISACA®



Khawaja Faisal Javed, CISA, CRISC, BCMS LA, CBCP, CSA STAR, ECSA, ISMS LA, ITSM LA, ITIL v3, MCP
Is senior manager of operations and information and communications technology products with SGS Pakistan. With more than 23 years of experience, he has conducted more than 1,000 third-party certification audits/assessments of large enterprises in 40 countries worldwide against different international standards/frameworks as a lead auditor/trainer for ISO 27001, ISO 20000, ISO 22301, and other security and business continuity frameworks.

Javed was awarded a Showcase honoree award for Senior Info Security Professional, Asia Pacific in 2012 for his contribution to the field spanning more than two decades. Javed is also a member of the *ISACA Journal* review team, and a prominent and keynote speaker at international conferences and seminars.

Q: 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: In my opinion, the role of IS auditor has expanded as IS auditors are needed to be more involved in all the areas of the business, especially in project management. They should be involved in the projects to consider all the security aspects right from the start. However, the core roles of the IS auditor have not changed as such, since the IS auditor is expected to provide an objective insight into the risk and control processes in any organization. But with advancements in technologies and new, emerging threats, the IS auditor's auditing methodologies have to be adjusted, taking into account regulatory obligations, outsourcing, new exploitation techniques and more, as these pose serious challenges for this critical role. My humble advice for IS auditors is to keep abreast of these developments, update their knowledge on a constant basis and be flexible to adapt to the new techniques of auditing.

Q: How did you make the transition from IS auditor to your current role as senior operations manager of a certification body? What skills have helped you the most in this most recent role?

A: Well, in addition to my experience as an IS auditor, I am also an accredited lead auditor and trainer for many other management system standards, including Business Continuity Management System (BCMS), IT Service Management System (ITSMS), Quality Management System (QMS), Cloud Security Alliance (CSA) STAR, and EuroCloud Star (ECSA) Audit, with auditing experience of more than 20 years. As a senior manager of operations, my role has transformed from governance and compliance to the accreditation requirements as a technical reviewer/approver and mentor for other auditors in this field not only locally, but globally within my organization. My IS auditor experience has enabled me to understand and articulate the needs and expectations of an IS auditor, which has helped me assist and guide new IS auditors to increased levels of effectiveness.

Q: How do you see the roles of IS audit, governance and compliance changing in the long term?

A: I, personally, feel this role will have more responsibilities and is going to become more accountable at the same time. Due to the rise of security

the network

incidents/breaches and cybercrime, this role is going to be of high importance. As companies embrace new technologies, IS auditors must strive to understand how new technological developments and trends impact their organizations and internal process-level controls. They need to understand the exposure to cyberthreats as well as impacts on the viability of the business model. From a technology point of view, the IS auditor must recognize that social, mobile, big data and cloud transitioned from buzzwords to the new normal with associated threats. They also need to enhance their understanding of threats associated with the use of mobile commerce to the risk of destructive malware and advanced persistent threat (APT) attacks, since these will form the risk landscape of 2016 and beyond. Similarly, an effective IS audit risk assessment must address new or changing compliance requirements and see their impact on the business as a whole.

Q: How have the certifications you have attained advanced or enhanced your career? What certifications do you look for when recruiting new team members?

A: Certifications have definitely enhanced my career and provide the desired recognition at the global level. Having a certification shows a true commitment and dedication to your profession/occupation. In my organization, although all auditors have to be qualified based upon the Information Security Management System (ISMS) auditor criteria, the Certified Information Systems Auditor® (CISA®) certification is preferred for new hires, even if they are not yet ISMS-qualified (which, in most cases, is done on the job). We strongly encourage our ISMS auditors to acquire the CISA certification as soon as possible, and we completely fund the CISA training/exam process. Similarly, we also consider the Certified in Risk and Information Systems Control™ (CRISC™) certification as a preferred certification during the hiring process.

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

A: My biggest challenge has been the traveling involved in this job. I have traveled to 40 countries on five continents. Sometimes, due to the hectic schedule, I land back home on Saturdays and fly to the next destinations on Sundays. However, all that is done out of my passion for auditing and training. And I strongly believe that when you have motivation and passion, no hurdle or challenge can stop you.

1 What is the biggest security challenge that will be faced in 2016?

2016 will see a shift to focusing on the need to perform basic cyberhygiene practices.

2 What are your three goals for 2016?

- Volunteer more of my time locally to support my country's IS professionals
- Create awareness about cybersecurity risk, especially in the education sector
- Speak with as many industry leaders and professionals as I can

3 Who are you following on Twitter?

A few security gurus and business continuity magnets

4 How has social media impacted you professionally?

Professional outlets such as LinkedIn have helped me:

- Network with and meet my peers
- Get answers to many questions
- Share information on new threats/developments in this ever-changing professional field

5 What is your number-one piece of advice for other IS audit professionals?

Never stop upgrading and updating your knowledge and work to build a trusted partnership with all stakeholders involved.

6 What is your favorite benefit of your ISACA® membership?

Easy access to peers on different topics. When traveling, I get in touch with local ISACA chapters and meet with them or attend their networking events as a speaker.

7 What do you do when you are not at work?

- Spend time with my family and parents
- Watch Natural Geographic and Discovery channels
- Read articles and white papers on different topics (These days, my focus is on cloud security.)

Auditing IS/IT Risk Management, Part 2

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 click on the Comments link to share your thoughts.

Part 1 of this article described the commonalities, differences and possible overlaps between the IS/IT internal auditors and the IS/IT risk management functions managed by the chief information officer (CIO). It also suggested an audit universe for IS/IT risk management and introduced the case for collaboration between internal audit and enterprise risk management (ERM). **Figure 1** from part 1 is included here as a reminder.

The discussion that follows reflects the IS/IT auditor's perspective. Every topic can be subdivided into many more sections, but the intention of this column is not to provide a detailed manual (it would be a large book), just an overview.

Risk Controls

The international standard ISO 31000: 2009, *Risk management—Principles and guidelines*,[1] defines a control as "any measure or action that modifies risk. Controls include any policy, procedure, practice, process, technology, technique, method or device that modifies or manages risk."

An audit of IS/IT risk management could cover policies and procedures such as:

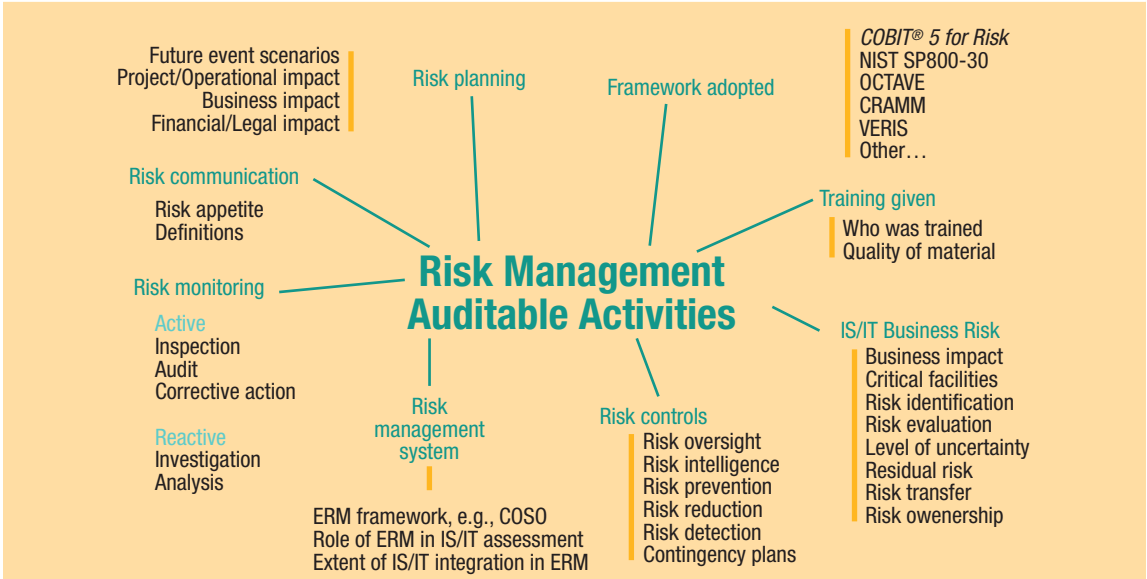
- **Risk oversight**—Audit committees and boards of management are ultimately accountable for risk oversight and should consider which individuals, teams or committees have the expertise to oversee particular risk. The auditor should seek evidence that this has been done or is being done and make observations as appropriate. If neither the audit committee nor the board are involved in the oversight of IS/IT-driven risk, a recommendation should reflect this fact.
- **Risk intelligence**—Many executives may believe that risk management requires special technical knowledge. The book *Risk Intelligence: Learning to Manage What We Don't Know*[2] disagrees and explains how four simple rules can improve risk analysis:
  1. Recognize which risk are learnable and reduce their uncertainty by discovering more about them.
  2. Identify risk you can learn about the fastest, particularly project risk.
  3. Take on risky projects one at a time. Learn about the risk underlying each before moving to the next.
  4. Build networks of business partners, suppliers and customers who can collectively manage new ventures' risk by playing distinct roles.

> **"The auditor should seek evidence that the appropriate activities are being done, to what extent and how well."**

In the specific case of IS/IT risk, risk intelligence should also include operational risk by establishing links with computer emergency response teams (CERT) and following media reports of current threats, e.g., botnets, malware, denial-of-service (DoS) attacks and industrial (and other) espionage. This sort of information does not mean the organization is no longer a target, but it does make the organization an "informed target."

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 '90s, 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.

Figure 1—Scope of Auditable IS/IT Risk Management Activities



Source: Ed Gelbstein. Reprinted with permission.

As always, the auditor should seek evidence that the appropriate activities are being done, to what extent and how well.

- **Risk prevention**—In the same way logic indicates that a house should not be built in a flood plain, there are many IS/IT risk that can be prevented through well-established principles such as need to know, least privilege and segregation of duties (SoD). These principles need no further discussion here except to say that there are many opportunities to strengthen controls around them, but this would more likely be done in an IS/IT audit rather than an IS/IT risk management audit.
- **Risk reduction**—Also referred to as risk mitigation, risk reduction is a set of activities undertaken to reduce the impact (financial, operational, reputational, etc.) of an event. Although this topic is too large to explore in detail in this article, the auditor should seek evidence that it has been addressed, for example, by assigning ownership to the risk as well as to the measures to be taken to reduce it, ideally incorporated in a risk register.
- **Risk detection**—Unlike detection risk in a financial audit where the auditor concludes that no material errors are present when, in fact, there are, in the context of IS/IT risk management, this reflects the capability to detect that an unauthorized third party is attempting to penetrate a network or system (or has already successfully done so) in order to affect its availability, confidentiality or integrity.

  Many vendors specialize in the field of security information and event management (SIEM). The auditor should explore to what extent such products are relevant to the organization and, if they are, whether they have been purchased or plans to do so exist.
- **Contingency plans**—The CIO should own and update incident response and disaster recovery plans, which must be updated and tested constantly given the rapid pace of change in technical architectures. The plans should also be tightly linked to the organization's business continuity plans.

Risk Management System

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control—*

Enjoying this article?

- Read ***Risk Scenarios Using COBIT 5 for Risk.*** *www.isaca.org/riskscenarios*
- **Learn more about, discuss and collaborate on audit tools and techniques and risk management in the Knowledge Center.** *www.isaca.org/knowledgecenter*

Integrated Framework,[3] published on 14 May 2013, places a stronger emphasis on the importance of IS/IT and includes other enhancements within its principles.

In May 2014, ISACA® published a white paper[4] highlighting areas of alignment and differences in the content of the COSO and COBIT® 5 frameworks and presenting the complementary and compatible nature of their guidance.

If the COSO framework has been adopted for ERM, the auditor should validate that the risk management of IS/IT is appropriately aligned with it to ensure integration between them.

Extent of IS/IT Risk Management Integration in ERM

Given the relatively short time since the 2013 publication of the COSO framework and COBIT 5, the transition toward a more integrated environment can be expected to take some time as ERM organizations, internal audit, and the CIO and chief information security officer (CISO) learn and start applying the changes.

Given that different disciplines (e.g., finance) may use different standards and even different definitions and metrics of impact and risk, lack of integration may create gaps in understanding, incompatible assessments and difficulties in integrating the results. The auditor should examine the extent of integration and make appropriate observations; if necessary, the auditor may wish to recommend having a single integrated and prioritized source of risk information for the whole of the business.

Risk Monitoring

Risk monitoring can be active and reactive:

- **Active**—This should include risk intelligence, as already discussed, and inspection (or self-assessment), IS/IT audits and whatever corrective actions have been identified.
- **Reactive**—This consists of after-the-event actions to understand what happened and how, with the objective of learning about the vulnerabilities in people, processes and technology that caused it and drawing lessons from the incident in the hopes of preventing a repeat event.

  These actions include analysis and investigation and, while the outcome may cause discomfort, it is better to know. One little-publicized example was the way in which the Stuxnet malware was introduced into the high-security uranium enrichment facility at Natanz, Iran, and then into computers that were not connected to any outside network. In truth, the process involved people and a USB flash memory drive—an approach that was considered so unlikely that there may not have been a risk scenario (discussed in part 3 of this series of articles) seriously considered.

Risk Communication

Risk appetite is a core consideration in an ERM approach.

It can be defined as "the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives."[5] Each organization needs to define it for different risk, relate it to the organization's sector of activity and culture, and express it in appropriate units (financial for impact, in minutes [or hours] for systems availability, etc.). While risk appetite means different things to

different people, there is a consensus that a properly communicated, relevant risk appetite statement can help organizations achieve their goals and sustain their operations. This is hard to do, but without it, it is not possible to manage risk in any meaningful form.

The auditor should examine risk appetite statements relating to IS/IT for completeness and relevance and verify the extent of contribution and agreement from senior management.

Definitions

According to ISO 31000, risk is the "effect of uncertainty on objectives," and an effect is a positive or negative deviation from what is expected. The key word here is "uncertainty," as things are more than likely not going to go according to plan.

Many professions and activities have their own set of definitions of risk, and this can lead to misunderstandings, if not confusion. For example, a dialogue on risk between a medical surgeon and an investment banker, albeit unlikely, should be a facile illustration of mutual incomprehension.

The auditor should explore the extent to which the definition of risk used by IS/IT professionals is understood by the ERM team and other functions of the business.

Preliminary Conclusions

This article should not be seen as the end of the story, only its beginning. As the role of risk management increases in business importance there will be many more areas for the internal audit function to consider, such as the risk associated with data being discarded/destroyed, the use of encryption, single points of failure, and external suppliers and vendors. Part 3 of this article will discuss risk scenario planning.

Endnotes

1 International Organization for Standardization, ISO 31000:2009, *Risk management—Principles and guidelines*, *www.iso.org/iso/home/standards/iso31000.htm*

2 Apgar, David; *Risk Intelligence: Learning to Manage What We Don't Know*, Harvard Business School Press, USA, 2006

3 Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control—Integrated Framework*, 2013, *www.coso.org*

4 ISACA, *Relating the COSO Internal Control—Integrated Framework and COBIT*, USA, 2014, *www.isaca.org/coso-and-cobit.*

5 Rittenberg, L.; F. Martens; "Understanding and Communicating Risk Appetite," COSO, 2012, *www.coso.org*

Moral Dialogue on the IT-leveraged Economy

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 click on the Comments link to share your thoughts.

We face moral questions in four "spheres," or roles: as a person, as an economic agent, as a company leader and beyond a firm's boundaries.[1] Although the world of work has existed for a long period of time, perhaps since the beginning of human existence, the idea of a business as a separate sphere was crystallized only as the work roles became more apparent and structured, as in the agricultural society, then in the industrial age and, more recently, in the knowledge economy. Moral dialogue on the role of a firm within and beyond its boundaries is more recent than dialogue on the role of a person in private life. As the economy keeps evolving, nuances, if not the character of ethical dilemma, take on new colors. The purpose of this column is to explore moral questions in the new, technology-dominant economy.

In dealing with the ethics of business firms, we are often guided by Freeman's separation thesis,[2] which says that people tend to treat an issue as a business decision distinctly separate from the same issue as a moral decision. Perhaps the comfort level of the decision maker is high when the two are dealt with separately. However, in as much as this makes the exercise less messy, the discreteness both simplifies and marginalizes the uncertainty and fuzziness of ethics.[3] A natural order of treatment here should be a joint, concurrent, integrated debate on both the business and ethical issues.

Perhaps it was easier in the distant past to separate a business decision from its ethical side. But this is not feasible in most situations anymore. A decision has ethical consequences and, in turn, dealing with such ethical consequences could result in a reconsideration of the business decision. As if this is not complicated enough, the decision scenario becomes even more challenging as we bring the societal implications into consideration. If a hypothetical organization were an entity isolated from society, ethical considerations would probably have a well-defined boundary. However, the inevitable presence of the society in the background weighs in, often heavily, on the moral grounds. In the past, a business's impact on society was probably not as vivid, but in recent decades, the recognition that the ethics of a business entity could widely impact the society is evident. Businesses should—and most of them probably do—project ethical consciousness to bring society into its consequential decisions. From environmental pollution to lead-contaminated potable water,[4] an economic entity can no longer disregard the societal threads in its moral fabric.

Business, Society and Technology

In the distant past, technology was often visualized in the form of an artifact, an idea, a product or a process. The invention of the wheel or the printing press was likely driven in the absence of an explicit consideration of its moral consequences to society. There was the separation of technology from its potential use in the consideration of ethics. Even the economywide considerations of ethical consequences of an artifact were neutral or socially controlled. From this perspective, one tends to think of technology or its artifact as value neutral. For example, one might argue that a printing press is value neutral and its value in use depends on its user.

In reality, however, technological innovations influence society and often shape the behavior of humanity over time. Thus, "the assumption that artifacts [of technology] are separate and either outside the influence of humans or completely within the purview of human wishes misses the intersection of society and technology where the two are not separate."[5] In fact, technological innovations of recent decades have been heavily value laden for the society and, as a consequence, the intersection of society and technology has become a critical component of ethical analysis. The most graphic example of this is the scrimmage between privacy rights and the desire to bring people together on a given platform such as Facebook.

The interconnectedness of society and technology is often incubated in businesses, where research and development of technology—especially applied research—produces avenues for future cash flows.

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 motivations for enterprises such as Facebook, Twitter and LinkedIn are sourced in specific business applications of technology, although the broader technology may have its birthplace somewhere else (e.g., Stanford University [California, USA] or the Massachusetts Institute of Technology [MIT], USA). One could presume that it is the business that should weigh in on the powers of the technology (it is "playing with") on society as a whole as far into the future as possible. In this manner, the triad of business, society and technology is often driven by what a business or an industry does in the technology space.

Putting the corporate world in charge of assessing ethical dilemmas is not without risk. Ogburn's cultural lag thesis helps explain the puzzle. According to Ogburn, material culture advances more rapidly than nonmaterial culture.[6] Advances in technology belong to the material culture, while the technology's ethical consequences reside in the nonmaterial culture. So the application of technology through products happens much faster in the material culture than the moral dialogue on the use of technology in the nonmaterial culture (**figure 1**). In an examination of whether technology has introduced new ethical problems, Marshall asserts, and I agree, that the cultural lag now appears to have greatly accelerated.[7]

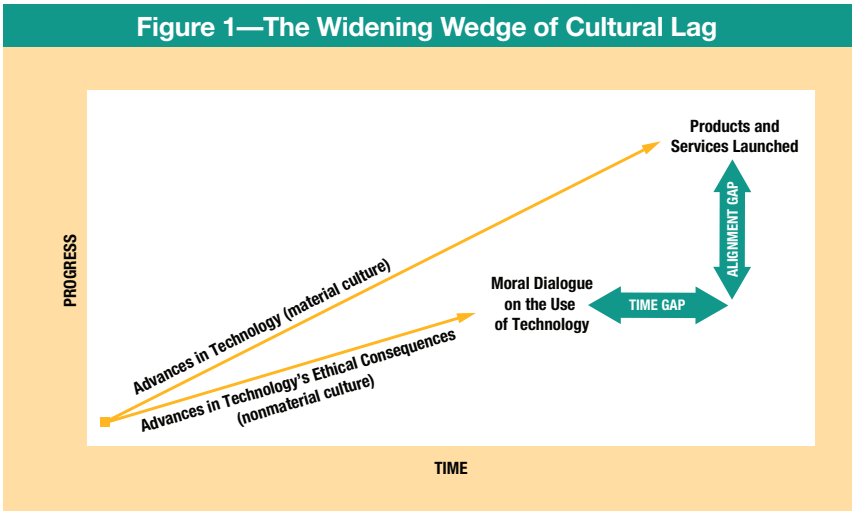
Marshall puts forth three reasons why ethical systems lag behind technology development. The material world moves fast for these reasons:

1. Concentration of equipment, resources and information on the single-minded research and development efficiency (for the sake of economic goals)
2. The race to seek patents and get products to markets first
3. The discovery and application of natural laws of the physical world, which can be engineered in controlled, experimental environments (devoid of moral questions)

And the development of ethical systems is slower because:

1. The development of ethical guidelines does not take place in a controlled environment.
2. There may not be any direct financial rewards for the introduction of a dominant ethical perspective.

Figure 1—The Widening Wedge of Cultural Lag



Source: Vasant Raval. Reprinted with permission.

3. The social forces that an ethical system would seek to influence are not as controllable as physical aspects of the world.[8]

A balanced view would also suggest that corporate leaders cannot necessarily anticipate well in advance the societal influence and consequent moral questions related to the technology "genie" they let out of the bottle at a rapid pace. Compounding the issue is that the problems surrounding the use—or misuse—of technology lie in a lack of understanding of technology's inherently social and moral dimensions.[9]

Rethinking the Moral Dilemma

Clearly, there are technology forces afoot that make technology more than just a sleeping partner on the ethics landscape. Here is how this is happening. While some innovations in information technology come from software and hardware, the most visible contributor these days is electronic communication. Ever since the launch of the Internet, much has changed because of the innumerable options to do things remotely. This includes innovations in the categories of offshore outsourcing, cloud computing, social networking, mobile devices, near-field communications, and the Internet of Things. Global connectivity and access from anywhere, anytime provide the high-octane energy to not just surpass brick-and-mortar businesses, but to perform even more impressively. Online banks with no physical

branch presence; Uberization; gaming and animation; YouTube, Whatsapp and other friends-and-family networks; supply chains reshaped by the drone delivery systems; and driverless cars—these are just a few examples of how the business models are being turned upside down. The material world dominates the scene and imposes a sense of urgency.

Everything that is hung on the Internet—a loosely connected network of networks—brings the virtual presence of information resources, global access, massive scaling, real-time transaction capabilities, and huge amounts of structured and unstructured data. While the opportunities are massive, so are the ethical challenges.

Who Is in Charge?

So, the loaded questions are these: Who is in charge? Who will guard and guide the moral frontiers? Or, can we expect the moral issues to get sorted out organically over time? Looking at lawmakers and regulators for proactive solutions seems somewhat fruitless for two reasons. Like corporate leaders, they also do not know what will emerge around the corner. Additionally, law making—even translating current law to include technology in its fold—has been difficult and slow. The regulators are struggling to put their arms around drone use while the industry is chugging along with its experiments to get ready for tomorrow.

Another viable candidate would be the corporate leaders, to the extent they can anticipate and are willing take on the nonmaterial culture relevant to their mission. But their firm's economic goals may keep them from giving priority to expanding into the nonmaterial consequences of their actions beyond the threshold requirements of the current laws and regulations. And yet, there are hopeful signs; for example, it is reported that Facebook has adopted the practice of deleting those accounts suspected in a crime so that further damage to society may not occur. For research use, Yahoo has committed to the release of the largest-ever cache of data of some 20 million anonymous users so that we can learn how large numbers of people behave online.[10] And Alphabet will expand how it applies Europe's right-to-be-forgotten for search engines to comply with the stricter privacy requirements of the European Union (EU).[11]

The picture is even more complex when you consider the fact that, as illustrated by Sony's case, the corporate existence can be closely connected to cyberwars among nations (North Korea and the US in Sony's case). The ownership of a nonmaterial cultural issue thus becomes cloudy. Should the US government act on Sony's hack, or should Sony autonomously respond to the compromise inflicted upon it by a foreign government? On worldwide societal issues of ethics, drawing the boundary around a firm, a community, a nation or even a continent fails to yield any meaningful control. The case of net neutrality illustrates this point well. Net neutrality refers to equal access rights to all users of the Internet, regardless of the user, the access mode or nature of use. The idea behind net neutrality is similar to the expectations of common carriers, such as the utilities that control infrastructures. The only, and yet the most impactful, difference is that net neutrality refers to the virtual world that lives on the Internet and affects almost all human beings and organizations around the globe.

In the past, the moral dialogue on the physical equivalent of net neutrality was vividly present in the regulation of utilities. Marshall referred to the overarching issue as control of essential facilities. He hinted that technological advances may "affect the meaning of dominance and the role of free market forces," and questioned if there is a point at which dominance of a market becomes so much a part of our essential culture that it would shift the status of a pervasive resource to that of a public trust.[12] It appears that only the government could control issues of net neutrality through regulation; however, there are too many governments around the globe to control a seamless global resource and differences in their attitudes and behavior are problematic. The Facebook initiative to provide access to basic Internet resources (through its Free Basic app) to the disadvantaged has been rejected by the Indian courts suggesting the initiative compromises net neutrality.[13] So the jury is out on how we as a one-world community will deal with net neutrality issues. If this is any indication of what lies in the future, we are destined to face greater challenges and difficult, almost unsolvable, ethical puzzles.

Endnotes

1 Badaracco, J. L., Jr.; "Business Ethics: Four Spheres of Executive Responsibility," *California Management Review*, Spring 1992, p. 64-79
2 Freeman, R. D. E.; "The Politics of Stakeholder Theory," *Business Ethics Quarterly,* vol. 4, 1994, p. 409-422
3 Martin, K. E.; R. E. Freeman; "The Separation of Technology and Ethics in Business Ethics," *Journal of Business Ethics,* vol. 53, 2004, p. 353-364
4 The city of Flint, Michigan, USA, is currently enmeshed in this dilemma, which borders on a major crisis.
5 *Op cit*, Martin and Freeman, p. 354
6 Ogburn, W. F.; *Social Change with Regard to Cultural and Original Nature*, B. W. Huebsch, Inc, USA, 1966
7 Marshall, K. P.; "Has Technology Introduced New Ethical Problems?," *Journal of Business Ethics,* vol. 19, 1999, p. 81-90
8 *Ibid*, p. 84
9 Buchholz, R. A.; S. B. Rosenthal, "Technology and Business: Rethinking the Moral Dilemma," *Journal of Business Ethics,* vol. 41, p. 45-50
10 Dwoskin, E.; "Yahoo Releases Largest-ever Cache of Internet Data," *The Wall Street Journal*, 14 January 2016, *www.wsj.com/articles/yahoo-releases-largest-ever-cache-of-internet-data-1452819412*
11 Barr, A.; S. Schechner; "Google Bends to European Pressure on Right to be Forgotten Rule," *The Wall Street Journal*, 11 February 2016, *www.wsj.com/articles/google-bends-to-european-pressure-on-right-to-be-forgotten-rule-1455231966*
12 *Op cit*, Marshall, p. 88.
13 Soni, A.; "India Deals Blow to Facebook in People-powered 'Net Neutrality' Row," *The Guardian*, 8 February 2016, *www.theguardian.com/technology/2016/feb/08/india-facebook-free-basics-net-neutrality-row*

book review

Securing the Virtual Environment

How to Defend the Enterprise Against Attack

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 click on the Comments link to share your thoughts.

More than 60 percent of businesses utilize the cloud for performing IT-related operations, and over the next five years there is expected growth of 44 percent annually for public cloud use versus 8.9 percent growth for on-premises computing.[1] *Securing the Virtual Environment: How to Defend the Enterprise Against Attack* explains that some advantages of virtualization include increased IT agility, greater hardware utilization, improved disaster recovery abilities and better business continuity capabilities.

By Davi Ottenheimer and Matthew Wallace

However, there is security risk, which is likely to contribute to an increasingly risky environment associated with cloud use in the future. In fact, ransomware attacks soared by 113 percent in 2014,[2] and statistics show that no industry is immune to cybercrimes.[3] Even companies that are not yet using the cloud may be doing so in some form soon. Based on the increased amount of cyberattack activity, those who move to the cloud should first have a firm understanding of security and compliance in virtual and cloud computing environments. *Securing the Virtual Environment: How to Defend the Enterprise Against Attack* can help enterprises begin to understand the challenges associated with the use of new virtual technologies.

This book is aimed at anyone with an interest in security and compliance in virtualized and cloud environments—appealing to both technical and nontechnical readers. For the nontechnical, there is information on the risk and rewards of the virtualized and cloud environments and examples of these are provided throughout the book. The book does not delve deeply into any particular cloud platform, but provides good coverage of the basics of virtualized environments, which makes it an excellent primer on the subject. For technical readers, the authors suggest beginning with the appendix and the included DVD to find instructions on how to build a virtual attack lab for use in the hands-on sections of the book. The authors aim to allow the reader to see that technology can be beneficial—not just for the advantages it brings, but also to empower organizations with tools to better manage their security environment.

One of the most useful aspects of this book is the inclusion of security basics that made what could be a complex topic (attacks in a virtual infrastructure environment) much more understandable. The book leads the reader through that journey, starting with an introduction on the basics of the cloud and security and then addressing attacks, risk, favored attack methods and virtualization compliance. Since virtualization and the cloud change so rapidly, the book also provides suggestions on web resources that can help enterprises navigate through securing their virtual environment. Through this book, readers not only get an education in cloud and virtualization, but gain a better understanding of how this technology has been implemented in their enterprise environment.

Endnotes

1 Woods, J.; "20 Cloud Computing Statistics Every CIO Should Know," SiliconANGLE, 27 January 2014, *http://siliconangle.com/blog/2014/01/27/20-cloud-computing-statistics-tc0114/*
2 Symantec, 2015 *Internet Security Threat Report, Volume 20*, 2015, *www.symantec.com/security_response/publications/threatreport.jsp*
3 Kassner, M,; "New Ponemon Report Shows Cybercrime Is on the Rise," *TechRepublic*, 3 November 2014, *www.techrepublic.com/article/new-ponemon-report-shows-cybercrime-is-on-the-rise/*

Editor's Note

Securing the Virtual Environment: How to Defend the Enterprise Against Attack is available from the ISACA® Bookstore. For information, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

Reviewed by A. Krista Kivisild, CISA, CA, CPA
Who has had a diverse career in audit while working in government, private companies and public organizations. She has served as a volunteer instructor, training not-for-profit boards on board governance concepts; has worked with the Alberta (Canada) Government Board Development Program; has served as the membership director and CISA® director for the ISACA® Winnipeg (Manitoba, Canada) Chapter; and is a member of the ISACA Publications Subcommittee.

The Complexity Is in the Details

New EU Data Protection Law Promises User Control

feature

Также на русском
www.isaca.org/currentissue

Four years after its introduction, the European Commission has recently come to agreement on the General Data Protection Regulation (GDPR) as organizations around the globe await the details, which should be released soon.

Often described as "fit for a digital age" by its supporters in Brussels, Belgium, the legislation aims to put users in control of their data and harmonize the rules under which private data may be obtained or retained across the 28-nation bloc. The GDPR updates the antiquated 1995 privacy regulation, drafted three years before the founding of Google. In an effort to keep up with technology and address privacy issues important to the European community, the European Parliament came to agreement on the European Union (EU) data protection law in December 2015, with details to be released in the near future and to become enforceable in 2018.

Because this new legislation declares itself applicable to any organization that makes its goods or services available to any part of the EU, it takes little imagination to understand its reach and scope. GDPR is not merely a new version of the 1995 legislation, but a revolutionary new rule set that organizations will need to quickly understand, adopt and comply with or face significant financial consequences.

The fundamental aim of the new regulation is to put users in control of what is stored about them online. "The new rules will give users back the right to decide on their own private data," says Parliament's lead member of European Parliament (MEP), Jan Philipp Albrecht.[1] One prominent feature of the new legislation extends the popular right to be forgotten, a rule active in the EU since 2006, which allows users to demand deletion of their photographs, videos or personal information from any Internet records that allow them to be found by search engines. The right was initially implemented for search engines, but it has now been extended to all web services, including social media sites such as Facebook.

The right to know you have been hacked is a popular component of the GDPR and requires organizations to report to a central authority within 72 hours any data breaches that pose a risk to data owners. Users subject to high-risk breaches are also required to be notified as soon as possible, although the ambiguity of this language causes some to be skeptical of the directive's enforceability.

Critics of the new data-protection regulation take aim at a number of its clauses. One of the most controversial aspects is in the punishment for noncompliance—organizations face fines of up to 4 percent of their annual global revenue for not complying with any part of the GDPR. "Such high sanctions dis-incentivize business and investment," says Intel's global privacy officer David Hoffman.[2] Skeptics are already calling the regulation the latest Silicon Valley shakedown and say it is escalating conflict with technology giants such as Google, Facebook and Microsoft.

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 click on the Comments link to share your thoughts.

Michael Vanderpool, CISA, CISSP
Is an IT auditor with Credit Suisse, based in the city of Wroclaw, Poland. His more than 12 years in information technology experience has been mostly with information security, risk and compliance. With a background in the technology and financial sectors, Vanderpool has performed a variety of IT risk assessments, audits and control reviews for international corporations and banks while utilizing international frameworks such as COBIT®, COSO and ISO 27001. Prior to joining Credit Suisse, Vanderpool worked for UBS and IBM.

Ambiguity in some of the guidelines and language in the GDPR is also a cause for concern. One example is with the requirement that some organizations hire a data protection officer. According to the regulation, small or medium-sized organizations are exempt from the obligation to appoint a data protection officer insofar as data processing is not their core business activity. Under this definition, would companies that conduct background checks be exempt? Such organizations are often targeted by data thieves, and large-scale breaches at this kind of company are not uncommon, but if such organizations define "personnel management" or "recruitment processing" as their core business, they can claim exemption even though they host extensive valuable personal information, sometimes permanently.

"Legal uncertainty and big fines are a toxic cocktail," notes Interactive Advertising Bureau European board member Allan Sorensen.[3] The large, globally calculated penalties for regulation infractions, combined with the (at times) vague wording, cause some to wonder if the regulation is designed more for the EU to make another cash-grab from Google than to protect user data. In response, GDPR sponsor Jan Philipp Albrecht claims, "The only ones who will profit from this law being postponed again and again will be the big data companies from Silicon Valley."

> **"There are clearly many stakeholders caught in the crosshairs of the GDPR."**

Medical research organizations have come out against the regulation, claiming it would slow or even halt their ongoing data-driven research efforts. More than 50 patent organizations and medical research charities have written to MEPs about concerns with overly restrictive data laws. Some organizations claim that the changes to the law may be unworkable at best and illegal at worst, especially for large-scale projects.[4]

Although many medical researchers are content with the latest changes to the regulation's wording, there are clearly many stakeholders caught in the crosshairs of the GDPR. Even organizations making early attempts at compliance with the new rules have their hands full. Each of the 28 bloc nations will interpret the EU regulation independently, and in some cases there is discretionary leeway in defining actual laws. For instance, the minimum age a child can use social networking sites without a parent's express approval must fall between ages 13 and 16, but the specific age can be defined by each country.

The early stated goal of creating a "one-stop shop," i.e., a single point of contact for any complaints about a company, suggests that the offending company's main point of presence in the EU is the country's regulator who would handle the complaint. Due to voiced concerns, however, it is now permitted that any nation's regulator can file a complaint with the main point of presence's regulator, depending on where the complainant resides and where the complaint is filed. As Johannes Caspar, the head of Hamburg's data protection authority in Germany says, "The mechanism laid down in the data-protection regulation establishes a hyperbureaucratic procedure that will lead to more complexity and longer procedures."[5]

Access to one's own data allows users to see exactly which data are being retained by a web site and how they are being used. The right to data portability (which many critics label a boondoggle) allows users to download their personal data and preferences for import and use on another web site. Data portability has been controversial and many claim it neither facilitates data protection nor belongs in the regulation. Its references have already been minimized in the most recent regulation summaries, and many expect it to be left out of the final draft altogether. One scenario illustrating this requirement would involve customers of a shopping web site to be able to download their shopping preferences and upload them to a competitor site. Depending on each shopping web site's product

categories, hierarchies and naming taxonomy, this process, which might sound simple in the halls of Parliament, creates real-world hurdles for technology architects, and critics claim it adds no value to the stated fundamental goal of the regulation to protect user data.

As an illustration of the data portability requirement, imagine owning Pizza Company A, which takes orders online. Customers have an online profile, which contains their address, phone number and order history to make new delivery orders fast and efficient. Customer John Smith calls and demands to be provided with his profile and history so that he can order from Pizza Company B. The new regulations require that the information be sent to him. Does this new process add value to Pizza Company A? Does it serve to protect John Smith's data? And unless Pizza Company B's pizza offerings are exactly the same as Pizza Company A's, the history will serve little purpose to Pizza Company B when it takes his first order. The process does, however, increase John Smith's data exposure (through additional email transmissions) and places a new burden on Pizza Company A, which, according to the new regulations, is required to provide data provision service to (nonrevenue-generating) ex-customers.

The challenge in complying with European Commission directives is well known to technology companies. Since Article 17 of the Data Protection Regulation's release in 2012, technology companies have struggled to maintain compliance with the right-to-be forgotten requirement while still providing their users a positive online experience. For example, eBay has struggled to implement the strict requirement to immediately delete users' data, made exceptionally difficult because of the number of databases in which that user data resides.

Also in the crosshairs of the GDPR is the practice of profiling users, a widespread practice online that allows web sites to gather and categorize information about their visitors, allowing them to tailor the web site experience and present more relevant ads. Beyond just use for advertising though, technology has been used by insurance companies to monitor and reward safe driving behavior and by social media sites to recognize and tag photographs containing the faces of their users. Such implementations will now require consent for each use, and all companies will now be required to disclose to each web site visitor:

- Why users are being profiled
- Into what categories (buckets) they are being sorted
- Who can access the data
- The logic involved in these determinations
- The consequences of such processing

While some of these new requirements are already commonly seen in such disclaimers as, "We use your information to enhance your shopping experience," the required disclosure of the actual logical algorithm used is particularly groundbreaking. As Alvaro Bedoya, executive director of the Center on Privacy and Technology at Georgetown University (Washington DC, USA) Law Center, says, "Right now, so much of our online lives are determined by algorithms that are totally opaque. The right to access the 'logic' behind data processing could be a significant step forward in opening that black box." Technology companies such as Google often view their algorithms as their most valuable trade secrets. The disclosure of specific logical formulas is viewed by many as a thinly veiled attempt by the European Commission to see behind the curtains of how these companies operate.

The territorial scope of the GDPR remains one of its most controversial aspects. With its stated reach being any organization that makes its goods or services available to any subject in the EU, the European Union could soon be regulating the Internet. Popular web sites such as Google and Facebook will either need to offer a different program to European customers or evolve their global services to become compliant. And with just one infraction of the rules resulting in a potential

Enjoying this article?

- Read ***Keeping a Lock on Privacy: How Enterprises Are Managing Their Privacy Function.*** *www.isaca.org/2015-privacysurvey-*
- **Learn more about, discuss and collaborate on privacy/data protection in the Knowledge Center.** *www.isaca.org/topic-privacy-data-protection*

4 percent revenue fine (for Google this is currently US $3 billion), companies face some difficult decisions in the coming months.

With its stated objectives being "to strengthen privacy rights and boost Europe's digital economy," many critics claim the regulation misses the mark entirely. While there are some components that effectively address privacy concerns, other aspects are extremely expensive and difficult to comply with, leaving technology companies with difficult decisions to make in the coming months when it comes to serving their European customers. Even those who decide to alter their services in order to comply with the new regulation face some daunting challenges in the next 24 months. "The scale and breadth of the EU's changes to privacy rules will deliver unprecedented challenges for business and every entity that holds or uses European personal data both inside and outside the EU," explains Stewart Room, head of data privacy at PwC.[6] "Most companies will be shocked at the scale of the new rules and the work that needs to be done before the laws take effect in two years—it is not much time for the magnitude of the internal changes that will be required."

As is common with European Commission rulings, the regulation will now face additional scrutiny and transposition when the 28 bloc nations absorb the individual requirements into their national laws in the coming months. While the GDPR is scheduled to take effect in 2018, it is not difficult to imagine even further delays if individual member countries cannot reach internal agreement on the required implementation and enforcement of the ruling.

It will be particularly interesting to see the Irish reception of the regulation, as Ireland is the European home to many foreign technology companies. A 2013 criticism of the regulation by the Irish presidency centered on the lack of a risk-based approach in drafting the regulation. Where actual risk is found to be lower, the Irish wanted the amount of regulation to be minimized. The presidency also voiced concern over the "needs of micro, small and medium-sized enterprises (SMEs)."[7]

So, as the 28 bloc nations receive the details of the draft in the coming weeks, no one should be surprised to see further debate about the GDPR, which was initially proposed in 2012. It all boils down to the details, and details have been known to hide unwelcome surprises.

Endnotes

1 European Parliament News, "New EU Rules on Data Protection Put the Citizen Back in the Driving Seat," press release, 17 December 2015, *www.europarl.europa.eu/news/en/news-room/20151217IPR08112/New-EU-rules-on-data-protection-put-the-citizen-back-in-the-driving-seat*

2 Dow Jones Business News, "EU Privacy Law Has Broad Implications," Nasdaq, 17 December 2015, *www.nasdaq.com/article/eu-privacy-law-has-broad-implications-20151217-00441*

3 Dwoskin, E.; "EU Data-Privacy Law Raises Daunting Prospects for U.S. Companies," *The Wall Street Journal*, 16 December 2015, *www.wsj.com/articles/eu-data-privacy-law-raises-daunting-prospects-for-u-s-companies-1450306033*

4 European Parliament, debate transcript, Strasbourg, France, 11 March 2014, *www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20140311&secondRef=ITEM-013&language=EN&ring=A7-2013-0402*

5 Fioretti, J.; "EU Data Protection Reform May Promise More Than it Delivers," *Reuters*, 5 January 2016, *www.reuters.com/article/us-eu-dataprotection-idUSKBN0U41CQ20160105*

6 BBC News, "EU Data Laws Threaten Huge Fines," 16 December 2015, *www.bbc.com/news/technology-35110909*

7 Hunton & Williams, "Irish Presidency Reports on Progress of the Proposed EU Regulation," Huntonprivacyblog.com, 26 March 2013, https://*www.huntonprivacyblog.com/2013/03/26/irish-presidency-reports-on-progress-of-the-proposed-eu-regulation/*

Encryption in the Hands of End Users

Также на русском
www.isaca.org/currentissue

As part of a defense-in-depth strategy, many organizations are expanding their usage of encryption. While encryption can provide protection from unauthorized access and reduce the likelihood of data theft, it is very difficult to implement systems and processes that can provide reasonable assurance of confidentiality in real-world implementations. In recent years, many software products have begun offering built-in encryption capabilities that are more user-friendly and manageable. When it comes to purpose-built encrypted communication tools or standards-based system-to-system encryption, the level of maturity is usually quite high. But many organizations are not prepared for the risk and pitfalls of end-user-managed (user-to-user) encryption.

The Call for Encryption

Industrial espionage, nation-state hackers and organized crime are concerns for even the smallest organization. This has not, however, slowed the rate of data capture and sharing among partners, regulators and customers. Organizations now regularly share large quantities of proprietary data and employees' or customers' personally identifiable information. Heightened awareness by the board and increased regulatory pressure are leading to increased focus on and funding for data protection.[1]

Most organizations today are comfortable deploying in-transit encryption. Security teams can easily sell the need for transport layer security (TLS)-secured web applications or push for secure protocols, such as Secure File Transfer Protocol (SFTP) and Secure Shell (SSH). Unfortunately, there are many data transfer workflows outside of IT's control or that must meet externally imposed requirements. As a result, critical and high-risk data still travel through email and attachments. More and more, users are also making use of both authorized and unauthorized cloud storage and file-sharing services.

Because it is impossible to identify and control all of these scenarios, many organizations respond by deploying end-user-managed encryption tools, hoping that users will be responsible enough to integrate encryption into the existing processes (e.g., an IT request to encrypt before sending an email). However, this approach essentially delegates the security responsibility to uninterested end users who are looking for the path of least resistance.[2]

Welcome to the Jungle

In theory, encryption is just a matter of applying some math on bits of data before and after sending a file or message. However, there is a vast ecosystem of encryption technologies, algorithms, configurations, tools and file formats. Complicating matters, end-user encryption tools are notoriously unfriendly from the end user's perspective.[3] Management and transfer of encryption keys and/or passwords and ensuring secure storage are daunting requirements to place on end users.

Even if the best, most seamless tools and training are implemented, there is still the issue of compatibility with partners. If one partner is on a different platform, deploying that platform requires additional investment and implementation efforts. Given that organizations have multiple partners, the overhead from purchasing and supporting multiple tools can quickly escalate. Failure to support the tools that internal users need to make their business partners happy will result in end users seeking creative solutions and workarounds.

> **"End-user encryption tools are notoriously unfriendly from the end user's perspective."**

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 click on the Comments link to share your thoughts.

Eric H. Goldman, CISA, Security+
Is an information security professional with experience in financial services and manufacturing. He focuses on human factors and human-computer interaction in the realm of information security. He can be reached at *Eric.Goldman@owasp.org*.

In addition to providing the "right" tools, it is also important to block unauthorized encryption solutions. Whitelisting is part of the solution, but today's user is likely to go searching for solutions in the cloud, and users may end up at some fly-by-night web site. This is problematic because a site's usage cannot be monitored or controlled. Furthermore, the services may not be properly secured or may be outright malicious. For example, that tool may offer to encrypt uploaded files, but may, unintentionally or purposefully, retain the original unencrypted copy. The user's attempt to improve security, could, unfortunately, result in a data exposure.

Even within an approved application list, there are many tools that can provide some form of encryption as a side feature. For example, many compression tools allow a widely accepted, but woefully outdated and weak form of .zip file-extension encryption (see sidebar). Allowing or encouraging users to use such tools is ill advised. Using weak or outdated encryption provides no real security value, and employing such tools could negatively impact an organization's reputation because partners may perceive a lack of knowledge or willingness to invest in security.

Even When It Works...

While an organization may be able to deploy tools that meet its needs and are compatible with partners, it is still not in the clear. Most tools are not end-to-end solutions, which increases opportunities for human error in the process. Other tools may not be enterprise ready and may not allow enterprises to disable inappropriate encryption parameters. When an organization deploys tools, it should ensure that the security team will be able to maintain oversight and control over algorithms, key length and any other variables. For example, if Office Open XML (OOXML) files (Microsoft Office 2007+ format) are being used, it is possible to control password length, complexity and algorithms centrally through the Group Policy/Office Customization Tool.[4] Standardizing using OOXML can be done, but, unfortunately, the defaults are not secure straight out of the box. There is no guarantee that partner organizations' configurations will adequately meet an enterprise's standards, and auditing partners' environments may not be practical. Furthermore, an enterprise cannot be sure that filters or other tools will not block the files along the way, since Office macro malware is a well-known threat.

Even if the technical deployment and compatibility issues have been addressed, it is important to also consider operational processes. For example, in the case of OOXML files, the user may save an encrypted copy in a directory with the original and then accidentally attach the unsecured version (users are notoriously bad at naming files, and neither the file extension nor the icon change when an OOXML file is encrypted). Crafty users may also circumvent Group Policy by emailing the original file for use at home and using a personal copy of Office without the restrictions, which results in an undesired, unencrypted external transmission. In most cases, for end-user-managed encryption, password-based symmetric encryption is preferred since it avoids the complexity of managing keys/certificates. However, the challenge of

The Case of the Zip File

A first attempt in many organizations to provide encryption facilities is to leverage the .zip format. Most common operating systems support opening password-protected .zip files, but this support is typically limited to an outdated and weak form of encryption. Some third-party tools can encrypt .zip files with robust encryption, but compatibility on the receiving end is no longer guaranteed. Even if both partners can use the more robust encryption configuration, there is no assurance users will choose the correct settings or set a strong password since most compression tools are single-user-focused and they lack the ability to administratively enforce which configurations are possible.

securely communicating that password still remains. It may be possible to implement a tool or service for such sharing, but, again, there is the issue of support and compatibility. As a result, users must be relied upon to securely communicate the shared password over another channel (e.g., call to provide passwords for email attachment). However, this becomes difficult to manage (which password goes with which email?), and a complex, long or random password will be hard to dictate verbally from user to user.

A key goal of encryption is to protect the file even when direct access is possible or the transfer is intercepted, so users must be educated on the risk of insufficient segregation of encrypted content and password. It is never acceptable to simply send the password in another email. Also, Short Message Service (SMS) should not be considered a separate channel since many users have email on their phones, and phone malware can just as easily access emails as SMS messages. Malware could detect encrypted attachments and then scan all emails to build a dictionary based on unique words or combination of phrases to test as likely passwords. The attack can be optimized by searching for nondictionary words or key phrases (e.g., "The password is").

Unintended Consequences

There are potential downsides to consider when deploying end-user-managed encryption. Content inspection is required to detect and prevent attacks (e.g., antivirus, spam filters) and prevent data theft (data loss prevention [DLP]). Generally, tools do not provide centralized management or monitoring, key/password escrow, or any type of pipeline into security analysis tools. If a DLP system has no way to learn the password/key, it cannot decrypt and read the file. Will the DLP tool default to block an encrypted file from leaving? On the receiving side, email filters cannot inspect an attachment for macro viruses if they cannot decrypt the file. As a result, end users now have to make more difficult decisions, of which they may not understand all of the consequences.

Encryption Is Not a Substitute for Access Control

Both encryption and system access control provide confidentiality. Two key differences are that access control enables the access rights to change over time and the authorization is separate from the data themselves. An encrypted file, in essence, embeds the authentication and authorization within itself. Without some additional system, there is no way to later revoke access once someone else has the password or key; it is not possible to take back a digital file. Further, unlike access control, there is no way to implement rate-limiting (e.g., denying requests for short periods of time) on brute-force password guessing.

Mistakenly, sometimes encryption is used in lieu of access control. In such cases, the proper solution is likely some form of digital rights management (DRM) or information rights management (IRM). With IRM, there is the possibility to add a call back to the server that can discontinue access even if the proper password is provided, enabling centrally managed access control even outside an organization's boundaries.

In addition, in the case of extra-organizational file sharing, encryption on its own does not limit reuse or further sharing because the receiver can simply decrypt and discard the encrypted file or share the decryption password. For highly confidential information, secure virtual data rooms may be appropriate.[5] In any case, encryption and DRM are not replacements for other usage and handling controls such as legal agreements (e.g., nondisclosure agreements) or visible and digital watermarking. Providing an encrypted document on its own usually does not legally bind another party to handle data in any particular way.

Enjoying this article?

- **Learn more about, discuss and collaborate on access control and cybersecurity in the Knowledge Center.** *http://www.isaca.org/knowledgecenter*

Another unexpected consequence of empowering users to use encryption is the risk of self-inflicted denial of service (DoS). DoS is traditionally discussed in the context of servers, but a file that cannot be decrypted is another form of denial attack—consider criminals using CryptoLocker and variants.[6] A user overzealous with security spirit may encrypt all files. That will result in a lot of passwords to remember. The user may utilize a secure password manager, but those tools also tend to lack escrow features. If that user leaves the company, no one else will have access to those encrypted documents.

There are also consequences stemming from permitting end-user-managed encryption, which may not be evident immediately. For example, how does the usage of encryption factor in with legal email retention requirements or other similar archiving processes? How will this impact content management and the ability to perform searches on data? Encryption also impacts file compression, which may be a problem for attachments, given size restrictions. Special considerations may need to be made for backup and replication procedures when there is a lot of encryption being used at the file level.

The Advantages of Centralization

Traditionally, IT departments have either attempted to find encryption features in tools already deployed, or they have deployed one or two specific end-user encryption tools common among key partners. In recent years, however, encryption gateway/proxy solutions have become a viable option. Similar to the shift from desktop clients to web applications, the encryption gateway centralizes the encryption process and allows for enhanced monitoring and control by IT. Much like any other proxy, traffic travels in-line and the encryption/decryption can be applied transparently and automated.

> **"Decision making on protocols is no longer left to the users."**

With a centralized deployment, it becomes much easier to set up connections with other partners who deploy centralized solutions, even from different vendors. The exchange of keys and certificates can be left to specialists and transmissions can use standards-based protocols. Decision making on protocols is no longer left to the users, allowing IT departments to work together on acceptable configurations or to employ machine-to-machine negotiations to ensure that only compliant encryption settings are permitted. Even if the recipient is not on the same platform, it may be possible to intelligently onboard the user/organization, leverage an IRM platform or utilize a secure file hosting service (at least access control).

The user's workload can be reduced to clicking a button or inserting a keyword (e.g., "Encrypt") into the subject line of an email. Organizations could also deploy a web portal or drag-and-drop tool to prepare the file and escrow the key/password. DLP or mail filters may be able to intelligently detect when encryption should be provided in case the user forgets or can redirect users when blocking the transmission.[7] For the receiver, the file can be decrypted in a centralized manner automatically or held for release by the user, thus allowing inspection and sandboxing to happen between decryption and access by the end user.

Limit to Authorized Encryption

Once a centralized or user-managed solution has been deployed, it is necessary to take steps to block unauthorized encryption and encrypted file egressing over unauthorized channels. This helps block outdated encryption algorithms and prevent malicious insiders or hackers from using encryption to exfiltrate data. This is similar to the type of inspection and blocking already common for secured web transactions.[8] DLP system rules should be configured to block any encryption that cannot be inspected and/or is traveling over an unapproved service, port or destination.

In addition, it is advisable to monitor software and processes on end-user systems to ensure that

Who Is the Data Owner?

Encryption is typically thought of as securing communication between two or more individuals, and only those people involved with the transfer. However, in a business scenario, it is more likely that two organizations, rather than the individual users, should be considered the owners. Many message-encryption protocols and stand-alone file encryption tools are fundamentally designed for personal use scenarios. However, in a corporate environment it is often necessary to have some form of key escrow or ability to view the unencrypted version of data by others outside of the transaction, such as legal or security teams (or at least their automated tools).

When one is evaluating encryption software and systems, it is important to consider how the tools will impact the organization's legitimate access to data. If the tools are enterprise ready, they will integrate with the DLP and IDS somehow, such as by communicating the plaintext, transferring the keys or coordinating with local software agents before encryption. Such systems must also securely manage all of the keys/passwords to prevent misuse and targeting by hackers, and should also include approval workflows and logging as appropriate.

Personal communications can and should still rely on robust, backdoor-free encryption technologies to prevent eavesdropping. In enterprises, the fundamental ownership issue means that users must understand and accept that communication is being secured between enterprises, not people.

no unauthorized encryption software is installed or being used. If such software is found, an investigation can determine if there is a legitimate business need and see if it is possible to convert that workflow to a different, authorized encryption tool. Because of the growing usage of the cloud, web traffic should be reviewed to block unauthorized web sites and services that users have used, or may attempt to use, to encrypt or decrypt data.

Ensure User Understanding and Awareness

Even with a transparent solution, proper education on encryption responsibilities and capabilities is crucial. Users must understand that encryption is more than password protection, and not all encryption is equal. DLP and artificial intelligence (AI) will never catch all cases where encryption is needed so it is best to train users to manually initiate encryption; this will provide users with peace of mind. Also, reinforcement and reeducation must be provided periodically.

Policy is also important for ensuring clarity. The enterprise must clearly define the approved configuration tools, procedures and consequences so that there is no ambiguity among users. For example, users should be prohibited from sending encrypted data home (e.g., no personal encrypted backups). The security policy should make it clear that management reserves the right, where permitted by law, to inspect and decrypt all communications and files for security, legal and other applicable reasons.

> **"Encryption is more than password protection, and not all encryption is equal."**

Conclusion

Organizations must be aware of the challenges and risk associated with putting encryption into the hands of users. Beyond finding and configuring the right technology, enterprises must ensure processes are well defined and there is sufficient user training. A centralized solution can reduce costs and support

effort, while streamlining processes and enabling better integration with DLP. In any case, encryption must be controlled and limited or it will create a security blind spot.

Endnotes

1 NYSE Governance Services and Veracode, *A 2015 Survey: Cybersecurity In The Boardroom*, 2015, *https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf*

2 Besnard, D.; B. Arief; "Computer Security Impaired by Legitimate Users," *Computers & Security*, vol. 23, iss. 3, 2004, p. 253-264

3 Whitten, A.; J. D. Tygar; "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," USENIX Security Symposium, 1999, p. 169-184, *https://www.usenix.org/legacy/events/sec99/full_papers/whitten/whitten_html/*

4 Microsoft Technet, "Group Policy and Office Customization Tool Settings in Office 2010 for OpenDocument and Office Open XML Formats," 2016, *https://technet.microsoft.com/pt-br/library/dd723552(v=office.14).aspx*

5 Pang, A.; D. Stanton; T. Nagle; "Managing Cyber-Security Risks in M&A," *Financier Worldwide*, July 2014, *www.financierworldwide.com/managing-cyber-security-risks-in-ma*

6 US Federal Bureau of Investigation, "Criminals Continue to Defraud and Extort Funds From Victims Using Cryptowall Ransomware Schemes," Internet Crime Complaint Center (IC3), 23 June 2015, *www.ic3.gov/media/2015/150623.aspx*

7 Microsoft, "Conditions and Exceptions for Transport Rules," Microsoft Developer Network, 2010, *https://msdn.microsoft.com/en-us/library/ff628740(v=exchsrvcs.149).aspx#Attachments*

8 Lyngaas, S.; "Decrypting Outbound Data: A Key to Security," *FCW*, 11 August 2015, *https://fcw.com/articles/2015/08/11/ssl-encryption.aspx*

Can Elliptic Curve Cryptography Be Trusted?

A Brief Analysis of the Security of a Popular Cryptosystem

Many smart card, cell phone, Internet of Things (IoT) and Bitcoin businesses have already implemented elliptic curve cryptography (ECC), and for good reason. This asymmetric encryption and decryption method is shown by the US National Institute of Standards and Technology (NIST) and third-party studies to significantly outperform its biggest competitors, offering significantly shorter keys, lower central processing unit (CPU) consumption and lower memory usage.[1, 2]

As security is an instrumental aspect of cryptography, it is important to evaluate every cryptogram carefully—not only for efficiency, but also for imperviousness against all kinds of cryptographic attacks. There are multiple ways to assess the security capabilities of ECC to determine if it is a worthwhile venture.

What vulnerabilities or possible weaknesses in design exist with ECC? Can ECC withstand the test of time, and what implementation issues does it face?

ECC for Security

Although there is no such thing as a perfect, widely applicable and unbreakable cryptosystem, there are many ways to keep data safe when at rest and when in motion. There exist a variety of classes of cryptoalgorithms, including hashing algorithms, symmetric cryptoalgorithms and asymmetric cryptoalgorithms. ECC, just like RSA, falls under the asymmetric algorithm (public/private key) classification. This type of cryptogram solves a variety of problems, one of which is allowing two nodes or individuals who have never communicated to each other before to pass information to each other in a secure manner. These algorithms are also a crucial cog in the mechanism of many protocols, standards, services and infrastructures. Bitcoin, X.509/PKI, Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Key Exchange (IKE), Secure Shell (SSH), Domain Name System Security Extensions (DNSSEC), Pretty Good Privacy/Gnu Privacy Guard (PGP/GPG), Secure/Multipurpose Internet Mail Extensions (S/MIME), RFC 3161, most things with digital signatures (e.g., digitally signed portable document formats [PDFs]), Z and Real Time Transport Protocol (ZRTP), and Secure Internet Live Conferencing (SILC) all deeply rely on asymmetric encryption and decryption in one way or another.

Once it is established that asymmetric encryption is needed, it is time to choose the best-fitting tool. The statistics look great for ECC. NIST-recommended key-size tables depict the shorter key advantage ECC has. For an equivalent symmetric key size of 80 bits, RSA requires 1,024 bits, while ECC requires 160 bits (a 3:1 ratio). When the symmetric key size grows to 256 bits, the ratio jumps up to 64:1. Thus, elliptic curves are computationally lighter for longer keys.[3] Further studies show that the time different processors take to encrypt and/or decrypt data can be 400 times faster for ECC than for an equivalent RSA length.[4]

The security side of ECC is complex. As of today, there are numerous standards defining and governing it, including the American National Standards Institute's (ANSI) X9.62, the Institute of Electrical and Electronics Engineers' (IEEE) P1363, the Standards for Efficient Cryptography Group (SECG), NIST's Federal Information Processing Standards (FIPS) 186-2, ANSI X9-63, Brainpool, the US National Security Agency's (NSA's) Suite B, and ANSI FRP256V1.

ECC is adaptable to a wide range of cryptographic schemes and protocols, such as the Elliptic Curve Diffie-Hellman (ECDH), the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Elliptic Curve Integrated Encryption Scheme (ECIES). The mathematical inner workings of ECC cryptography and cryptanalysis security (e.g., the Weierstrass equation that describes elliptical curves, group theory, quadratic twists, quantum mechanics behind the Shor attack and the elliptic-curve discrete-logarithm problem) are complex.

Veronika Stolbikova
Currently works as a principal infrastructure analyst (information security risk management) at Quintiles. Her areas of interest include security posture and vulnerability assessments, security risk management, secure development, and cryptography.

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 click on the Comments link to share your thoughts.

Currently Known Attacks

There are a significant number of potential vulnerabilities to elliptic curves, such as side-channel attacks and twist-security attacks. These attacks threaten to invalidate the security ECC aims to provide to private keys.

Side-channel attacks generally occur when measurements are made on the physical implementation of a cryptosystem, resulting in leaks of information. Side-channel analysis includes a variety of attacks, such as simple timing attacks, simple power attacks, differential power attacks and fault analysis.[5] During timing attacks, for instance, the malicious user measures the difference in time between observed peaks in power consumption with an oscilloscope. Relying on the fact that different operations or input values have a significant time variance, the attacker can deduce the secret key. Power attacks, on the other hand, are similar to timing attacks except for the fact that the actual shape and amplitude of voltage peaks is analyzed by the attacker. A variety of power attacks exist, including simple power analysis (SPA) and differential power analysis (DPA).

Simple countermeasures exist for all types of side-channel attacks. Both timing and simple-power attacks can be prevented with the implementation of the Montgomery power ladder (a scalar multiplication technique used to compute) into the ECC instead of using one of the other similar techniques (e.g., double-and-add, sliding window). Not only do Montgomery ladders have the advantage of providing fast scalar multiplication for ECC, but they also tend to behave regularly, masking the computation against timing and simple power-side-channel attacks.[6] Unfortunately, not all existing ECC curves support the use of ladders. The number of curves that do not support this technique is vast (e.g., Anomalous, NIST P-224, BN [2,254], BrainpoolP256t1, ANSSI FRP256v1), so it is important to check if one's ECC implementation uses a curve that both implements and supports Montgomery ladders.[7] Furthermore, simple timing attacks can be prevented by inserting dummy adds into the algorithm to act as an ignored variable; this makes the number of process operations to be performed the same regardless of the value of the secret key.[8] DPA-type side-channel attacks can be prevented in a variety of manners, including adding significant entropy to the secret key, disguising group points and using randomized projective coordinates.[9]

Another category of attacks on elliptic curves is known as twist-security (fault) attacks. Such attacks usually succeed when several conditions are met, and they all lead to the leakage of the victim's private key. Typically during a twist attack, the malicious party shares a carefully selected public key that does not lie on the agreed-upon ECC curve and that will lead to a shared key that can be easily reversed. After the victim computes a shared key (computed out of the victim's private key and the malicious public key) and computes a hash out of the shared key, the malicious party is able to extract the victim's secret key. Twist attacks can be broken down into many subcategories including small-subgroup attacks, invalid-curve attacks and invalid-curve attacks against Montgomery ladders. Small-subgroup attacks make it possible to simply enumerate the victim's private key by using a carefully selected point of small order as the public key. During the much more severe invalid curve attacks, the attacker picks a point of small

order that lies on an elliptical curve with a different constant coefficient. However, as invalid-curve attacks are limited by the use of ladders such as the aforementioned Montgomery ladder, specific twist attacks exist against those as well.[10] However, twist-security attacks generally are fairly easily mitigated by careful choices of curves and validation of various parameters.

Possible Future Attacks

While quantum computing is already facing a large variety of problems, such as its poor decoherence rates, error correction issues, state preparation issues and problems with quantum gates,[11] its advancement may bring additional challenges to ECC once it becomes a technological reality instead of the theoretical concept it is today. As quantum computers continue making strides in development, businesses must consider if quantum computers have potential implications on their ECC implementations.

Quantum computing will provide two major cryptanalytic weapons: Shor's and Grover's algorithms (and variations thereof). Shor attacks make factoring easy, essentially making it trivial for the attacker to uncover the secret key in an asymmetric cryptosystem. Grover attacks make brute-forcing easier by creating a uniform superposition over all possible inputs, destructively interfering states that are invalid and, consequently, finding inputs that satisfy a given function. Shor's and Grover's algorithms may have major implications not only for ECC, but also for asymmetric cryptography altogether. Furthermore, ECC's advantage in shorter key lengths in classical computing will prove to be a disadvantage in quantum computing. ECC will be easier to break than RSA cryptosystems due to a lower qubits (quantum equivalents of traditional bits) requirement.[12] While quantum computers present a frightening threat to ECC and asymmetric cryptography, this is not imminent, as quantum computers need to first overcome some very difficult physical limitations.

Issues With ECC Implementation

History has shown that, although a secure implementation of the ECC curve is theoretically possible, it is not easy to achieve. In fact, incorrect implementations can lead to ECC private key leaks in a number of scenarios. Such leaks can occur when incorrect results are calculated and when the input does not end up on the selected curve. Furthermore, they can happen when branch-timing errors occur or when cache-timing errors occur. In a nutshell, a lot of things can go wrong while ECC is being implemented.[13]

There are numerous examples of how failed implementation of ECC algorithms resulted in significant vulnerabilities in the cryptographic software. A great example is that of the Sony ECDSA security disaster. Although Sony used ECDSA to sign software for their PlayStation game console, they did not properly implement the algorithm. Using static parameters instead of random ones made Sony's implementation of the algorithm solvable and subsequently useless.[14]

Furthermore, there are examples of improper implementation of ECC in OpenSSL that resulted in common vulnerabilities, such as Common Vulnerability and Exposure (CVE)-2014-3572, CVE-2014-0076 and CVE-2008-5077. These vulnerabilities range from omission of the server key exchange message to malformed signatures. Worse, such issues can lead to an unauthenticated, remote attacker gaining access to Secure Sockets Layer (SSL) private keys. Improper implementation issues are a frightening security issue and must be tackled through security code review, static code analysis and penetration testing.

Possible NSA Backdoor

Over the last 10 years, there has been serious media and security community speculation that the NSA inserted a backdoor into one of the ECC standards, undermining its strength.[15] While there are currently many other third-party Cryptographically Secure

Pseudo-random Number Generator (CSPRNG) and ECC standards in existence that remain outside of the scope of this issue, the suspicions first fell on the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) elliptic curve pseudo-random generator that was used in the algorithm. One of the weaknesses publicly identified at the time had all the markings of a purposefully designed CSPRNG backdoor.[16] A 2013 Reuters report of a secret US $10 million deal with RSA only served to fuel these fires.[17] After this revelation and much public debate, Dual_EC_DRBG was excluded from the standards and is no longer used.

> **"There is no guarantee that any one team could efficiently find all existing and yet-to-be-discovered weaknesses in a cryptosystem."**

However, there are now similar suspicions about NIST Standard Curves. Since the Edward Snowden revelations, there has been significant concern that the ECC pseudo-random number generator was fabricated to inject an NSA backdoor into ECC cryptography.[18] However, the debate is still ongoing on this subject. Some cryptographers suspect that curves were deliberately chosen as having a mathematical weakness known only to the NSA. Others argue that some security considerations were not widely understood at the time the NIST curves were introduced and that some security issues were due to NIST using the US Secure Hash Algorithm 1 (SHA1) to generate algorithm parameters.

Test of Time

All cryptographers work toward a common goal: to create a cryptosystem that is too hard to break. In a sense, one could consider a cryptosystem's resistance capability to malicious attacks as its quality. However, while other products, such as cars, can be tested for quality by their own manufacturer or approved third parties, there is no guarantee that any one team could efficiently find all existing and yet-to-be-discovered weaknesses in a cryptosystem. Thus, the security community generally recommends opening up new cryptoalgorithms for the world to test the system against various types of threats. Only cryptosystems that can survive extensive community testing over time can be considered as having withstood the test of time. Equally, most security analysts strongly advise against using security through obscurity (relying on the algorithm not to be known to the attacker).[19]

ECC's strength can be analyzed by determining how well it has withstood the test of time. For example, ECC has faced multiple successful and unsuccessful brute-force attacks. In 2004, a team of mathematicians with 2,600 computers that were used over a period of 17 months completed the Certicom Elliptic Curve Cryptography (ECC) 2-109 challenge.[20] In 2009, the 112-bit prime ECDLP was solved using 200 PlayStation 3 consoles.[21] However, to date, cryptanalysts believe that the 160 bit-prime field ECC should remain secure against public attempts until at least 2020.[22]

For the first 30 or so years of ECC's existence, elliptical curves in cryptography were analyzed and experimented with mostly for theoretic and aesthetic reasons. However, during the 1990s, ECC rose in popularity. This resulted both in publicity backlash and significant scrutiny of ECC by opponents attempting to find flaws in it. While the debate between RSA and ECC continued, the latter cryptosystem finally achieved status as an accepted standard. In the end, however, ECC did not significantly rise to fame until the NSA published "The Case for Elliptic Curve Cryptography" in 2005.[23] Nonetheless, it can be said that ECC has been available for everyone to test for quite some time now and that the public should be fairly comfortable that ECC is not merely based on security through obscurity.

Conclusion

Despite the significant debate on whether there is a backdoor into elliptic curve random number generators, the algorithm, as a whole, remains fairly secure. Although there are several popular vulnerabilities in side-channel attacks, they are easily mitigated through several techniques. Quantum attacks loom over ECC, but they are yet to be widely available. Although twist-security attacks can threaten ECC, they can be militated against. Furthermore, although longer ECC keys are broken into publicly every now and then, the same is true for all other popular algorithm types. But no matter how secure ECC is theoretically, it must be properly implemented. History has shown that such a thing

is not trivial, as large teams and corporations have failed to achieve this goal. Above everything else, the aforementioned reality highlights the necessity for proper testing of both security and proper implementation of the algorithm.

Endnotes

1 National Security Agency (NSA), "The Case for Elliptic Curve Cryptography," USA, 2015
2 Lauter, K.; "Elliptic Curve Cryptography for Wireless Security," Microsoft Corp., 2004, *www.msr-waypoint.com/en-us/um/people/klauter/ieeefinal.pdf*
3 *Op cit*, NSA
4 *Op cit*, Lauter
5 Bar-El, H.; "Introduction to Side Channel Attacks," Discretix Technologies Ltd., 2003
6 Joyce, M.; S.-M. Yen; *et al.*; "The Montgomery Powering Ladder," Cryptographic Hardware and Embedded Systems, CHES 2002, volume 2523, *Lecture Notes in Computer Science*, Springer-Verlag, 2003, p. 291-302, *https://choucroutage.com/Papers/SideChannelAttacks/ches-2002-joye.pdf*
7 Bernstein, D.; T. Lange; *et al.*; "SafeCurves: Choosing Safe Curves for Elliptic-curve Cryptography," *http://safecurves.cr.yp.to*
8 Kadir, S.; A. Sasongko; *et al.*; "Simple Power Analysis Attack Against ECC Processor on FPGA Implementation," 2011, *http://140.98.202.196/xpl/articleDetails. jsp?arnumber=6021757&reload=true&searchWithin=%22Authors%22:.QT.Sasongko,%20A..QT.&newsearch=true*
9 Coron, J. S.; "Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems, Cryptographic Hardware and Embedded Systems," *Lecture Notes in Computer Science*, vol. 1717, 1999
10 *Op cit*, Bernstein
11 Ponnath, A.; "Difficulties in the Implementation of Quantum Computers," 2006, *http://arxiv.org/pdf/cs/0602096.pdf*
12 Yan, S. Y.; *Quantum Attacks on the Public-Key Cryptosystems*, Springer, USA, 2013
13 *Op cit*, Bernstein
14 The Central Scrutinizer, "Sony's PS3 Security Is Epic Fail—Videos Within," PSX-Scene Forum, 29 December 2010, *http://psx-scene.com/forums/content/sony-s-ps3-security-epic-fail-videos-within-581/?s=68e141dc91333038e2223ee86e3c748f*
15 Schneier, B.; "Did NSA Put a Secret Backdoor in New Encryption Standard?," *Schneier on Security* blog, 15 November 2007, *https://www.schneier.com/essays/archives/2007/11/did_nsa_put_a_secret.html*
16 Schneier, B.; "The NSA Is Breaking Most Encryption on the Internet," *Schneier on Security* blog, 5 September 2013, *https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html#c1675929*
17 Menn, J.; "Exclusive: Secret Contract Tied NSA and Security Industry Pioneer," *Reuters*, 20 December 2013, *www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220*
18 Hales, C.; "The NSA Back Door to NIST," *Notices of the AMS*, vol. 61, no. 2, *www.ams.org/notices/201402/rnoti-p190.pdf*
19 Douligeris, C.; D. N. Serpanos; "Network Security: Current Status and Future Directions," IEEE, 2007
20 Certicom, "Certicom Announces Elliptic Curve Cryptography Challenge Winner," 27 April 2004, *https://www.certicom.com/news-releases/300-solution-required-team-of-mathematicians-2600-computers-and-17-months-*
21 Bos, J.; M. Kaigara; *et al.*; "PlayStation 3 Computing Breaks 2^60 Barrier 112-bit Prime ECDLP Solved," *Laboratory for Cryptological Algorithms*, 25 November 2015, *http://lacal.epfl.ch/112bit_prime*
22 Bos, J.; M. Kaigara; *et al.*; "On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography," Microsoft Research, 1 September 2009, *http://lacal.epfl.ch/files/content/sites/lacal/files/papers/ecdl2.pdf*
23 Koblitz, A. H.; N. Koblitz; A. Menezes; "Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift," *Journal of Number Theory*, vol. 131, iss. 8, 2011, p. 781-814 *www.sciencedirect.com/science/article/pii/S0022314X09000481*

Protecting Information—Practical Strategies for CIOs and CISOs

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 click on the Comments link to share your thoughts.

Information is a vital business asset, but it is not always recognized as such. Information leaks have crippled many organizations in the past, sometimes to the point that repair is impossible. The failure to visualize the effects of loss of critical information can lead to major consequences. Organizations that do not position their information security group (ISG) strategically within the organization's structure often fail to receive the desired benefits. Stakeholders complain that their ISG is always a cost center, i.e., its function and resultant budget allocation are always high compared to other departments. Many employees feel the ISG is effective only in a reactive mode—responding to (but not necessarily anticipating) security incidents. Quantifying return on investment and ensuring the exact benefits from information security projects are relatively difficult.

Information security is usually a top priority for the chief information officer (CIO). CIOs should ensure a top-down approach and culture to working toward information security within the organization. A practical way of initiating information security is for the CIO to work with the chief information security officer (CISO) to define a governance framework and then entrust the operational responsibility entirely to the CISO. In many organizations, CIOs lose technical focus due to the exponentially fast-changing technology landscape. The challenge they face is to approach the security landscape technically, convince the board of this approach, move the ISG from a cost center to a profit center and invest proactively. The ideal way to accomplish this is for the CIO to introduce a revenue model projecting the possible losses that may result from not making these changes, e.g., impacts of a security breach supplemented with a cost-benefit analysis.

IT security governance should not be confused with IT security management. IT security management is concerned with making decisions to mitigate risk, while governance determines who is authorized to make decisions. Information security governance refers to the leadership, organizational structure, roles and responsibilities, and various processes established for information security. While management recommends security strategies, governance ensures that security strategies are aligned with business objectives and consistent with regulations.

Accurately Positioning the CISO and Delegating Tasks

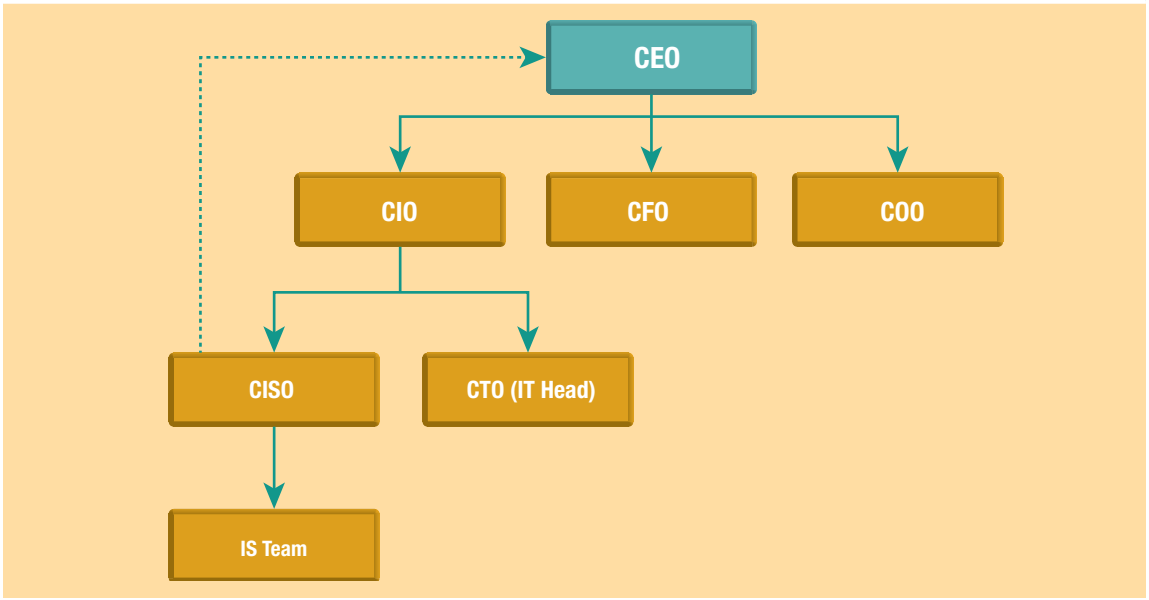
Information security should be a priority at the board level, so the next priority of the CIO is the tactical positioning of the CISO (**figure 1**). Certain organizations mandate the CISO to report directly to the CIO (meaning the CIO has authority over the CISO) and, in a dotted-line way, to the chief executive officer (CEO) meaning the CEO has influence, but not authority. Such organizations care a lot about information security. This reporting structure enables the CISO to handle escalations effectively and ensure support even from top-level stakeholders.

By developing and utilizing a sound security governance framework, the CISO can ensure that information security strategies are well aligned with business objectives and applicable laws and regulations. While the CISO standardizes and fine-tunes the individual information security requirements of each business group, the CIO should be the master integrator initially. Once operations are mature, the CIO can effectively delegate the responsibility of integration to CISO. The CIO and CISO should balance internal security, compliance needs and budget considerations.

The CISO should analyze, in depth, the value addition from information security projects and streamlined operations. The security managers,

Devassy Jose Tharakan, CISA, ISO 27001 LA, ITIL, PMP
Has more than eight years of experience in IT infrastructure security. He works with a leading financial entity in India as information security manager. In this capacity, he is responsible for enterprise security architecture and projects to counter cybersecurity attacks and he heads the security audit practice. In his prior engagement with Elenco Emirates Group as group IT manager, he was active in various infrastructure security knowledge forums in United Arab Emirates. His passion is to help enterprises adopt the right security strategy for better risk management and increased efficiency. He has helped many banking, insurance, retail and defense enterprises redesign their security infrastructure and adopt information security strategies.

Figure 1—Scope of Auditable IS/IT Risk Management Activities



selected by the CISO, should work with internal business groups in selecting the right tools that are effective and scalable in the given context.

The CISO

In the information security governance program, the roles and the responsibilities of the CISO should be well defined. One of the main responsibilities entrusted to the CISO is to draft a long-term information security strategy and obtain approvals from the board. This should be consistent with security plans for the individual systems. The CISO should be a strong mentor and should always encourage team members to adopt a consulting posture to address the security requirements of business groups and conceptualize the external threat landscape. The CISO should collect feedback based on the defined metrics and report to the board on the effectiveness of the information security program.

Prior to protecting all of the available information, initial attempts should be focused on identifying where critical information resides within the organization and who owns it. Data classification based on information criticality should be the foundation of any information security strategy. Once critical information is identified, success depends upon the controls used to protect it.

The Role of the Information Security Team

The information security team, which operates under the leadership of the CISO, should always be at the disposal of the business to consult and guide. Rather than spending all of its time developing security policies and implementing them, the information security team should work together on strategies to mitigate operational risk. Upper management should ensure that the information security team gets the right amount of visibility and respect from all of the core business functions. This can be done by framing information security as a core value and priority of the organization.

The priority of the information security team is to identify the areas of low and high risk in the organization. Risk frameworks should align closely with enterprise risk management (ERM) portfolios, if available. Such alignment helps avoid the ambiguity that can arise when there is conflict among individual risk management strategies for various information security and business continuity projects.

Mitigating Operational Risk

Adequate segregation of duties (SoD) and control responsibilities should be established in all of the functional areas of an organization. It is not always required to have professionals who are very technical or experienced perform basic tasks. For example, user access can be provisioned by a trained member of the security operations center (SOC) team. It is recommended to cross-train the operations team members, which can help in organizing and improving an enterprise's internal business continuity plan.

> **"The information security team... should always be at the disposal of the business to consult and guide."**

Many medium-sized enterprises use a hybrid model of outsourcing their security operations by maintaining a small team in-house primarily for budget control. Outsourcing security operations is a good choice for medium-sized organizations, as it helps them reduce the hassles of maintaining an always-functioning environment. The outsourced team may have considerable specialized knowledge on security operations acquired from its work with multiple clients—knowledge that is not possessed by the in-house department.

Of course, outsourcing is not without risk. There is always a chance vital information may leak about an enterprise's network, security architecture or vulnerabilities in the architecture. But this concern can be addressed through instruments such as nondisclosure agreements (NDAs).

For larger organizations, especially for those in the government or financial domains, it is always better to have an in-house team for primary security operations, as the degree of data confidentiality involved is relatively high. The incident response time of in-house teams always seems to be better than their geographically separated outsourced counterparts. In countries where weak legal systems exist, stringent criteria should be used to evaluate support contracts from outsourcing partners or security vendors. The terms, conditions and responsibilities mentioned in the contract should be completely unambiguous and workable by both parties. Any legal disputes arising during the valid contract period can increase the risk posture of the organization that outsources key security functions.

Effective strategies should be deployed in such cases to maintain the integrity of information security between the in-house team and the vendor. The technical capabilities of the vendor should be evaluated before the engagement. This can include a review of financial statements, past performance of the outsourcing partner and brand reputation. Some vendors will highlight extravagant team profiles during the initial discussions and fail to deploy them when the project is awarded. It is recommended to have an exit strategy and backup plan if any of the critical security vendors or partners fails to meet the set expectations, which would abruptly raise risk levels.

Conclusion

As experienced when working with a defense-sector manufacturer in United Arab Emirates, the importance and ease of having a well-structured information security system became apparent. The foundational pillars of information security were laid out by the government, and adopting them by an enterprise was extremely easy.

But in developing countries, such as India, many companies struggle to maintain a fully functional information security ecosystem. The expectations and responsibilities entrusted to CIOs and CISOs are quite high. In such cases, the CISO can take control by acting as the master integrator of information security, as that role is best suited to ensure that information security goals are well aligned with enterprise goals. This should, in turn, create a strong security ecosystem. Combined with an in-depth knowledge of the underlying architecture, the CISO can equip the information security team to better respond to information security concerns and cyberrisk.

Enjoying this article?

- **Learn more about, discuss and collaborate on information security management in the Knowledge Center.** *www.isaca.org/topic-information-security-management*

Going Beyond the Technical in SIEM

The majority of modern companies encounter information security challenges every day, ranging from external targeted attacks to internal leaks, despite using various information security approaches and tools. IT is rapidly evolving, in keeping with the threat landscape; but new approaches and tools mean new vulnerabilities. Violators are becoming smarter and faster. The classic confidentiality, integrity and availability (CIA) triad has not been enough to address these challenges, especially when information security incidents occur (i.e., the CIA triad was violated fully or partially).

Global analytical reports find a growing number of incidents annually and increasing incident sophistication.[1] In other words, incidents have happened, are happening and will be happening. For timely incident detection and deep forensics, it is necessary to expand information security abilities and the CIA triad, ensuring accountability. However, accountability creates millions of security events;[2] therefore, it is important to ensure effective security information and event management (SIEM)[3] within an information security management system (ISMS).[4]

This article addresses an existing imbalance between technical issues and process aspects related to SIEM. This gap is the root cause of some skepticism with and disappointment in SIEM.

SIEM Process

Be aware that before implementing SIEM, it is necessary to establish the basis of the ISMS, which will include considering the global management commitment, asset inventory and categorization and risk assessment. The SIEM process can be implemented when the needed enterprise security tools are obtained and the process capability model level is no lower than the managed process outlined in COBIT® 5.[5]

The SIEM process consists of following a five-step cycle (see **figure 1**).

This SIEM approach is based on the plan-do-check-act (PDCA) cycle. This article focuses on the policy establishment step of the SIEM cycle.

SIEM Policy Establishment

High-ranking management should demonstrate a commitment to the ISMS, including SIEM, by ensuring the SIEM policy is established and is compatible with the business direction, context and risk approach. Usually, the chief information security officer (CISO) prepares this internal policy and obtains the approval of all stakeholders. This policy should be mapped with existing internal policies, such as defining detailed event lists into standards and baselines for servers and network tools.

The SIEM policy should contain these basic components:

- Purpose of the policy
- Scope of the SIEM infrastructure
- Responsibilities of involved individuals
- Compliance

Purpose

Purpose describes the need for a policy and should rely on and link to business tasks, objectives and context. There are many reasons for developing a SIEM policy. Some of the reasons include:

- Having a comprehensive IT security vision
- Developing incident detection
- Improving IT security forensics and analytics
- Establishing compliance

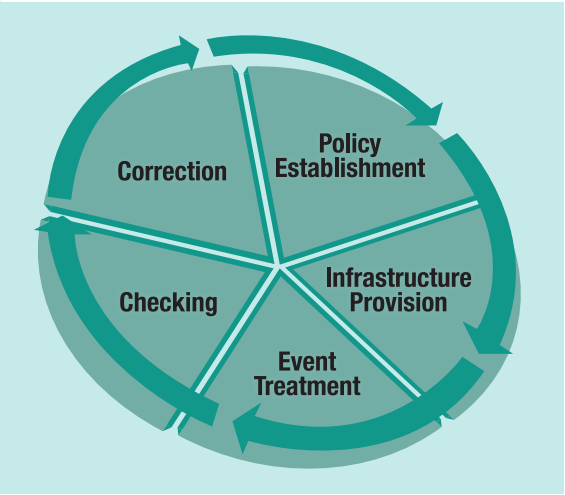
Scope

Scope is the biggest part of the SIEM policy due to its description of the SIEM infrastructure. A SIEM infrastructure is more than just the SIEM system. It is a common misconception that a SIEM system is the essential component for SIEM infrastructure. The SIEM system is a technological solution and is just a component of the SIEM infrastructure. A SIEM infrastructure consists of different event sources, event storage, analysis tools and a monitoring console and also includes external information providers, e.g., McAfee Global Threat Intelligence, RSA FirstWatch and Kaspersky Security Intelligence Services. Event sources are an essential component

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 click on the Comments link to share your thoughts.

Aleksandr Kuznetcov, CISM
Is head of the information security department at the research and development center at Vulkan LLP. In this capacity, he leads the security information and event management (SIEM) implementation team. He has 10 years of experience in information security and five years of experience in SIEM. He is an active author and public speaker on his areas of expertise. He is also pursuing a postgraduate degree at Financial University (Moscow, Russia).

Figure 1—The Steps of the SIEM Cycle



Source: Aleksandr Kuznetcov. Reprinted with permission.

of SIEM infrastructure as the event source puts data into audit trails (i.e., registered events). Without registered events, a SIEM system is useless.

An event source is any software or fireware (a set of software and hardware). This can include:

- Firewalls (FW)
- Host/network intrusion detection/protection systems (IDS/IPS)
- Virtual private network (VPN) tools
- Unified threat management (UTM) systems
- Certification authority (CA)
- Encryption tools
- Endpoint security tools
- Antivirus (AV) tools
- Vulnerability scanners (VS)
- Data loss prevention (DLP) systems
- Identity and access management (IAM) systems
- System software (e.g., operation system, hypervisor)
- Application software (e.g., database management system, web server)

There are two main criteria that determine if a piece of equipment is the event source:

- Logging ability
- Ability to provide access to log data

If the first criterion is not possible, the equipment in question is not an event source. If the second criterion is not possible, the equipment is an isolated event source.

The main component of event sources are security tools, which are enterprise-level solutions that comply with the two previously discussed main factors (i.e., logging ability and ability to provide access to log data). Tools such as FW, IDS/IPS or UTM are network security tools.

There is a separate type of event source that supplies network packets. This type of tool includes Switched Port Analyzer (SPAN) ports, Test Access Point (TAP) solutions and sniffers. Network packets may be more useful than log data.

Brian Girardi, vice president of product architecture and research at RSA, said, “We need more complete data sources and visibility into networking data, which means the way we keep, manage, process and model data must change. We need to make it more consumable—not just more data, but better data.” To make data more consumable, the following questions should be considered:

- Where are data collected?
- What is collecting data?

The following steps can provide enterprises with some direction when answering the previous questions:

- Segment the network in consistency with asset groups and critical levels, i.e., define trusted zones (e.g., internal segment, preproduction segment) and critical zones (e.g., the payment card industry segment, demilitarized zone).
- Define interconnection points between zones.
- Data should flow relatively freely within trusted zones, whereas data flowing in and out of the trusted zone (interconnection points) require more control.

Therefore, data should be collected:

- Within trusted zones at the basic level (logs)
- Within critical zones at the advanced level (first, logs; second, network packets)
- Into interconnection points at the advanced level (first, network packets; second, logs)

When discussing what is being collected, remember that the first principle of gathering is that collecting all data is not the main goal of SIEM. Collected data must be valuable, and unused data are not required and should be discarded. Unused data are of no value and waste the time of the SIEM team. Remember that collection from a 100 Mbps line (network packets) equates to 1 terabyte (TB) of storage per day. Not all organizations are prepared to spend enough to develop this kind of storage capacity. To better manage this large storage requirement, consider the following:

- Become familiar with baseline and normal events (create a business-day profile, define top of services, sources and destinations).
- Filter out known good and unwanted network traffic (allowed by information security policies), i.e., reduce the amount of information, but do not just drop or filter it because it takes up space.
- Focus on the critical security information. This can provide better visibility into unknown and untrusted data.
- Focus on the places where there are no information security controls.
- Periodically (e.g., monthly) review defined baselines and profiles.

Responsibilities

While senior management should retain overall responsibility for the SIEM policy, a SIEM process owner should be appointed. This process owner does not have to be the chief information security officer (CISO). Senior management should define SIEM team structure.

Compliance

Compliance defines how to judge the effectiveness of a SIEM policy (i.e., how well it is working) and what happens when this policy is violated (the sanction). Sometimes, metrics and key performance indicators are described in this portion.

Conclusion

The SIEM has become the core of an ISMS and security operation centers (SOC), but it is unwise to rely on just the technical aspects of SIEM. The SIEM policy is essential for ensuring effective SIEM within an ISMS. The time used for SIEM policy development is worthwhile; it will save effort in future steps. The biggest part of the policy—scope—deserves special attention, and it is important to remember that the basis of SIEM infrastructure is event sources, not the SIEM system.

Endnotes

1 PricewaterhouseCoopers, *The Global State of Information Security Survey 2016*, 2015, *www.pwc.com/gsiss2015*

2 A security event is a change in or retention of the status, which has implications for IS, management, the health of the component(s) of IT infrastructure and/or ISMS of a company. It also affects the audit trail (file, database table or some other location) information for this event.

3 SIEM is a part of the ISMS of a company, including technological components, processes and staff.

4 ISMS is a part of the overall management system of a company, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve IS.

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

A Secure Data-gathering Approach in Wireless Sensor Networks

Considering QoS Via Hashing Mechanism

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 click on the Comments link to share your thoughts.

Data collection is a challenging task in wireless sensor networks (WSNs) due to the limitations in communication bandwidth and the energy budget.[1] Many practical applications require continuous long-term data collection, without interruption for months or even years. Generally, WSNs consist of some number of battery-powered sensors. Through a multihop path, a sensor node transmits the information wirelessly to a receiver node with a limited communication range. Here, the multi-hop represents the communication between two end nodes via a number of intermediate nodes. Therefore, a single communication contains multiple paths to transmit the information. An efficient data-collection strategy is designed to minimize the energy cost of the sensor nodes; it also improves the network lifetime. In many applications, the gathering of continuous datasets from a resource-constrained WSN is unnecessary and difficult. It causes serious problems during the transmission of large amounts of data to the sink node. Due to the limited bandwidth of sensor nodes, packet drop reduces the quality of data. The largest amount of energy is consumed when more data are collected because data are transmitted or collected in the form of packets. In general, 0.1 J of energy is allocated for each and every packet; therefore, if more data are collected, obviously, a large amount of energy is consumed.

Secure communication is the most essential task to ensure the integrity and authenticity of transmitted data. In many applications, secure data transfer between the sensor nodes and the base station is also essential.[2] While transferring the message, the base station must ensure that the obtained message should not be modified. A lightweight authentication scheme was required to protect data from unprivileged users, which is used in various WSN applications, e.g., military domains and health care monitoring. Generally, the multihop path becomes the target of attacks. It attacks nodes physically and creates a traffic collision or makes communication jam on the channel by generating radio interferences. Data encryption is essential in sensor networks when the sensors can be the subject of many types of attacks. Attackers can easily monitor and inject false data when the data are transmitted without encryption in the network.[3] In general, sensor nodes encrypt the data on a hop-by-hop basis. An intermediate node keeps the keys of all sensing nodes, decrypts the received encrypted value and gathers all of the received values. Finally, the result in transmission to the base station is encrypted. This method is complicated and expensive due to the received data being decrypted before aggregation. Additionally, it produces an overhead imposed by key management.

To overcome these issues, this article focuses on a secure data-gathering scheme that considers throughput, delay and energy quality of service (QoS) parameters. To reduce the computational overhead of sensor nodes, this article proposes a new hash-based authentication scheme for WSNs that produces a strong and unique message authentication code for a particular message. A preshared secret key is obtained from the Elliptic Curve Diffie-Hellman Key Exchange (ECDH-KE) algorithm. This algorithm is designed based on a modified hash function that is used to calculate the message authentication code for giving messages. This algorithm delivers both integrity and the authenticity of a message with a single hash value. Before transmitting the message, the signature is verified by each sensor node to minimize the overhead introduced in the network.

Using ECDH-KE

Suppose that Alice wants to transmit data to Bob. Initially, the network is formed by generating a private key for all nodes. After that, a neighbor estimation is done using Euclidean distance. To discover the route, the distance of the node from the source, Alice, to the destination, Bob, is calculated. The formula for finding the distance is:

Michael Roseline Juliana
Is an associate professor in the Department of Electronics and Communication Engineering at St. Michael College of Engineering and Technology (Kalayarkoil, Tamilnadu, India).

Subramaniam Srinivasan, Ph.D.
Is professor and head of the Department of Computer Science and Engineering at Anna University at the regional office in Madurai, Tamilnadu, India. He has published more than 90 research papers in journals, conferences and workshops.

$D = v\ (a_2 - a_1)^2 + (b_2 - b1)^2$

Where (a_1, b_1) are the positions of the source node and (a_2, b_2) are the positions of the node from which the distance is calculated. After the distance is calculated, the route is computed. For authentication, the ECDH-KE formula is used, as it is a dependable algorithm in terms of communication, overhead limitations and energy consumption of the WSN. The ECDH-KE algorithm requires a preshared secret key to be used between sensor nodes (SNs) and the base station (BS). Between the BS and SN, a secret key (S_k) is proposed. The process is illustrated in **figure 1**.

For transmitting messages, the authenticity and integrity must be easy and secure to calculate. A modified secure hash algorithm is used to compute the message authentication code of a given message, M. Using a regularly distributed pseudorandom function, a modified hash function is proposed. The default secure hash function uses the following logical functions in the main loop:

$fp\ (X,Y,Z) = (X\text{^}Y)\ v\ ((\sim X)\text{^}Z)$

$fp\ (X,Y,Z) = X+Y+Z$

$fp\ (X,Y,Z) = (X\text{^}Y)\ V\ (X\text{^}Y)\ V\ (Y\text{^}Z)$

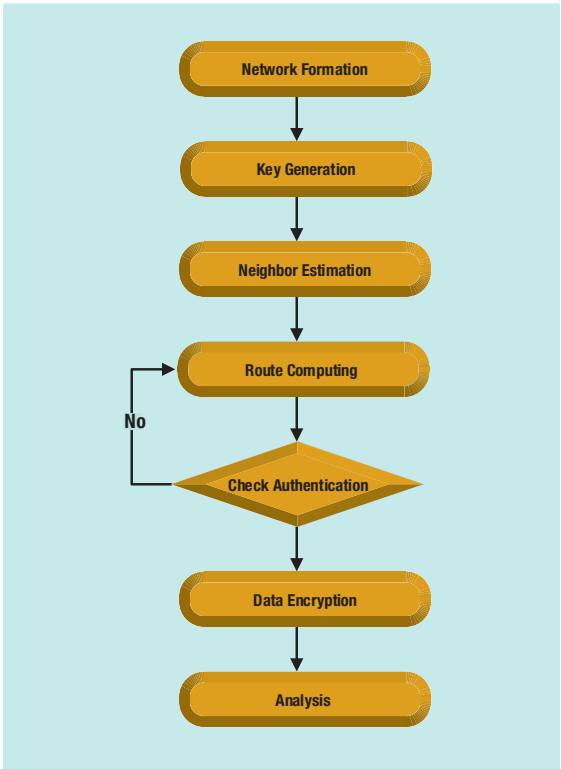
$fp\ (X,Y,Z) = X\ ?\ Y\ ?\ Z$

With the help of the pseudorandom function, the previous logical functions are modified. Due to its randomness and lack of a repeating period, unique hash values are obtained for each message. The modified pseudorandom function with a secret key is defined as:

$F\ (Qp\ ) = Qp\ *\ v2\ *S_k$

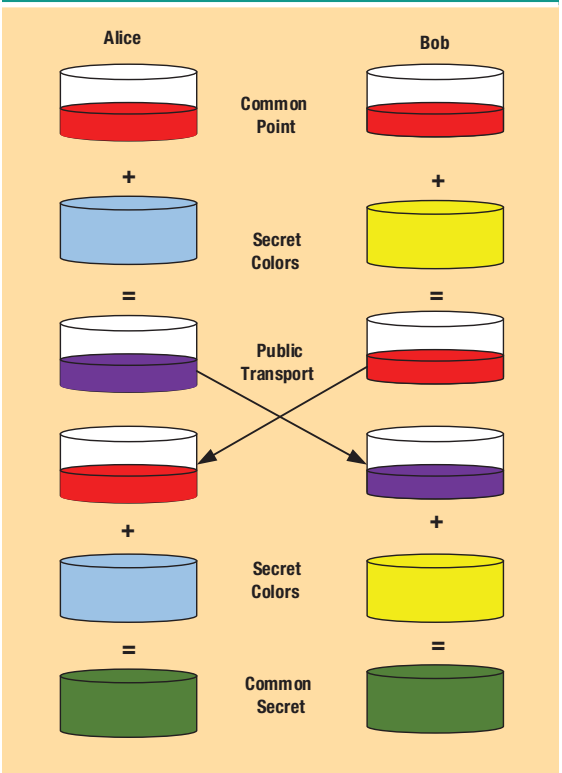
The previous equation is used as a message integrity and authenticity code. Based on the input message and secret key, the output value of the hash function

Figure 1—Flow Diagram of Proposed Method



Source: M. R. Juliana and S. Srinivasan. Reprinted with permission.

Figure 2—Elliptic Curve Diffie-Hellman Key Exchange



Source: M. R. Juliana and S. Srinivasan. Reprinted with permission.

Enjoying this article?

- Learn more about, discuss and collaborate on network security and wireless in the Knowledge Center. *www.isaca.org/knowledgecenter*

is obtained. The appropriate hash value for the message can be computed by holders of the secret key only. **Figure 2** uses color to show the simple model of key exchange.

Alice and Bob have kept their private keys (represented in **figure 2** as their color) securely to themselves and have sent their public keys directly to each other. They fix a finite field, F_f, an elliptic curve, E_c, which was defined over the finite field, and base point $B?E_c$. Alice selects a random $a?F_f$, which keeps the key secret. It then computes the public key $aB?E_c$ and transmits it to Bob. On the other side, Bob selects a random integer, b, and computes bB, which is transmitted to Alice. The common secret key is $?E_c$.

An elliptic curve over a field is defined as:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

For any cryptographic technique, there is an analog for the elliptic curve. The ECDH-KE is one of the systems. In the proposed method, the encryption of the message is done by the Diffie-Hellman exchanging key. In encryption, the sender calculates the multiplication between the coordinates of the key.

Algorithm 1: ECDH-KE

- Step 1: Alice and Bob select a finite field, F_f, and an elliptic curve, E_(c,), defined over it, E_c (F_f).
- Step 2: Both publicly choose a random base point, B, belonging in Ec.
- Step 3: Alice selects a secret random integer, n. Then she calculates $nB?E_c$ and forwards it to Bob.
- Step 4: Bob selects a secret random integer, m. Then he calculates $mB?E_c$ and forwards it to Alice.
- Step 5: nB and mB are public keys and n and m are secret keys.
- Step 6: Alice calculates the secret key, nmB=n(mB).
- Step 7: Bob calculates the secret key, nmB=m(nB).

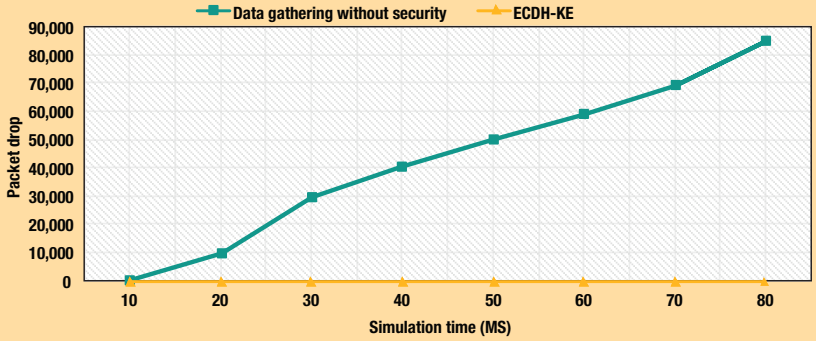
Performance Analysis

This section discusses the performance evaluation of the proposed ECDH-KE formula. The security-based data-gathering ECDH-KE method is compared with the existing data-gathering method that does not have security. The criteria of packet drop, energy consumption, network lifetime, residual energy and throughput are used for analyzing the performance.

Figure 3 shows the comparison graph for the number of packets dropped against simulation time. The execution time varies from 10 to 80 milliseconds. When more than one packet of data fails to reach its destination during transmission, packet drop occurs. When compared to the existing method, the ECDH-KE method results in fewer packet drops.

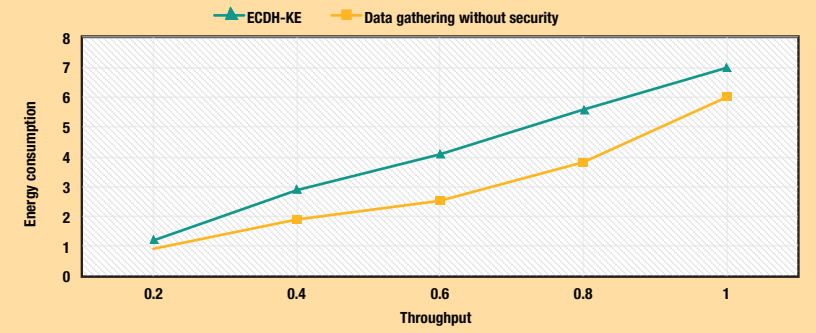
The amount of energy consumption for the

Figure 3—Comparison of Packet Drop With Simulation Time



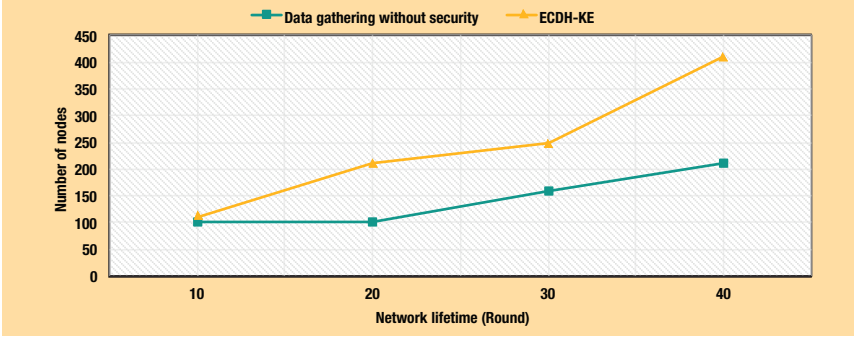
Source: M. R. Juliana and S. Srinivasan. Reprinted with permission.

Figure 4—Comparison of Energy Consumption With Throughput



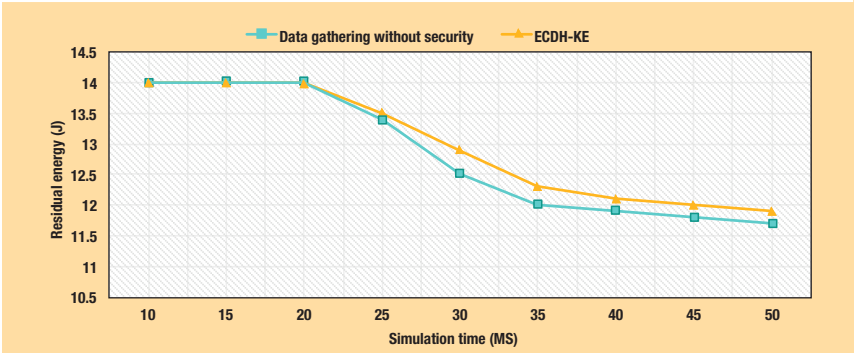
Source: M. R. Juliana and S. Srinivasan. Reprinted with permission.

Figure 5—Comparison of Network Lifetime With the Number of Nodes



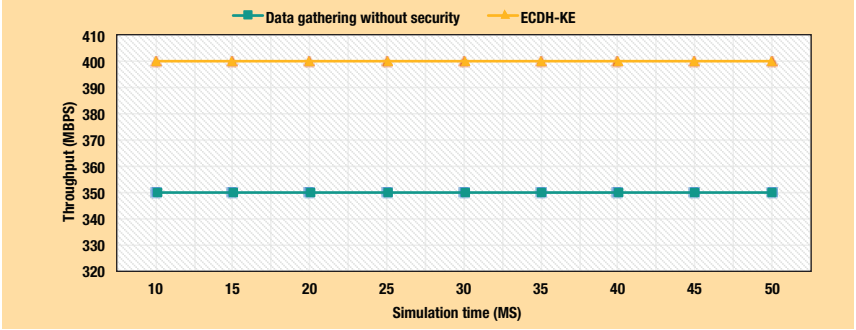
Source: M. R. Juliana and S. Srinivasan. Reprinted with permission.

Figure 6—Comparison of Residual Energy vs. Simulation Time



Source: M. R. Juliana and S. Srinivasan. Reprinted with permission.

Figure 7—Comparison of Residual Energy vs. Simulation Time



Source: M. R. Juliana and S. Srinivasan. Reprinted with permission.

amount of work that can be performed (throughput) is plotted in **figure 4**. Energy is measured in joules, and throughput is measured in megabits per second (Mbps). The energy consumption of the ECDH-KE method is compared with the existing method. As seen in **figure 4**, the proposed method achieves significant energy savings in comparison to the existing method.

The lifetime of the network for the ECDH-KE method compared with the existing method is shown in **figure 5**. The graph considers the number of active nodes and compares that to the number of iterations in a network. The residual energy analysis of the proposed ECDH-KE method and existing method is depicted in **figure 6**.

Figure 7 shows the throughput comparison graph for ECDH-KE and data gathering without a security method. The output performance shows that the proposed method provides significantly more throughput than the existing method.

Conclusion

This article proposes an ECDH-KE algorithm to provide a security-based data-gathering approach. A preshared secret key exchange is used between the sensor nodes and base station, and it provides better security for data gathering. The transmitter computes the product between the coordinates of the key in the encryption algorithm. The experimental results show the effectiveness of ECDH-KE in terms of network lifetime, energy consumption and throughput, as compared to the existing method. Most of the existing research methodologies construct the secure data-gathering approach in WSN. However, there is one more issue that is important for data gathering, which is the consumption of energy. For future enhancement, this proposed methodology can be extended to reach low energy consumption through data gathering in a WSN.

Endnotes

1 Wang, F.; J. Liu; "Networked Wireless Sensor Data Collection: Issues, Challenges, and Approaches," *IEEE Communications Surveys & Tutorials*, vol. 13, June 2010, *http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5497857*

2 Shu, T; *et al.*, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes," *IEEE Transactions on Mobile Computing*, vol. 9, July 2010, *www.computer.org/csdl/trans/tm/2010/07/ttm2010070941-abs.html*

3 Bahi, J.; *et al.*, "Secure Data Aggregation in Wireless Sensor Networks: Homomorphism versus Watermarking Approach," *Ad Hoc Networks*, vol. 49, edited by J. Zheng, *et al.*, Eds., Springer Berlin Heidelberg, 2010, p. 344-358

Big Data—Hot Air or Hot Topic?

In August 2014, the ISACA® London (UK) Chapter organised an event in collaboration with PricewaterhouseCoopers (PwC) in London. The topic of the event was big data and concerns about the changes that this concept may bring to organisations. During the event, there were several questions and table discussions for the audience about the topic. This article summarizes the material presented during the event, the answers the audience provided to survey questions distributed during the session, and the key thoughts and topics covered during the table discussions.

There are many different definitions of the term 'big data', and concerns about whether it will necessitate significant changes in business operations in the short term. However, it is broadly recognised that, as technology becomes cheaper and more user friendly, there are more data than there used to be, and those data get more media attention than ever before.

Advantages

One of the key advantages of big data is that it can provide new insights that may lead to making more informed decisions. This is not applicable just for organisations, but also for customers. Consumers compare experiences across industries and expect to be able to find reviews and give feedback, have their views taken into account, and collaborate with their favourite brands. Consumers are better informed than ever, which means they make smarter decisions that lead to better outcomes. The rapid evolution of personal technology has created consumer thirst for innovative new services and products.

Angel Serrano, CISA, CISM, CRISC
Is a board member of the ISACA® London Chapter. For the last 10 years, he has been working for PricewaterhouseCoopers, focusing on data analytics and business intelligence in the financial sector. His background also includes IT risk assurance and IT security management.

Risk

There are risk factors as well as advantages to using big data. A more data-savvy public often objects to the kind of profiling that data analytics is so good at executing. Regulators, too, are becoming more aware of the power of data analytics. To use data, one needs to have the data. In the future, effective data analytics will require an effective data strategy to plan for the collection of data, including purchasing and accessing external data sets.

It has never been so easy to use data to make mistakes more quickly than ever before. With big data and faster decision making, understanding the quality of the data is of primary importance. Taking advantage of the availability and power of data can cut costs, raise revenue and help futureproof a business. But that is also true for the organisation's competitors.

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 click on the Comments link to share your thoughts.

Approach to Big Data

Data analytics is a powerful tool, but the key to successful use of data relies on understanding what is being looked for in advance or applying systematic techniques that can be relied on to determine answers. A specific, measurable, actionable, realistic, timely (SMART) approach to big data is a powerful option

and has been and is being deployed. Organisations must pick the appropriate technique and method and be bold enough to act on the findings. They must ensure that in any big data exercise, a customer fairness lens is always applied to validate any findings and evidence to ensure regulatory compliance.

There are several themes organisations need to master to be successful:

- **Know the customer.** Understand the rapidly evolving digital customer's behaviours, needs and desired outcomes, and the impact on profitability and growth.
- **Develop products.** Create new business ideas for incubation and development to scale.
- **Create strategy.** Design a strategy that addresses the required proposition and optimal operating model and a clear route to achieving it.
- **Foster interaction.** Adopt agile approaches to design, build and integrate enterprise-wide social, mobile and web solutions.
- **Manage risk.** Be equipped to protect the organisation's assets, data and reputation against the threats of the digital world.

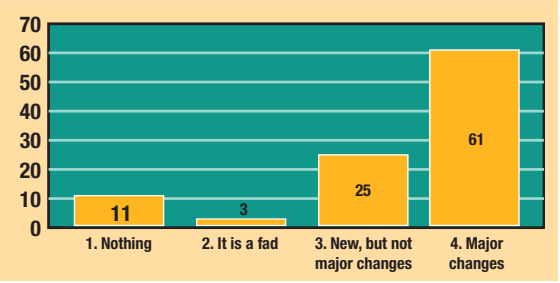
Difference Between the Traditional and SMART Approaches

In the traditional approach, the first step is to collect and manage data, then analyse them, draw insight with that analysis and, finally, make decisions based on the analysis performed. In the SMART approach, the first step is to predetermine decisions and, based on those determinations, gain necessary insight. Determine the data required to draw such insight, then collect and manage the necessary data. However, data managers should pay attention to the quality, completeness and accuracy of the data collected for the purposes of the analysis, which continues to be a major concern in this approach.

Questions for the Audience

During the event, there were 10 questions addressed to the audience, which were answered by more than 100 attendees. These are the questions and answers in percentages from the audience.

Figure 1—Is There Anything New About Big Data?



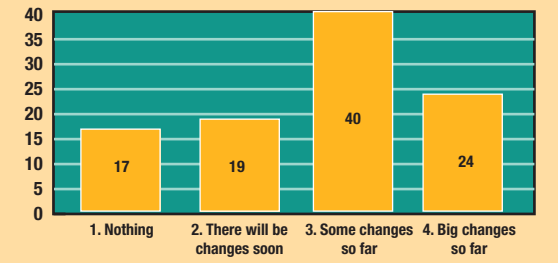
Source: Angel Serrano. Reprinted with permission.

Question 1: Is there anything new about big data (**figure 1**)?

The possible answers to this question were:

1. No, there is nothing new.
2. It is a fad, and it will all disappear when people realise nothing has changed.
3. It is new, but it is not going to change the world.
4. It is going to change the world.

Figure 2—Is Big Data Changing Your Business?



Source: Angel Serrano. Reprinted with permission.

Result: More than 60 percent of the audience believed that the change will be significant and, therefore, that drastic changes will happen in organisations' operations in the short term. Comments raised during the event indicated that the general feeling of the audience is that organisations that do not embrace big data soon may lose competitive advantages over competitors.

Question 2: Is big data changing your business (**figure 2**)?

The possible answers to this question were:

1. No changes so far, no changes soon.
2. No changes so far; there will be changes soon.
3. Some changes so far, but they are minor.
4. Big changes so far, more in the near future.

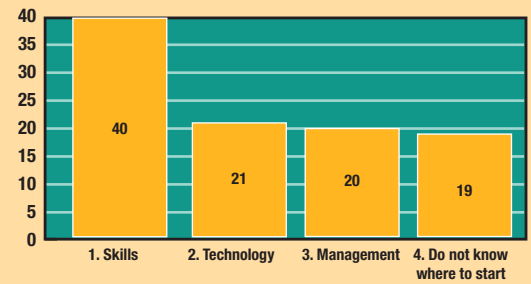
Result: Most of the people in the audience believed that there will be changes, but there were different opinions on how big those changes will be. Some of the comments indicated that there have been more changes in financial and telecommunication organisations than in the rest of the sectors.

Question 3: What will stop you from embracing big data (**figure 3**)?

The possible answers to this question were:

1. Skills
2. Technology
3. Management's disinclination to embrace it
4. Do not know where to start

Figure 3—What Will Stop You From Embracing Big Data?



Source: Angel Serrano. Reprinted with permission.

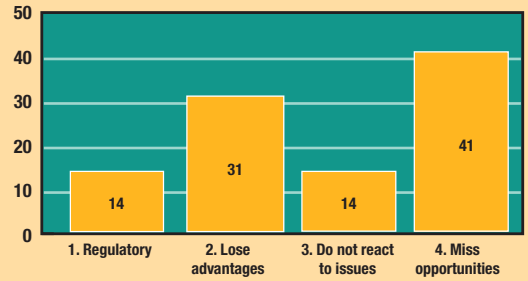
Result: It was broadly recognised that lack of skills is one of the key challenges to embracing big data. Most of the organisations represented in the audience do not have resources with the necessary capabilities to implement big data solutions. Comments from the audience revealed that organisations were trying to hire data analysts, but they were having difficulties finding candidates with the necessary expertise.

Question 4: What do you believe is the main risk of not embracing big data (**figure 4**)?

The possible answers to this question were:

1. Regulatory noncompliance
2. Lose advantages against competitors
3. Do not react to potential issues on time
4. Miss potential opportunities

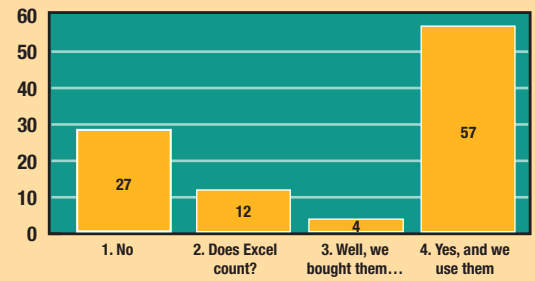
Figure 4—What Do You Believe Is the Main Risk of Not Embracing Big Data?



Source: Angel Serrano. Reprinted with permission.

Result: It was broadly recognised from the comments collected that the commercial side of big data and loss of potential opportunities were the main risk areas of not embracing big data in all sectors in general, whereas the regulatory risk factors were just recognized in financial services organizations.

Figure 5—Does Your Organisation Use Data Analytics Tools?



Source: Angel Serrano. Reprinted with permission.

Question 5: Does your organisation use data analytics tools (**figure 5**)?

The possible answers to this question were:

1. No
2. Does Excel count?
3. Well, we bought them, but we have not used them.
4. Yes, and we use them to analyse our data.

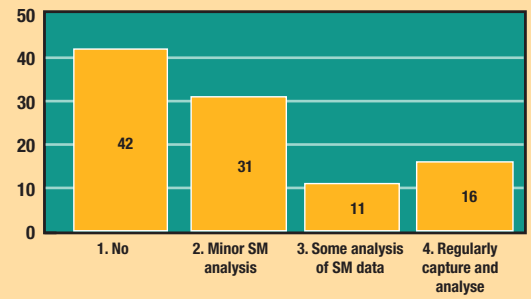
Result: More than half of the audience affirmed to have data analytics tools that they use to analyse data. Some of the comments raised indicated that those tools are usually managed by IT teams and they were not embedded in the business.

Question 6: Does your organisation collect social media data (e.g., Twitter, LinkedIn, Facebook) (**figure 6**)?
The possible answers to this question were:

1. No
2. Minor social media analysis. Our marketing people look at Twitter and Facebook.
3. We have done some analysis of social media data.
4. We regularly capture, analyse and act on social media data.

Result: The majority of the audience recognised that unstructured data (i.e., social media) are not collected nor used properly for further analysis in a robust process. Some comments from the audience reflected that their organisations are far away from using social media regularly.

Figure 6—Does Your Organisation Collect Social Media Data?



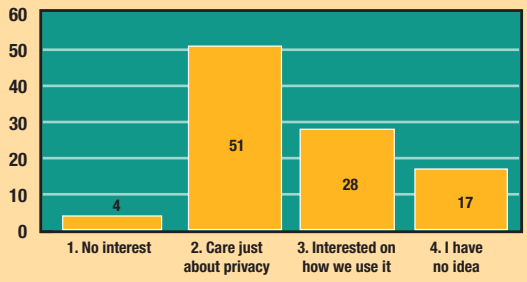
Source: Angel Serrano. Reprinted with permission.

Question 7: How do your customers feel about data issues (**figure 7**)?

The possible answers to this question were:

1. They have no interest in data issues.
2. They care only about privacy and security.
3. They are interested in how we use and profile our data.
4. I have no idea.

Figure 7—How Do Your Customers Feel About Data Issues?



Source: Angel Serrano. Reprinted with permission.

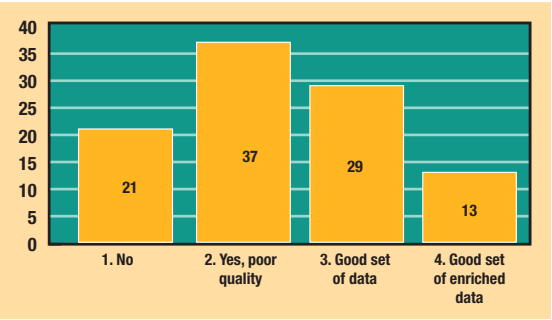
Result: Customer data privacy and security were key issues for the audience. The audience mentioned a couple of recent scandal examples and showed their concerns of managing big volumes of data with access from different applications and systems. The main concern was to control unauthorised access to all systems and applications and maintain those controls.

Question 8: Do you have the data you need (**figure 8**)?

The possible answers to this question were:

1. No.
2. Yes, but the quality is poor.
3. Yes, we have a good set of data.

Figure 8—Do You Have the Data You Need?



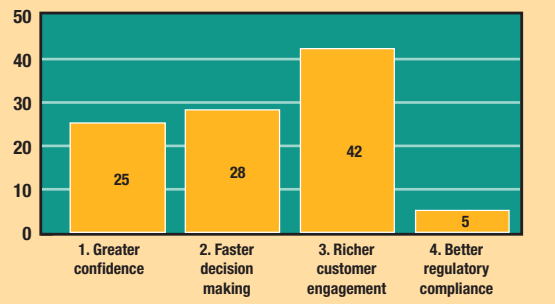
Source: Angel Serrano. Reprinted with permission.

4. Yes, we have a good set of data and we enrich it with external sources.

Result: There were some concerns among the audience about the impact of the quality of the data collected on the accuracy of the results obtained, particularly on the unstructured data. For most of the companies, this is the first time they are going through this process and, therefore, this was the main reason for those concerns.

Question 9: What do you think is the biggest advantage of big data (**figure 9**)?

Figure 9—What Do You Think Is the Biggest Advantage of Big Data?



Source: Angel Serrano. Reprinted with permission.

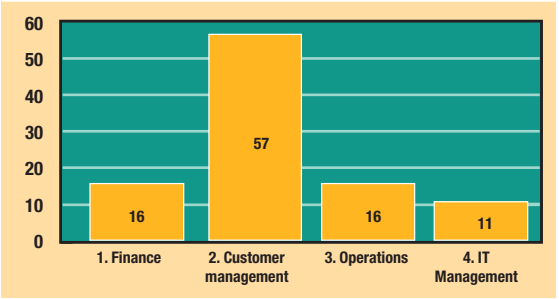
The possible answers to this question were:

1. Greater confidence in decisions
2. Faster decision making
3. Richer engagement with customers
4. Better regulatory compliance

Result: In line with the results of question 4, the commercial side of big data, as characterised by interaction with customers, is the key advantage for almost half of the audience.

Question 10: Where in your business do you believe that big data is going to have the biggest impact (**figure 10**)?

Figure 10— Where in Your Business Do You Believe That Big Data Is Going to Have the Biggest Impact?



Source: Angel Serrano. Reprinted with permission.

The possible answers to this question were:

1. Finance
2. Customer management/relations
3. Operations
4. IT management

Result: As indicated in questions 4 and 9, customer management is the area identified by the audience where big data can have the biggest impact.

Conclusion

During the event, there were table discussions and question and answer sessions, and most of the comments raised by the attendees were collected. It was broadly recognised that most of the companies have started to embrace big data; however, in the coming years there will be more changes in order to adapt business operations so they can handle larger volumes of data.

Enjoying this article?

- Read *Generating Value From Big Data Analytics.* *www.isaca.org/big-data-analytics*
- Learn more about, discuss and collaborate on big data in the Knowledge Center. *www.isaca.org/topic-big-data*

It was generally recognized through the survey that improvements in customer management and the identification of new opportunities will be the key advantages for companies that embrace big data. On the other hand, the biggest concerns about big data implementation were customers' data privacy and the impact of the quality of the data collected on the results' accuracy. Some of the recent scandals have raised the awareness in organisations and, therefore, security controls should be implemented around these technologies to avoid unauthorised access. Additionally, the lack of experience implementing these technologies could cause data quality issues, which may lead to inaccurate analysis. To avoid these issues, organisations should implement controls, such as reconciliations or validation tests, to ensure the validity of the information.

It was also recognised that the impact of big data in organisations depends on their sector. There were different views of the risk for companies from the financial sector and other sectors. Organisations from nonfinancial services did not consider regulatory requirements a key risk, whereas organisations from the financial sector did.

During the final debate, PwC mentioned some areas to consider before implementing these technologies. Those areas and some of the comments from the audience included:

- **Data strategy**—Organisations wishing to invest in significant data-led propositions need to understand the commitment required in terms of skills, infrastructure and software. A data strategy is required to set a course for how this may be achieved. This strategy should be aligned with the business and IT strategies and should focus on fulfilling business requirements.
- **Data analysis and management information**—As the volume of data proliferating in organisations continues to grow and data analysis tools become more sophisticated, there are significant opportunities for companies to enhance customer experience through the detailed analysis of data. This can range from increased understanding of customer behaviours to developing more sophisticated pricing structures and market positioning. It is critical for the success of the analysis to have the right tools and skills to manage the data collected.
- **Data governance**—Data governance policies, procedures and controls should be implemented in order to obtain the appropriate data quality levels. Organisations need to be able to use data with confidence in their integrity and quality and with the assurance that poor data are not feeding important analyses, the output of which may be driving important business decisions.
- **Data privacy**—The increase in the amount of data held by clients also represents an increase in the risk of a data privacy breach or contravention of the terms of the UK Data Protection Act of 1998 (DPA).
- **Capacity**—Organisations should ensure that systems and technology are able to support the volume of data necessary to analyse the volume of data required.
- **Skills**—Organisations should ensure that they have appropriate skills to manage the volume of data required now, and the appropriate recruiting process and training programs in place to improve the skills of personnel as technology changes.
- **Data architecture**—Organisations should consolidate all sources of data required for the analysis in a common data model such as a data warehouse. Data architecture design and extract, transform and load (ETL) processes are critical areas for the success of this common data model and should be assessed and included in the strategy.

How Boards Realise IT Governance Transparency

A Study Into Current Practice of the COBIT EDM05 Process

In our increasingly digitised economy, IT has become fundamental to support, sustain and grow organisations. Successful organisations leverage the potential of digital innovation and understand and manage the risk and constraints of technology.[1]

Previously, the governing board could delegate, ignore or avoid IT-related decisions, but the disruptions from new technologies (e.g., cloud, Internet of Things, big data) are increasingly being felt at the board level. Emerging research calls for more board-level engagement in enterprise governance of IT and identifies serious consequences for digitised organisations in case the board is not involved.[2] Yet, it appears that enterprise-technology governance competence remains the 'elephant in the boardroom' for more than 80 percent of boards of directors (BoDs).[3]

In this context, a co-created research project was established by the Antwerp Management School, Cegeka, KPMG and Samsung, to focus on the role of the BoD in governance of enterprise IT (GEIT). The 2015–2018 research project explores contemporary best practices and competencies for BoD involvement in IT to realise technological innovation potential and ensure control over the associated risk. By offering BoDs a clearer path to reach their IT governance objectives, the project aims to strengthen their involvement and obtain a true end-to-end GEIT.

> **"Successful organisations leverage the potential of digital innovation."**

This article reports on one of the investigations being done, specifically, how nonexecutive boards are reporting on their accountability for IT in their yearly reports. As such, it immediately relates to the COBIT® 5 Evaluate, Direct and Monitor (EDM) process EDM05 *Ensure stakeholder transparency,* which expects the board to 'make sure that the communication (on IT governance) to stakeholders is effective and timely and that the basis for reporting is established to increase performance'.[4]

From this research, it appears that, notwithstanding the pervasive role of IT, the disclosure on IT governance is still limited and rather focused on reactive elements—for example, in response to IT-related risk events happening. More reporting in high IT-intense sectors, as well as in publicly listed companies was observed. The latter is probably a result of investors being more willing to invest more in organisations that have their digitised assets under control.

Steven De Haes, Ph.D.
Is a full professor of information systems management at the University of Antwerp—Faculty of Applied Economics and at the Antwerp Management School (Belgium). He acts as the academic director of the IT Alignment and Governance (ITAG) Research Institute.

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

Tim Huygh,
Is a Ph.D. candidate in IT governance at the department of Management Information Systems of the Faculty of Applied Economics at the University of Antwerp (Belgium).

Salvi Jansen
Is a business engineer in management information systems and a consultant at KPMG Advisory in Belgium.

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 click on the Comments link to share your thoughts.

The research leads to the belief that as the dependency on IT continues to grow within all industries, IT governance disclosure might well become a critical piece of the nonfinancial information in most annual reports. As such, BoDs will become increasingly incentivised to disclose on the matter and will, therefore, demonstrate greater expectations for reporting by executive management toward them (e.g., IT performance/compliance reports, IT risk scenarios and events, IT value delivery). This research will supply examples from the field for boards and executive management to set up and operate an adequate disclosure strategy.

Why Governing Boards (Should) Provide Transparency Around IT Governance

In their 2014 empirical study, Turel and Bart[5] concluded that 'High levels of board-level IT governance, regardless of existing IT needs, increased organizational performance', clearly demonstrating the importance of BoDs taking up their accountability for IT. They concluded that boards should not shy away from governing and controlling the IT assets for their organisations to approach IT more strategically, identify overlooked opportunities and, ultimately, achieve superior performance in the digitised economy.

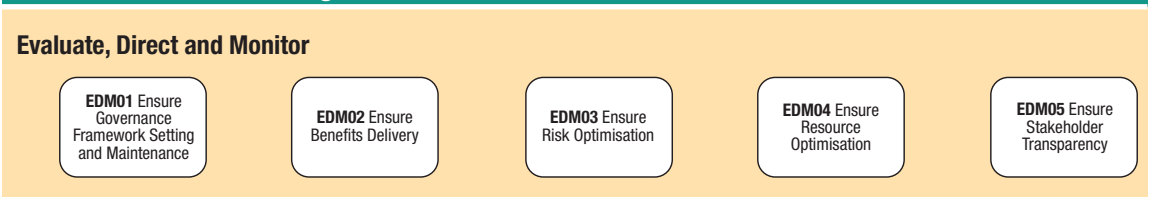
Next to such empirical findings, more theoretical research in IT governance has clearly advocated for the importance of IT governance communications to external stakeholders of the firm.[6, 7] This theoretical underpinning, rooted in voluntary disclosure theory and agency theory, predicts that firms can improve their liquidity and firm valuation through better information intermediation, enhance market reputation, and reduce both litigation costs and the cost of capital.[8]

Notwithstanding the empirically and theoretically demonstrated importance of IT governance disclosure, other studies point out that, on average, the involvement of boards in GEIT is low and that boards should become more IT-savvy to be able to govern the digitised organisation. Andriole published an article in this context in 2009 that reported on the 'surprisingly' low maturity of boards in this area.[9] Valentine concluded that less than 20 percent of corporate boards worldwide report having enterprise-technology-capable directors.[10]
In conclusion, boards need to extend their governance accountability from a single focus on finance and legal as proxy to corporate governance to include technology. In this way, they can provide digital leadership and organisational capabilities to ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives.

How COBIT 5 Stresses the Need for IT Governance Transparency

This conclusion was confirmed by ISACA® with the release of its COBIT 5 process model in 2012 (see *COBIT® 5: Enabling Processes*). In this overarching approach, COBIT 5 identifies 37 processes spread over a governance and a management domain. The five governance processes (**figure 1**) are the board's responsibilities in IT, covering setting the governance framework; handling responsibilities in terms of value (e.g., investment criteria), risk (e.g., risk appetite) and resources (e.g., resource optimisation); and providing transparency regarding IT to the stakeholders. The latter process addresses the key topic of this article, which COBIT describes as the process required 'to ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions'.[11]

Figure 1—COBIT 5 IT Governance Processes



Source: ISACA, COBIT 5, USA, 2012)

Research on IT Governance Transparency in Belgium

To gain insight into current IT governance transparency practices, researchers analysed the publicly available annual reports of 12 Belgian companies. The nonfinancial information on these reports was expected to contain information on IT governance practices as part of the overall corporate governance measures.

As the IT governance disclosure rate would unavoidably vary among the companies selected, the companies were clustered (**figure 2**) to deduce whether those within transform industries, in which IT profoundly alters traditional ways of doing business by redefining business processes and relationships, disclose more on IT governance as opposed to organisations in nontransform industries.[12] Secondly, researchers observed whether those that are publicly listed disclose more than those that are not, because they are incentivised to do so by the market. While testing both propositions, examples of language and narratives that could be considered as a good practice of IT governance disclosure were captured.

With regard to the rate and content of IT governance disclosure, the researchers were interested in knowing which topics make it into the annual reports and which do not. The framework used to determine the rate and content of the IT governance disclosure is one recently proposed in academic literature.[13] This disclosure framework proposes that nonexecutive boards can report on four areas of concern: IT strategic alignment, IT value delivery, IT risk management and IT performance management. In each of these domains, expected reporting items were derived from literature, as follows:

- For IT risk management, items on the information security plan and policy were expected.
- For IT performance management, explicit information on IT expenditure was captured.
- For IT value management, elements relating to IT project updates were sought.
- For IT strategic alignment, information was sought regarding the position of the chief information officer (CIO) and the existence of an IT steering committee.

Reporting rates were reviewed; hence, these results are by no means an indication of what really was present in the organisation, but only what was reported.

Research Observations

In general, a low average reporting rate on IT governance was observed. Firms report most in the domains of IT risk management and IT performance measurement (**figure 3**). Surprisingly, IT strategic alignment is the least disclosed category among the organisations in the sample. These results indicate that there is room for improvement in overall IT governance transparency in annual reports. Academic literature clearly suggests the potential benefits of disclosure on nonfinancial aspects in general and IT governance-related aspects in particular, providing firms with a clear incentive to consider increasing their IT governance disclosure.

As mentioned, the IT usage intensity within the industry (transform vs. nontransform) could have an impact on the IT governance disclosure rate. By comparing the transform and nontransform groups of companies (while keeping their reporting context the same—all listed companies in Belgium), a difference in the overall disclosure rate was

Figure 2—IT Governance Disclosure Research Sample

Transform Industries, Listed	Nontransform Industries, Listed	Transform Industries, Not Listed
ING (banks)	CFE (construction and materials)	Argenta (banks)
KBC (banks)	Deceuninck (construction and materials)	Belfius Bank (banks)
Delta Lloyd (insurance)	Saint-Gobain (construction and materials)	Bank Degroof (banks)
Mobistar (mobile telecommunications)	Nyrstar (industrial metals and mining)	Keytrade Bank (banks)

Source: S. De Haes, A. Joshi, T. Huygh, S. Jansen. Reprinted with permission.

determined. Transform listed companies had an average reporting rate of 35 percent, whereas nontransform listed companies were at 14 percent.

With an overall disclosure rate of 35 percent to 26 percent (all transform Belgian companies), listed companies have a better overall disclosure rate than companies not listed. The reasons for this can be found in prior research, which states that disclosing nonfinancial information can improve a firm's valuation on the stock market. This incentivises companies to explicitly mention practices with a known valuation impact such as having a dedicated CIO[14] or investing in IT (when in a transform industry).[15]

Figure 3—IT Governance Disclosure Realised

IT Governance Disclosure Domain	Average Reporting Rate*
IT strategic alignment	Low (8%)
IT value delivery	Low (24%)
IT risk management	Medium (35%)
IT performance measurement	Low (32%)

0-33%: Low reporting
34-66%: Medium reporting
67-100%: High reporting

* Average reporting rate based on the average percentage of organisations reporting in a specific disclosure area, within three categories of measures.

Source: S. De Haes, A. Joshi, T. Huygh, S. Jansen. Reprinted with permission.

A Call to Action for Governing Boards

When considering the potential valuation impact of IT and the relatively unexplored nature of IT governance at the corporate level, this type of research can be valuable to governing boards and executive committees to establish the right questions to ask their direct reports. Chances are high that practices are in place that are not reported on, which is a missed opportunity to convince stakeholders of the governance system. Formalised practices will enable boards and executive committees to take preventive action, detect deficiencies and take mitigating action, enabling them to show that they are, indeed, in control of IT at a strategic level.

This research on the annual reports of Belgian companies showed that IT governance disclosure is generally rather low and might be indicative of the IT governance maturity at the executive and/or nonexecutive level. As IT risk and IT opportunities continually increase and stakeholders rely on nonfinancial information given to them to valuate the firm, BoDs and executive committees are incentivised to take up their IT governance role and report on it.

A high degree of board involvement in IT governance has a positive effect on organisational performance (internal perspective), and the general principle of reporting nonfinancial information, as well as certain IT governance practices, is known to have a positive effect on the valuation of a firm (external perspective). A convincing case can be made that further analysis will enable researchers to identify more good practices, provide benchmarking information to determine an ambition level suitable to the individual context of each firm, and establish a formal set of practices that can be implemented to enable better organisational performance and reporting that satisfies stakeholder needs.

Endnotes

1 De Haes, S.; W. Van Grembergen; *Enterprise Goverance of IT: Achieving Alignment and Value, 2nd Edition*, Springer, USA, 2015
2 Turel, O.; C. Bart; "Board-level IT Governance and Organizational Performance," *European Journal of Information Systems*, vol. 23, March 2014, p. 223-239
3 Valentine, E; *Enterprise Business Technology Governance: New Core Competencies for Boards of Directors in Digital Leadership*, Queensland University of Technology, Brisbane, Australia, 2015
4 ISACA, *COBIT® 5: Enabling Processes*, USA, 2012, *www.isaca.org/COBIT/Pages/Product-Family.aspx*
5 *Op cit*, Turel and Bart
6 Gordon, L. A.; M. P. Loeb; T. Sohail; "Market Value of Voluntary Disclosures Concerning Information Security," *MIS Quarterly*, vol. 34, no. 3, 2010, p. 567-594

7 Raghupathi, W; "Corporate Governance of IT: A Framework for Development," *Communications of the ACM*, vol. 50, no. 8, 2007, p. 94-99
8 Healy, P. M.; K. G. Palepu; "Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure ILterature," *Journal of Accounting and eEconomics*, vol. 31, iss. 1, 2001, p. 405-440
9 Andriole, Stephen J.; "Boards of Directors and Technology Governance: The Surprising State of the Practice," *Communications of the Association for Information Systems*, vol. 24, article 22, March 2009
10 *Op cit*, Valentine
11 ISACA, *COBIT® 5: Enabling Processes*, USA, 2012, *www.isaca.org/COBIT/Pages/Product-Family.aspx*
12 Anderson, M. C.; R. D. Banker; S. Ravindran; "Value Implications of Investments in Information Technology," *Management Science*, vol. 52, iss. 9, 1 September 2006, p. 1359-1376, *http://pubsonline.informs.org/doi/abs/10.1287/mnsc.1060.0542*
13 Joshi, A.; L. Bollen; H. Hassink; "An Empirical Assessment of IT Governance Transparency: Evidence From Commercial Banking," *Information Systems Management*, vol. 30, iss. 2, 2013, p. 116-136
14 Chatterjee, D.; V. J. Richardson; R. W. Zmud; "Examining the Shareholder Wealth Effects of Announcements of Newly Created CIO Positions," *MIS Quarterly*, vol. 25, no. 1, March 2001, p. 43-70
15 Dehning, B; V. J. Richardson; R. W. Zmud; "The Value Relevance of Announcements of Transformational Information Technology Investments," *MIS Quarterly*, vol. 27, no. 4, December 2003, p. 637-656

crossword puzzle

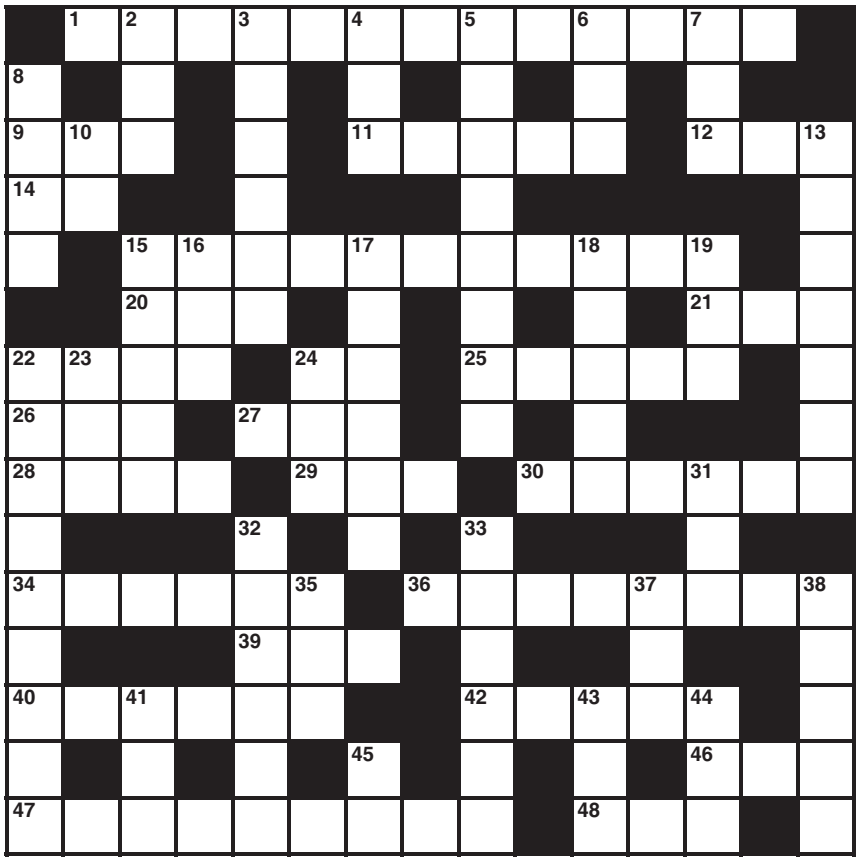
by Myles Mellor
www.themecrosswords.com

ACROSS

1 It is often thought to be the basis for access control, goes with 5 down
9 Type of cyberattack, abbr.
11 Tracks left by malware attacks, goes with 33 down
12 IT equipment that can be single-sided, double-sided or multilayer, abbr.
14 Greek country code
15 Bona fides
20 Word before flag
21 No longer used
22 Snail-like communication
24 Height, (abbr.)
25 Author of *The Black Swan: The Impact of the Highly Improbable*
26 "____ a Trojan Horse!"
27 Standard
28 High-___ (cutting-edge)
29 Ogburn's cultural ___ thesis
30 Short-sightedness
34 One followed by 100 zeros
36 First chairman of the US National Commission on Fraudulent Financial Reporting
39 Peak
40 Father of computer science, whose life was portrayed in *The Imitation Game*
42 Word used with dilemma and choices
46 Part of OPEC
47 Removes sensitive information from a document
48 Network of physical objects connecting electronic devices, abbr.

DOWN

2 Increases, as an amount
3 Minimized loss, in some way
4 Gist
5 See 1 across
6 Include
7 Business management software, abbr.
8 Trendsetting
10 Alternative intro word
13 Type of architecture that provides the ever-expanding volume of information that is essential to malware detection and analysis, 2 words



15 Important certification for an IS auditor, abbr.
16 Relative, for short
17 Snare
18 Relieve concerns
19 Gasping cry
22 Lessens the seriousness of
23 Eroded, with into
24 Famous film computer
31 Cats___ (person used by another as a tool)
32 Compromised computers running on automatic
33 See 11 across
35 Record
37 It has come to mean the core of a company's culture or production emphasis
38 Product
41 Kind of command
43 Profit
44 Auction segment
45 It is Down Under, abbr.

Answers on page 58

quiz #166

Based on Volume 1, 2016
Value: 1 Hour of CISA/CISM/CGEIT/CRISC Continuing Professional Education (CPE) Credit

TRUE OR FALSE

BRAGA ARTICLE

1 The COBIT® 5 Assessment Programme incorporates the COBIT 5 Process Reference Model and ISO/IEC 27110 as the basis for the measurement framework and assessment process.

2 Capability level 1 indicators are specific for each process and assess whether the implemented process achieves its process purpose.

3 At level 3, process documentation has to specify who is responsible for its design (process owner) and its scope; roles; Responsible, Accountable, Consulted and Informed (RACI) chart; and internal control matrix.

KRESS ARTICLE

4 Accenture is a global giant in technology services with more than 500,000 professionals.

5 In the Accentures case, the team increased the number of IT audits provided by more than 250 percent between 2012 and 2015.

6 While digital technology enabled many of the performance improvements, just as critical are the changes in mind-set that were made throughout the process.

7 One lesson learned is to make cautious decisions to drive step-driven increases in the enterprise's capabilities.

COE ARTICLE

8 The *Global State of Information Security Survey* in September 2014 shows that as information risk factors have evolved, security strategies have kept pace.

9 The US National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organization identifies 198 security practices.

10 Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, directs NIST to work with stakeholders to develop a voluntary framework for reducing cyberrisk to critical infrastructure.

KORPELA ARTICLE

11 Data visualization is about being simple and representing data effectively.

12 A bubble chart is an engaging way to visualize the frequency distribution of words with textual data.

13 A heat map is a grouping of line charts copied and pasted together.

14 A doughnut chart is basically a pie chart with a hole in the middle.

CPE quiz

Prepared by
Kamal Khan
CISA, CISSP,
CITP, MBCS

Take the quiz online

CPE quiz #166

THE ANSWER FORM

Based on Volume 1, 2016

TRUE OR FALSE

BRAGA ARTICLE

1. _____
2. _____
3. _____

COE ARTICLE

8. _____
9. _____
10. _____

KRESS ARTICLE

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

KORPELA ARTICLE

11. _____
12. _____
13. _____
14. _____

Name _____

PLEASE PRINT OR TYPE

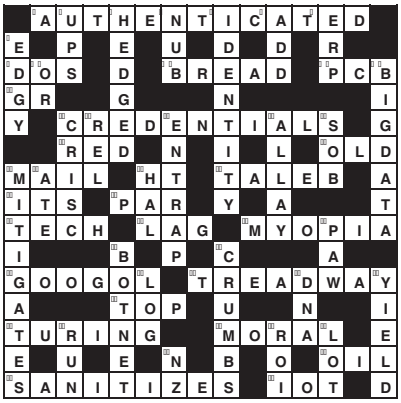
Address _____

CISA, CISM, CGEIT or CRISC # _____

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.



standards guidelines tools and techniques

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.

Please note that the new guidelines are effective 1 September 2014.

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

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)

Please note that the new guidelines are effective 1 September 2014.

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

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

Reporting
2401 Reporting
2402 Follow-up Activities

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 programs, 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*.

Prior to issuing any new Standard or Guideline, an exposure draft is issued internationally for general public comment.

Comments may also be submitted to the attention of the Director of Privacy and Assurance Practices 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*.

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 these products 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.

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

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

ISSN 1944-1967

Subscription Rates:

US:
one year (6 issues) $75.00

All international orders:
one year (6 issues) $90.00.

Remittance must be made in US funds.

advertisers/web sites

Capella University	*capella.edu/ISACA*	3
Chiron Technology Services	*chirontech.com*	Back Cover
Hiscox USA	*hiscox.com/bigideas*	1
International Cyber Security & Intelligence Conference	*www.icsic.ocmtontario.ca/registration*	17

leaders and supporters

ISACA®
Trust in, and value from, information systems

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

www.isaca.org/bookstore

NOW AVAILABLE!

A Practical Guide to the Payment Card Industry Data Security Standard (PCI DSS)

by ISACA

Print Product Code: APG

Web Download Product Code: WAPG

Member/Nonmember: $35.00/$60.00

This book explains the security requirements, processes and technologies that are required to implement the Payment Card Industry Data Security Standard (PCI DSS) which is a compliance requirement for all enterprises that process, store, transmit or access cardholder information for any of the major payment brands, such as American Express®, Discover®, JCB, MasterCard® and VISA® brands.

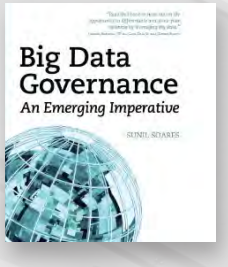
The guide provides a comprehensive overview of the PCI DSS and explains how to implement its demanding security requirements. The guide also contains a wealth of background information about payment cards and the nature of payment card fraud. The content in this guide goes beyond explaining the requirements by providing the following valued information:

- Concise summaries of the most current PCI DSS requirements *Version 3.1* (just released in 2015)
- Consolidated information from numerous PCI Council publications to help the reader better understand the true scope of payment card security
- Techniques to determine the scope of compliance, documenting cardholder data flows and defining the Cardholder Data Environment
- Provides guidance on implementing controls to comply with all 12 PCI DSS requirements and maintain compliance
- PCI DSS requirements mapped to COBIT® 5 processes and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 270012 controls
- Detailed explanation of compliance requirements for third-party services and cloud computing providers

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

Big Data Governance, An Emerging Imperative

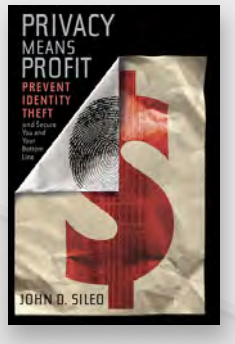


by Sunil Soares

Product Code: 1MCBD
Member/Nonmember:
$41.00/$51.00

Big data includes content from sources such as social media, telephone GPS signals, utility smart meters, RFID tags, weather monitors, and other sources. Such data tends to be operational in nature and is characterized by the "three V's": large volume, high velocity, and a variety of formats, including structured, unstructured, and semi-structured. A growing number of books address the topic of big data, but none deals with the challenge of governing big data. Yet big data governance is a crucial enabler to derive maximum value from a big data program. *Big Data Governance* addresses this knowledge gap, examining the industry imperatives that are driving the convergence of these two major trends in Information Management and explaining not only the why but the how of governing big data.

Privacy Means Profit: Prevent Identity Theft and Secure You and the Your Bottom Line



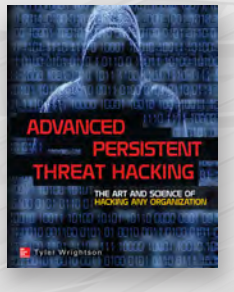
by John Sileo

Product Code: 1WPMP
Member/Nonmember:
$15.00/$25.00

Bulletproof your organization against data breach, identity theft, and corporate espionage.

In this updated and revised edition of *Privacy Means Profit*, John Sileo demonstrates how to keep data theft from destroying your bottom line, both personally and professionally. In addition to sharing his gripping tale of losing $300,000 and his business to data breach, John writes about the risks posed by social media, travel theft, workplace identity theft, and how to keep it from happening to you and your business.

Advanced Persistant Threat Hacking: The Art and Science of Hacking Any Organization



by Tyler Wrightson

Product Code: 43MAP
Member/Nonmember:
$34.00/$44.00

Master the tactics and tools of the advanced persistent threat hacker.

In this book, IT security expert Tyler Wrightson reveals the mindset, skills, and effective attack vectors needed to compromise any target of choice. *Advanced Persistent Threat Hacking* discusses the strategic issues that make all organizations vulnerable and provides noteworthy empirical evidence. You'll learn a proven APT Hacker Methodology for systematically targeting and infiltrating an organization and its IT systems. A unique, five-phased tactical approach to APT hacking is presented with real-world examples and hands-on techniques you can use immediately to execute very effective attacks.

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

Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises

by ISACA

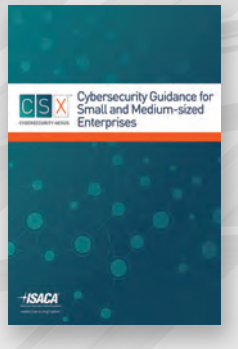
Print Product Code: CSXI

PDF Product Code: WCSXGI

Member/Nonmember: $35.00/$60.00

Cybersecurity is a topic of interest for most enterprises, regardless of their size. Cybercrime and cyberwarfare are not restricted to large, multinational enterprises. Increasing numbers of small and medium-sized enterprises (SMEs) are being targeted. In an SME context, information security and cybersecurity are often difficult to implement in a satisfactory and cost-effective manner. SMEs need hands-on guidance for affordable and effective cybersecurity. ISACA's *Cybersecurity Guidance for Small and Medium-sized Enterprises* and this *Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises* are designed to meet the needs of typical SMEs: reasonable security at affordable cost. These publications help SMEs to prepare for, and manage, typical cybersecurity issues, risk and threats

Cybersecurity Guidance for Small and Medium-sized Enterprises



by ISACA

Print Product Code: CSXE

PDF Product Code: WCSXGE

Member/Nonmember: $35.00/$60.00

Cybersecurity is rapidly becoming a critical activity in many enterprises, due to the increasing number of cyberattacks and cybercrime. Cyberattacks often target small and medium-sized enterprises, because cybercriminals expect information in SMEs to be less protected than in large enterprises. Protection against cyberattacks is an important element in ensuring that SMEs can protect their economic interests, reputation and intellectual property, and the information assets of their customers and business partners.

Build A Security Culture

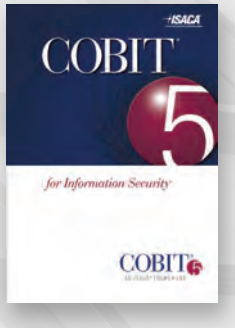
by Kai Roer

Product Code: 22ITGB
Member/Nonmember: $18.00/$28.00

Human Nature—Easy Prey for Hackers? Human behavior is complex and inconsistent, making it a rich hunting ground for would-be hackers and a significant risk to the security of your organization . An effective way to address this risk is to create a culture of security. Using the psychology of group behavior and explaining how and why people follow social and cultural norms, the author highlights the underlying cause for many successful and easily preventable attacks.

An effective framework for behavioral security. In this book Kai Roer presents his Security Culture Framework, and addresses the human and cultural factors in organizational security. The author uses clear, everyday examples and analogies to reveal social and cultural triggers that drive human behavior. He explains how to manage these threats by implementing an effective framework for an organizational culture, ensuring that your organization is set up to repel malicious intrusions and threats based on common human vulnerabilities.

COBIT 5 for Information Security



by ISACA

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

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

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

Secrets and Lies: Digital Security in a Networked World, 15th Anniversary Edition

by Bruce Schneier

Product Code: 115WSL
Member/Nonmember: $24.00/$34.00

This anniversary edition which has stood the test of time as a runaway best-seller provides a practical, straight-forward guide to achieving security throughout computer networks. No theory, no math, no fiction of what should be working but isn't, just the facts. Known as the master of cryptography, Schneier uses his extensive field experience with his own clients to dispel the myths that often mislead IT managers as they try to build secure systems. A much-touted section: Schneier's tutorial on just what cryptography (a subset of computer security) can and cannot do for them, has received far-reaching praise from both the technical and business community.

CyberSecurity and Cyberwar—What Everyone Needs to Know

by P.W. Singer and Allan Friedman

Product Code: 20X
Member/Nonmember: $17.00/$27.00

A generation ago, "cyberspace" was just a term from science fiction, used to describe the nascent network of computers linking a few university labs. Today, our entire modern way of life, from communication to commerce to conflict, fundamentally depends on the Internet. And the cybersecurity issues that result challenge literally everyone: politicians wrestling with everything from cybercrime to online freedom; generals protecting the nation from new forms of attack, while planning new cyberwars; business executives defending firms from once unimaginable threats, and looking to make money off of them; lawyers and ethicists building new frameworks for right and wrong. Most of all, cybersecurity issues affect us as individuals. We face new questions in everything from our rights and responsibilities as citizens of both the online and real world to simply how to protect ourselves and our families from a new type of danger. And yet, there is perhaps no issue that has grown so important, so quickly, and that touches so many, that remains so poorly understood.

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

infosecurity®

EUROPE

7-9 JUNE 2016 OLYMPIA. LONDON.

INTELLIGENT SECURITY:
SECURING THE CONNECTED ORGANISATION

Collect **CPE/CPD** credits

Everyone & everything you need to know about information security

Rather than taking our word for it, look at the facts below:

- **98%** of visitors were satisfied attending Infosecurity Europe 2015
- **93%** satisfied exhibitors with 80% rebooking at the exhibition
- **160 hrs** of free seminars and workshops for 2016
- **315+** vendors and service suppliers delivered a diverse range of new products and services
- **ROI £1.39+ bn** of estimated future orders, visitors expect to place with exhibitors as a result of attending Infosecurity Europe
- **4,435** professionals earned CPD / CPE credits

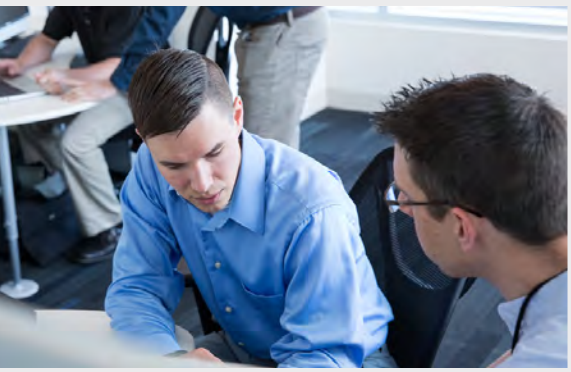
REGISTER FREE NOW

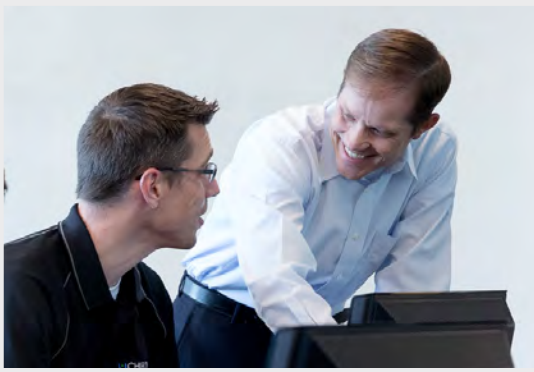
www.infosecurityeurope.com

Part of: infosecurity® GROUP

Organised by: Reed Exhibitions®

TRAIN LIKE YOU FIGHT





CHIRON'S TEAM OF EXPERT INSTRUCTORS BRING YEARS OF RELEVANT, REAL-WORLD EXPERIENCE INTO THE CLASSROOM.

Chiron's cyber protection program trainees are challenged and tested with real-world scenarios based on today's dynamic, agile and constantly evolving threat environment. Unlike simulated training, Chiron's classes are held in a laboratory setting unrestricted by rigid network security constraints that hamper the hands-on learning experience.

Our customized training approach creates qualified Information Operations professionals that are tested and equipped to handle the real-life cyber threats of today.

- OFFENSIVE AND DEFENSIVE CYBER OPERATIONS
- ADVANCED THREAT SIMULATION
- NETWORK FORENSICS AND THREAT ANALYSIS
- MALWARE REVERSE ENGINEERING
- SIMULATED TRAINING ENVIRONMENT

LEARN MORE ABOUT OUR TRAINING:

410-672-1522, ext. 113 | training@chirontech.com

or visit chirontech.com

CHIRON