Volume 5, 2016

ISACA Journal

How to Audit the Human Element and Assess Your Organization's Security Risk

Cyberinsurance: Value Generator or Cost Burden?

An Integrated Approach for Cyberthreat Monitoring Using Open-source Software

www.isaca.org

ISACA®

Trust in, and value from, information systems

CYBER STRONG.

Claim your future in the high demand Cybersecurity and information assurance/security fields. Students will be educated in the technical aspects of Cybersecurity systems and will be prepared for the management, operations and oversight of these systems.

Classes are forming now in our state-of-the-art Cybersecurity laboratory and online.

SAINT LEO UNIVERSITY®

Saint Leo University offers competitive degree programs designed to train students in the field of cybersecurity.
B.S. Computer Science - Information Assurance
B.S. Cybersecurity
M.S. Cybersecurity

800.707.8846 | SaintLeo.edu

National Security Agency and the Department of Homeland Security have designated Saint Leo University as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) through academic year 2021.

Society of Corporate Compliance & Ethics 15th Annual

COMPLIANCE & ETHICS INSTITUTE

SEPTEMBER 25-28 | SHERATON GRAND | CHICAGO

REGISTER NOW

IT COMPLIANCE TRACK

COVERING MORE THAN A DOZEN COMPLIANCE TOPICS RELATED TO IT

Learn more and register at **complianceethicsinstitute.org**

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 September and October 2016.

The Soft Skills Challenge, Part 5
Ed Gelbstein, Ph.D., and Stefano Baldi

Information Systems Security Audit
Shemlse Gebremedhin Kassa, CISA, MSCS

Cyberattacks: The Instability of Security and Control Knowledge
Jeimy Cano, Ph.D., CFE

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* blog, Practically Speaking, to gain practical knowledge 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

Unsung Security Heroes

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.

Long ago and far away, I was the president of the EDP Auditors Association, which, some years later, changed its name to ISACA®. So here we are, 35 years after my term in office, and I marvel at what ISACA has become: 140,000 constituents in more than 200 chapters in 180 countries. One of the things I am most proud of in today's association is the breadth of its membership and the community it serves. Still having a base in IS/IT auditing, ISACA now encompasses consultants, educators, IS security professionals, risk professionals, chief information officers and internal auditors.[1]

It has been said that those who are professionally interested in the security and control of information systems, primarily IS auditors, have an adversarial relationship with the information technology function.[2] I do not think this is necessarily true or necessary at all. My experience, at least in the last decade or so, is that there are many in the ranks of IT professionals who are significant contributors to information security and who ought to be recognized as such.

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.*

Database Administrators

If there is any one attribute of information security that is universally recognized, it is control over access to data. According to one writer, "the database administrator (DBA) has three basic tasks. In decreasing order of importance, they are: protect the data, protect the data, and protect the data."[3] DBAs, or perhaps more specifically, data administrators, define the rules for data in the form of metadata. These set the policies for the use of data, in terms of the ownership of elements, usage by applications (and, by extension, people), and permissions to access, change or delete data.[4] All of that sounds very much like information security to me.

System Administrators

When a system has many users, someone must be responsible for installation, support and maintenance of that system. That person is known as a system administrator (sysadmin) and has wide-ranging authority for the contents, capabilities and performance of servers, network devices and other configuration items. It is understandable that those whose interests lie in information security should be wary of sysadmins, given the power they have over the storage and use of data. But sysadmins are, or should be, the first to know when a system acts strangely or fails.[5]

In my experience, sysadmins are very protective of their domains and very focused on the security and continued operations of the devices and software they support. So, despite their potential to undermine security, they are often the very ones who make sure security is working.

Disaster Recovery Planners

Sometimes, despite all security measures, systems fail. When the cause is physical in nature, we call it a disaster, and when a disaster befalls a data center,

it is the disaster recovery planner who should have developed the procedures for restoring operations, usually at an alternate location. This person must have a broad understanding of infrastructure and applications in order to effectuate recovery within management's tolerance for downtime and data loss.

> **"In and of itself, disaster recovery is an aspect of information security."**

In and of itself, disaster recovery is an aspect of information security. Moreover, disaster recovery planners need to maintain access control, intrusion detection and other safeguards in the restored environment at the same level as in normal operations. Consequently, they have many attributes that make them participants in the management of information security.

Business Continuity Managers

Closely aligned (and allied) with disaster recovery planners are business continuity planners. Where the former prepare for recovery of IT operations, the latter ensure that business activities can continue at some acceptable level while systems are down. In instances in which no downtime is acceptable from a business perspective, the business continuity manager becomes the advocate for the end users in dealing with IT management.

Some would question whether business continuity management is an information security function at all. For many years, the basic global security standard, ISO 27001, defined business continuity management as a component of security. In the 2013 version, with the publication of ISO 22301 as a parallel business continuity management standard, the focus has shifted to maintaining security in recovery situations.[6]

Procurement Personnel

In our interconnected age, it is widely recognized that the security and recoverability of third parties are critical elements of information security. When systems in the form of products and services are purchased, it should be clear that the requirements for security are as high as those for systems developed internally— perhaps more so, inasmuch as the acquiring organization has little or no control over the vendor's development practices.

The person who is best positioned to insist on built-in security is the procurement manager. I will leave it to a future article to consider how this person, presumably without deep IT or security skills, might understand an organization's security requirements or recognize whether or not they are met. Nonetheless, procurement managers can be instrumental in achieving a consistent level of security across an enterprise.

Project Managers

Even if a system, whether acquired or developed internally, has the best security controls, those controls may be meaningless if not implemented properly. Sizable projects—and implementing systems is almost always a significant project—require capable project managers. It is these project managers who ensure that systems are put in place the right way, using the right methods and controls, meeting the owners' requirements, and, oh yes, on time and within budget. Somewhere in their mandate, project managers must make sure that security has been properly embedded in the systems.

Project managers should have the knowledge and skills to relate to all the security requirements of the system project they are overseeing. This requires an understanding of how the system in question meets those requirements and how the way that a system is implemented supports (or fails to support)

Enjoying this article?

- **Learn more about, discuss and collaborate on business continuity/ disaster recovery planning in the Knowledge Center.** *www.isaca.org/topic-business-continuity-disaster-recovery-planning*

security. Project managers must think broadly, considering not only the security of the subject system, but all the other systems running in the same environment, which, increasingly, means the entire application and infrastructure portfolio.

That is why those of us who do have some depth of information security knowledge must work with project managers and all the other professionals mentioned above, with a mutually respectful (and nonadversarial) relationship. Bringing all the skills together can only enhance an organization's security and the quality of the overall IT environment. So if you want to do something to foster information security, consider taking a project manager to lunch. And next week, a DBA. And after that, a sysadmin…

Who knows, maybe you can convince them to join ISACA.

Endnotes

1 ISACA, Membership, Guidance and Certification for IT Professionals, *www.isaca.org/About-ISACA/What-We-Offer-Whom-We-Serve/Pages/default.aspx*

2 Singleton, T.; "Why Everyone Dislikes the IT Auditor and How to Change It," *ISACA® Journal*, vol. 1, 2016, *www.isaca.org/Journal/archives/Pages/default.aspx*

3 Watkins, B.; "What Does a DBA Do All Day?," *Enterprise Cloud*, 26 June 2008, reprinted in *Tech Republic*, *www.techrepublic.com/blog/the-enterprise-cloud/what-does-a-dba-do-all-day/*

4 Cox, T. B.; "The Role of the Database Administrator," *Computer Weekly*, March 2000, *www.computerweekly.com/feature/White-Paper-The-role-of-the-database-administrator*

5 Gite, V.; "What Is the Role of the System Administrator?," nixCraft, 20 February 2006, *www.cyberciti.biz/faq/what-is-the-role-of-the-system-administrator/*

6 Verry, J.; "Is ISO 27001:2013 Clarification of Business Continuity Driving ISO 22301 Certification?," *PivotPoint Security*, 14 November 2013, *www.pivotpointsecurity.com/blog/iso-27001-2013-business-continuity-iso-22301/*

IS audit basics

The Soft Skills Challenge, Part 4

Mind Mapping

Many years ago during a rainy November evening in London, England, I decided to browse a bookshop to keep dry and warm and also see what had been released recently.

In the psychology section, there was a fairly thin book bearing a shiny cover and containing loads of drawings. It was called *The Mind Map Book*,[1] advertised in later editions as enabling the reader to "unlock your creativity, boost your memory, change your life." Good marketing, of course and, given that most books are one of the least expensive luxuries in life, well worth a purchase.

The book was very interesting, but it took time and some practice to appreciate its value. This column is a bit of an experiment, consisting as it does of a few illustrations (every one a mind map) and minimal text, all based on the book.

The mind map technique (**figure 1**) is not a silver bullet or a magic potion that will solve all the challenges of life. Instead, it is designed to help the user focus on one topic (the "would you like to" in **figure 1**) and link to it those things considered most relevant using as few words as possible and, most important, get it all done in just one page.

Figure 1—Benefits of Mind Mapping

Source: E. Gelbstein. Reprinted with permission.

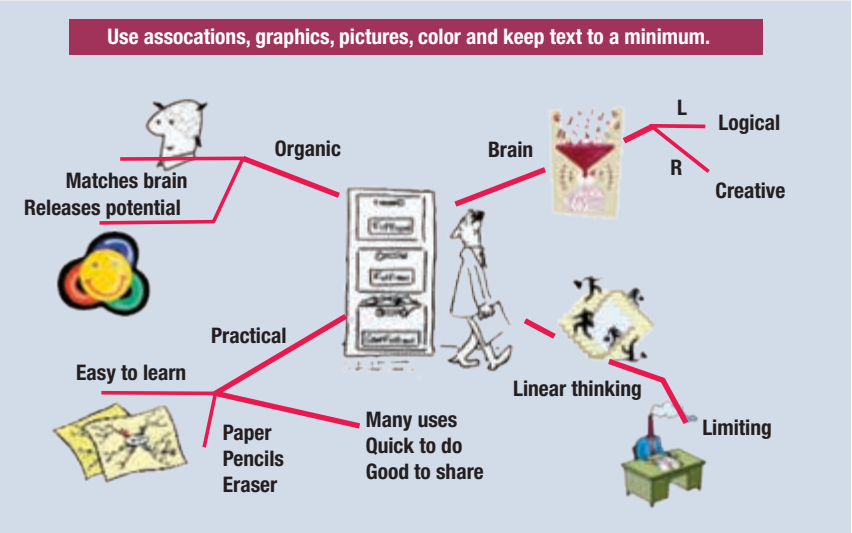
A familiar example might be to mind map "how to recruit a new IS auditor." Readers of this article can quickly come up with many issues that are pertinent to this objective, e.g., areas of specialization, qualifications, experience, the business case. By placing "recruit new IS auditor" in the center of a page, preferably in landscape, it becomes possible to group the issues just listed, relate them, check

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.

Stefano Baldi
Is an Italian career diplomat and an early adopter of information systems and communications as well as a driving force for the more extensive use of online learning. Baldi is the director of training at the Italian Ministry of Foreign Affairs. His diplomatic postings have included serving as the permanent representative of Italy at the UN in Geneva, Switzerland; and, subsequently, New York City, New York, USA, and at the European Union in Brussels, Belgium. Baldi has authored and coauthored several books on diplomacy-related topics and, with Gelbstein, has run courses for diplomats from around the world on topics such as information management and information security.

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.

Figure 2—Turning Mind Mapping Into "Play"



Source: E. Gelbstein. Reprinted with permission.

them for completeness and share the result with others. A fully developed mind map on "recruit a new IS auditor" can be found in later in this article.

These are the associations the mind map creator's brain has with "recruit a new IS auditor." Other people could have totally different ones, and comparing them may reveal some interesting topics to discuss further.

If discussions or further reflection show that something has been missed, it can easily be added. In this way, all the thoughts that were already floating in the mind of the map's creator are now organized in a visible and meaningful way. Having this organized view can then help to make informed decisions and understand the potential complexities that may arise (i.e., agreement of the human resources [HR] function, budget issues) and the many choices to be made (i.e., to employ or contract out, importance of soft skills).

And what has this to do with memory? The answer is simple, but not obvious: The brain is a visual organ and easily remembers pictures and diagrams. Reading linear text is an "unnatural" act as the characters need to be processed individually because they are arbitrary allocations of a shape to a sound. Making an effort to read text in an unfamiliar alphabet will make this concept clear.

I have used the technique when writing an article or preparing a presentation. The process takes three steps:

1. A fairly quick mind map with very few words (it does not matter if it is done by hand or using software}
2. Revision and ordering for good flow
3. Transition into text or presentation pages (again using as few words as possible)

This turns out to be a great time saver and leads to a "right first time, every time" result.

Going Further

Once learned, mind mapping is easy to do, and practice makes perfect. Therefore, it is good to indulge the "inner child" in all of us and use crayons or colored pencils to do sketches and ensure that both sides of the brain (the logical and the artistic) are engaged (**figure 2**).

This stimulates the creative process, encourages making associations between things that may appear unrelated and encourages the designer to think freely about the topic in focus.

Those who use this approach are likely to be surprised by the number of times someone looking at the elements in a mind map says, "I would not have thought of that."

Things to Do Using Mind Mapping

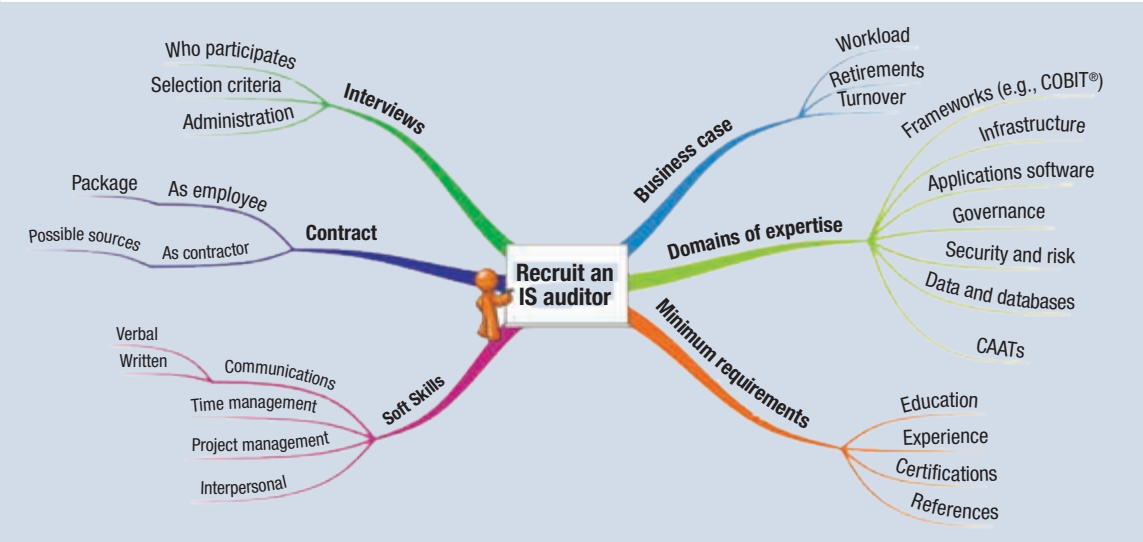
Mind mapping is a very individual activity as it relates to how associations are made in a person's mind. One thing is certain: At least one of the examples listed here could be useful in the professional activities of many people. It is important to not be concerned if at first others regard the activity as strange. Those unfamiliar with mind mapping may well decide to learn the technique once they see how useful it can be for endeavors including:

- **Note taking**—This becomes more effective than the traditional approach. Each idea can be placed where it fits, regardless of the order of its presentation. It encourages summarizing each concept in a few words. The resultant mind map can be seen and memorized and helps in developing a "big picture."
- **Learning and overviewing**—Because a mind map builds a larger view of a subject, it helps in understanding the links and connections among the various component parts and exploring them in more detail. This works well when drawing a mind map of a textbook while reading it. The process of creating the mind map increases the amount of information that is absorbed from the book and results in a one-page summary of all the things that matter. The same approach can be used in the preparation of training material.
- **Creative writing and report writing**—These are greatly assisted because a mind map rapidly produces a large number of ideas that can be organized into related groups or topics. The same applies to the preparation of presentations or speeches.

In addition, mind maps can be also used for:

- **Communicating complex issues**—A single-page format allows a good understanding of the whole and its parts, particularly when it shows explicitly how items are associated or related.
- **Meetings**—These can be supported by mind mapping in several ways: preparing the agenda, chairing, engaging the participants, making arrangements and even taking the minutes. If the corporate culture allows it, the minutes can be done quickly and efficiently because there is no need to spend time and effort writing long strings of text (as in "Mr. X stated that ABC and this was refuted by Ms. Y on the grounds that XYZ"). The important point is to allow the brain to listen actively to what is being said.
- **Negotiating**—A mind map can neatly summarize important issues, each position and freedom of action, options, etc., in one sheet and, thus, play a role in maintaining focus during the negotiations. Of course, not all negotiations can be concluded satisfactorily when the issues are many, complex and tainted by long histories of disagreement. These fall outside the scope of auditing.

Figure 3—Mind Map for Recruiting an IS Auditor



Source: E. Gelbstein. Reprinted with permission.

A Simple Example of a Mind Map on an Audit Topic

Figure 3 is intended as an example of how many items can be included in a single page and how little text is needed to document them. In the same way that "a picture is worth a thousand words," "a mind map is worth a hundred pages." This is especially helpful in avoiding instances of a text being written collaboratively, during which hours may be spent arguing about a word or a semicolon.

No doubt you will find things to add, remove or relocate in **figure 3**. Some may even say, "So what? I have been doing this so long I do not need to be told." This may be true, but not everyone may be in such a happy position.

You may have noticed that a similar approach—summary diagrams showing the relationship of items—is consistently applied through the COBIT® 5 family of documents, and the insight the diagrams offer greatly facilitates studying the material.

It was mentioned earlier that mind mapping needs only paper, crayons and erasers. However, there are also many sources of software that support this technique, ranging in price from almost free to what many would consider excessive. The advantages of a software product include the ability to share electronic documents, keep multiple versions of mind maps in well-organized folders and, once the quirks of the software have been mastered, produce neater maps more quickly.

There are numerous online sites[2] that give access to mind maps created by thousands of individuals on almost every subject. There are also many books in many languages that can offer guidance to improve skills.

> **"Mind mapping is a proven tool that enables the selection and meaningful illustration of interrelated topics."**

Conclusion

In a world characterized by information overload, a technique that can help with understanding, organizing and capturing salient points can be a lifesaver. Mind mapping is a proven tool that enables the selection and meaningful illustration of interrelated topics. Not only can it save you considerable time in assimilating valuable information, it supports the recall of that information by leveraging the brain's predilection for visual over verbal memory. Given the rapid pace of change in technology—and the subsequent publication of reams of material (or bytes) describing the change—anyone who works in a technology field, such as IS auditors, risk and control specialists, and information security professionals, can benefit from the mind mapping approach and structure.

Endnotes

1 Buzan, T.; B. Buzan; *The Mind Map Book: How to Use Radiant Thinking to Maximize Your Brain's Untapped Potentia*l, Plume, USA, 1996

2 *www.biggerplate.com/*

Enjoying this article?

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

MEMBER GET A MEMBER 2016

Get Members. Get Rewarded.

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

***Recruit 2 – 3 new members** and receive an attachable tracking device. Easily locate your valuable items, includes multiple customization options: a US $25 value.*

***Recruit 4 – 5 new members** and receive an indoor/outdoor home assistant that flies, 2.4 Ghz camera included. Flips upside down with 4.5 ch. 3D control and LED lights: a US $145 value.*

***Recruit 6 – 7 new members** and receive an any-surface projector. Turn any surface into your very own display and entertainment center: a US $279 value.*

***Recruit 8 – 9 new members** and receive hi-tech, smart luggage that you can control from your phone: a US $375 value.*

***Recruit 10 or more new members** and receive a high-quality gaming system with WiFi capabilities and built-in Blu-ray player. Also includes a controller and 2 games: a US $550 value.*

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

When ISACA grows, members benefit. More recruits mean more connections, more opportunities to network—and now, more rewards you can use for work or fun!

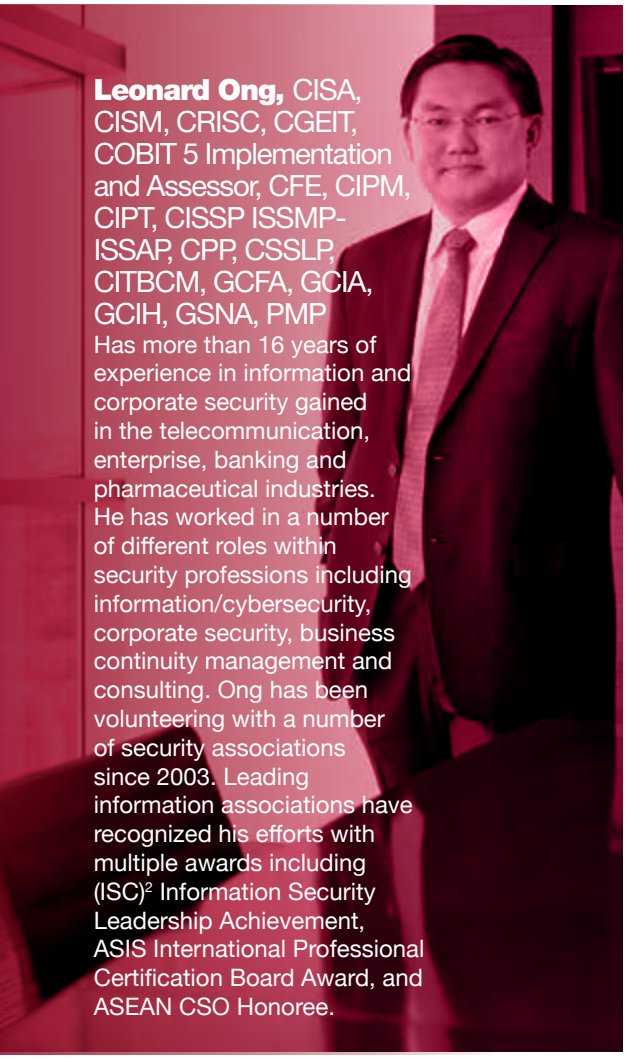
Get recruiting today. It's easy. Learn more at *www.isaca.org/GetMembers*

INFLUENCE MORE

ISACA®

Trust in, and value from, information systems

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



Leonard Ong, CISA, CISM, CRISC, CGEIT, COBIT 5 Implementation and Assessor, CFE, CIPM, CIPT, CISSP ISSMP-ISSAP, CPP, CSSLP, CITBCM, GCFA, GCIA, GCIH, GSNA, PMP
Has more than 16 years of experience in information and corporate security gained in the telecommunication, enterprise, banking and pharmaceutical industries. He has worked in a number of different roles within security professions including information/cybersecurity, corporate security, business continuity management and consulting. Ong has been volunteering with a number of security associations since 2003. Leading information associations have recognized his efforts with multiple awards including (ISC)² Information Security Leadership Achievement, ASIS International Professional Certification Board Award, and ASEAN CSO Honoree.

Q: How do you think the role of the information security professional is changing or has changed?

A: As information technology becomes integrated with business, information security professionals should be well versed in business context. The role is now changing from being reactive and supportive to proactive and enabling. Information security professionals are enabling and delivering new values just like other business functions.

Q: How do you see the roles of information security, risk and governance changing in the long term?

A: The functions will become intertwined more than they have ever been in the past. Professionals in information security, assurance, risk management and governance will have to work closely and seamlessly. I see that there will be both movement from one role to another, and professionals will become multidisciplined. ISACA® enables professionals to acquire new knowledge areas and validate that knowledge through certifications.

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

A: Through the process of certification, I have minimized my knowledge gaps by learning widely accepted bodies of knowledge. The certifications I have earned also help me to get recognized. When hiring, I do look at candidates who have relevant certifications more closely; for example, in a role focusing on IT risk management, a candidate who holds the Certified in Risk and Information Systems Control™ (CRISC™) would be desirable.

Q: What would be your best piece of advice for information security professionals planning their career paths and looking at the future of information security?

A: One should understand his/her strengths and areas of interest. Generally,

the network

there are technical and management tracks. In each of these tracks, there is an option to be a generalist or a specialist. The Cybersecurity Nexus™ (CSX) Cybersecurity Career Road Map is a great tool for mapping a career. One can choose to be a Certified Information Security Manager® (CISM®) (management) or a CSX Expert (CSXE™) (technical).

Q: What do you think are the most effective ways to address the cybersecurity skills gap?

A: Structured, practical and experiential learning with skill validation will have the greatest effect. Cybersecurity skills can be developed in various venues including colleges, universities and in the workplace through job conversion. An important element to bridge the gap is having the practical skill that can be usable in the field.

Q: You have been an active volunteer in a number of security associations for more than a decade. Why do you make volunteering a priority among the many demands on your time?

A: Everyone can make a difference in this world and I choose volunteering in security associations as a way to make a positive impact in our society. Given the elevated importance of technology, our roles in ensuring that we continue to benefit from positive use of technology through security are critical.

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

A: When the roles of information security and technology risk management were not seen as adding value to business, but rather unnecessary overhead, it was a challenging time. In order to transform the situation into a more conducive environment, I did extensive outreach to business leaders and other functions. As part of the outreach, I reintroduced our value proposition and how we can be a partner rather than a barrier.

1 What is the biggest security challenge that will be faced in 2017? How should it be addressed?

Lack of awareness and support from senior management. Address this by engaging the board and senior management and keeping them situationally aware.

2 What is on your desk right now?

A work laptop, a personal laptop, a business notepad, a travel journal, a set of fountain pens

3 How has social media impacted you professionally?

It is amazing that we are no longer confined by physical geographical boundaries to network and collaborate.

4 What is your number-one piece of advice for other information security professionals?

Be proud and continue to partner with business and other functions toward common enterprise goals.

5 What is your favorite benefit of your ISACA membership?

Meeting like-minded professionals globally and learning from those interactions. Also, access to regular publications, surveys and research.

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

Spend my time with my family and volunteer. In my role as a director on ISACA's Board of Directors, I visit various ISACA chapters and interact with chapter leaders and members. At the same time, I contribute in knowledge sharing by presenting at various conferences.

The Challenge of Being "Good"

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.

Moral behavior is, perhaps, easy to talk about, but difficult to put in practice. The answer to the question "Did I do the right thing?" may not be unequivocal. Moreover, what I might find as fundamentally the right thing to do may not accurately be mirrored—by intentional action or otherwise—in the action that follows. There are, indeed, several factors at work that produce the difference between a morally good thing to do and what eventually gets done. In this column, I will discuss some of the reasons for the gap. While this may not be an exhaustive examination of the challenge of being good, an exercise in bridging "ought" and "is" will illustrate what we need to watch going forward.

The Moral Question

For any project (or case) we are dealing with at the time, formulating a moral question may not be an easy task. If a situation has been brewing for some time, it is likely that the decision maker has had time to think about the case and construct potential moral questions. If the situation is imminent and offered no prior notice, it is difficult to sort out "on your feet" what might be a morally appropriate response. Additionally, if two or more people are involved in the case, there is a chance that the individuals involved will air their concern as related to the ethical side of the mainstream project. Nevertheless, unless the scenario is frequent, simple or familiar, one may find that answers to, or even questions of, moral action are hard to come by.

If there is room for reflection on the moral side of the problem at a later stage in the decision sequence, it would certainly provide an opportunity to revisit the moral issue in light of the progress made so far. This will help determine if the decision maker is comfortable with the way moral questions are identified and addressed and if there is any room for change in the problem statement and/or method to address it.

Compounding the difficulty here is the fact that moral (nonmaterial) questions are not identified in isolation; they are inherent in the material problem and how it is solved. There are good arguments to indicate that the immediacy and significance of the organization's material problems may consume so much time and focus from the people engaged in solving the problem that they have no resources left to explore the ethics of the situation.[1] This lack of attention may become even more severe as components of a large project are handed down to groups charged with solving just that part of the project puzzle. The material task assigned to a subteam is guided by the detailed specifications that accompany the charge. In contrast, even if the project-level team determines moral questions and how they should be addressed, the spirit of moral action may not reach the lower levels in project implementation. For these reasons, it is likely that nonmaterial issues are left behind while the material task gets accomplished in the rush to be the first in the market.

These days, the legal battles between Uber and Airbnb on one side and governments on the other have escalated on various issues. One argument put forth by the complainants (governments) is that the

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.*

new models Uber and Airbnb have introduced are not compliant with existing rules. For example, Bloomberg News reported that US Internal Revenue Service (IRS) rules are not clear for reporting earnings via on-demand platforms. As a result, Bloomberg reports, companies do not withhold taxes on income that they pay to service providers.[2] Could Airbnb, Etsy and Lyft have visualized the problem in the ecosystem they were putting together? The answer, of course, is that we do not know. It is likely, however, that some degree of brainstorming could have triggered questions, if not answers, on potential lack of tax withholding for independent contractors. Such reflection could have led to the question of whether the existing IRS rules are ambiguous and whether the company needs to seek clarification from the agency. In light of technology-enabled innovations, unprecedented questions might arise; as a result, the hope is that concerned organizations would be proactive in seeking answers. For example, the American Institute of Certified Public Accountants (AICPA) sent the IRS a letter requesting clarifications regarding the tax status of issues related to eCurrency, including rules for donating digital currency.[3]

A couple of observations emerge from the conflict between emerging new platforms such as Uber and the regulators. First, if regulation is an indication of the need for maintaining trust and harmony in a system,[4, 5] then the presence of regulations in the current ecosystem could provide some understanding of legally minimal best behaviors. After filtering what is irrelevant for the new ecosystem, one could derive a baseline understanding of why these rules currently exist and how they might impact the future regulation of the new industry. Second, both the Uber and Airbnb models left the sensitive human components (drivers, hosts) largely outside of their own perimeters. Since moral questions are inherently human issues, one could have thought of the new model as insulated from, or outside the scope of moral issues that concern the collaborators (drivers, hosts). But since the responsibility for those who engage in services presumably rests with the enterprise that owns the business model, some degree of analysis of current practices in the traditional environment was warranted. A weakness here has impacted the reputations of Uber and Airbnb.

While there are no foolproof responses to the developing wedge between progress on the material and moral sides, it would help to have measures in place for responsible behavior. For example, an integrated process where moral questions are asked, addressed and documented in tandem with the material questions would help recognize gaps, if any, and address them in a timely manner.

Who Is Responsible?

A good moral question must clearly articulate the problem and state for whom it is a problem. In a general question about the moral acceptability of a particular course of action or a technology, we do not necessarily identify for whom it is a problem.[6] The locus of some problems may be an individual or a family; for others, it may be an organization; and for still others, it may be the society or the governing agencies.

> **“Being ‘good’ has an aura of positivity for the right reasons...but moral actions exact costs of all kinds.”**

Often, a weak link in exercising the responsibility rests with the responsible party.[7] For example, in protecting our privacy, we need to take certain steps. In fact, all six conditions associated with privacy (notice, choice, use, security, correction and endorsement) include the phrase “the individual has the right to”; however, for various reasons, people prefer to disregard what they need to do. The mind-set that pervades the majority also determines the overall state of integrity in the ecosystem.
One reason people think one way and behave differently on ethical grounds is called “bounded awareness.” The concept can be explained as “the

common tendency to exclude relevant information from our decisions by placing arbitrary bounds around our definition of a problem, resulting in a systemic failure to see important information."[8] Additionally, it is asserted that people also suffer from "bounded ethicality," or "systematic constraints on our morality that favor our own self-interest."[9] As a result, ethical gaps arise, which become compounded at the organizational level. In fact, organizational gaps are more than the aggregate of individual members' gaps due to the groupthink phenomenon, which pulls the group toward unanimity and inhibits open dialog on ethically challenging questions.[10]

> **"The 'immorality of silence' pervades society to more of an extent than one can imagine."**

Inasmuch as individuals and their families are responsible for being "good" in their private lives, organizations—businesses and nonprofits as well as the government—are accountable for responsible governance. Ultimately, how well nonmaterial issues are addressed in organizations depends in large part upon the climate of the organization. If the climate is inducing appropriate behavior, chances are that serious proactive attempts will be made to identify and treat moral issues entailed in material issues.

Researchers warn that we should pay attention to what is not being talked about within an organization, for it can provide valuable information about informal values,[11] a powerful force in shaping the firm's culture. It is the leader's responsibility to set the tone at the top. However, it is also necessary for the organization to continually assess the climate's quality on an ongoing basis. Unless some vitals are monitored regularly, it will be difficult to seek comfort in the treatment of the moral issues as and when they arise.

Cost of Morality

Being "good" has an aura of positivity for the right reasons. It makes life purposeful and allows us to preserve our internal peace. It spreads calmness into our constantly churning mind and makes us happy. But moral action exacts costs of all kinds (i.e., money, energy, loss of opportunities). For example, a student may earn a low score on a test if he/she does not resort to cheating. However, for that student's academic advancement, his/her grades could be too important to sacrifice. Acting with honesty could cost him/her admission to a prestigious graduate program.

Whether you are a manager, a student, a whistleblower, a leader or an auditor, it is just not easy to disregard the potential consequences of your voluntary actions. Fear of retribution, threat of loss of job, other threats to the person or his/her family, and anticipated turbulence in one's life—these are at play in considering a bold action. Adding up everything and stacking it against what one would gain from that action often leaves people unwilling to "rock the boat." Passive observation of a wrongful act from the sideline is immoral, but how many jump in and fight against the actor? The "immorality of silence"[12] pervades society to more of an extent than one can imagine. For example, if no one challenges organizational wrongdoing, such as an invasion of privacy, the practice of violating others' right to privacy could become the norm.

Anonymity has proven to be a protective measure in encouraging people to speak up about wrongful acts. Whether anonymity is used to preserve personal liberties, protect trade secrets or improve the quality of responses, we need systems designed to ensure nonattribution.[13] Technology can provide solutions, such as whistle-blower systems, that help preserve informants' privacy.

The intervening medium of technology, if it is perceived by the prospective informer as safe, can result in timely and organic detection and treatment of the immoral action. We should note, however, that what works to protect anonymity in the right way also can create problems in other constructs.

For example, anonymity in eCurrency may engender illegal acts of money laundering. Even in anonymity-granting ecosystems, there is always the risk of someone breaching the secrecy. The case of the Panama Papers[14] is just one example of how technology can reveal the usually unseen miscreants and their partners.

Conviction in the Cause

Ethical judgments are based on formal and informal frameworks. An intuitivist framework helps one identify acceptable moral actions intuitively. A dominant-value framework identifies appropriate moral actions by generating conviction about the most dominant value from among the competing values in a moral dilemma.[15] Regardless of the framework used, one's perception of the various values is an important trigger for moral action. Without a strong identification with a value, one might fail to see the significance of an action one chooses to implement.

A number of examples can be noted here: in politics (Martin Luther King Jr. and Rosa Parks), sociology (Candace Lightener and Mothers Against Drunk Driving), business (Blake Mycoskie of Tom's Shoes), and technology (Julian Assange and WikiLeaks, Edward Snowden's case involving surveillance and the US National Security Agency [NSA]). Whether or not you believe in their cause, they each had a strong conviction about something being wrong and the need to correct the situation. That is why they took risk and, perhaps at great pains, delivered their opinion to others to cause something to happen. Whereas conviction in the cause is fundamentally important for moral action, it is also necessary that the person has the courage to do the right thing. Mustering courage is no easy task, for the worldly consequences of defying wrongdoing can be devastating to one's life. Therefore, courage is often mentioned in tandem with the cause and the former—when acted upon—often implies valiant behavior.

Morality as a Human Endowment

By definition, morality pertains to humans, not machines. All systems are essentially an allocation of tasks between humans and machines; some having a much larger role for humans than machines, others are dominated by the machines. Among the roles that continue to remain with the humans is the role of a moral agent. In this role, an IT professional not only strives to behave ethically, but also designs the automated tasks—the part that eventually belongs to machines—in a morally responsible manner. Thus, the imparted understanding of what is moral in machines is the responsibility of the human taking care of the man/machine allocation of tasks. For this, the consideration of nonmaterial issues up front is critical in nurturing predictable responsible behavior in automated systems.

> **"From automated cars to drones, a whole range of rules of moral behavior are programmed into the machines."**

Interestingly, development in the field of artificial intelligence (AI) has shrunk the role of humans in a human-machine partnership in automated systems. The diminished human role in new systems may appear small, but it is not insignificant; it is that part of the system that still needs human judgment and choices driven by values. The choices the human designer makes in creating the automated system tend to become permanently established in the life of the machine. The machines may learn to change their behavior, but only if machine learning has been programmed appropriately. The human element in the overall moral impact just cannot be understated or ignored. From automated cars to drones, a whole range of rules of moral behavior are programmed into the machines. Any judgment errors at the design stage spell greater risk of moral compromises. Questions of ethical behavior are fundamentally human questions. Whether outside of or within the legal perimeter of a business, human collaborators will continue to actively participate in the ecosystem. In the car-for-hire context, perhaps this question

will go away or change drastically when Uber deploys autonomous cars. And for drones, the rules dominate their behavior; until they are designed to learn, the responsibility for moral grounding of drones rests with the technologists. Eventually, when machines become nearly autonomous, machine ethics may be extended to what robots can learn.

Endnotes

1 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

2 "Billions From Airbnb and Others Go Unreported," *Bloomberg News*, as reported in the *Omaha World-Herald*, 24 May 2016

3 Saunders, L.; "The Latest Stumbling Block for Bitcoin: How to Tax It," *The Wall Street Journal*, 25 June 2016

4 Kohlberg's moral stage development work includes compliance with the laws and regulations as one of the stages. See Kohlberg, L.; "Moral Stages and Moralization: The Cognitive Development Approach," December 1975.

5 Kohlberg, L.; *The Psychology of Moral Development: The Nature and Validity of Moral Stages*, Harper and Row, USA, 1984

6 Van de Poyel, I.; L. Royakkers; "The Ethical Cycle," *Journal of Business Ethics*, vol. 71, February 2007, p. 1-13

7 Mims, C.; "In Securing Our Data, the Weak Link Is Us," *The Wall Street Journal*, 19 January 2016

8 Bazerman, M.; A. Tenbrunsel, "Blind Spots: The Roots of Unethical Behavior at Work," *Rotman Magazine*, Spring 2011, p. 53-57

9 *Ibid*.

10 *Ibid*.

11 *Ibid*.

12 Das, G.; *The Difficulty of Being Good: On the Subtle Art of Dharma,* Oxford University Press, United Kingdom, 2010, p. 59

13 Poore, R. S.; "Anonymity, Privacy, and Trust," *Information Systems Security*, vol. 8, iss. 3, 21 December 2006, p. 16-20

14 Stack, L. *et al.*; "The Panama Papers: Here's What We Know," *The New York Times*, 4 April 2006, *www.nytimes.com/2016/04/05/world/panama-papers-explainer.html?_r=0*

15 *Op cit*, Van de Poyel and Royakkers, p. 6

ISACA®
Trust in, and value from, information systems

2016 ISACA® TRAINING WEEK COURSES

TRAIN AT THE **HIGHEST STANDARDS.**

KEEP CURRENT ON **BEST PRACTICES.**

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

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

EARN UP TO 32 CPEs

for each 4-day course.

REGISTER EARLY:

US $200 Early Bird discount and group rates available!

ACCOMPLISH **MORE**

REGISTER TODAY AT:

www.isaca.org/train16-jv5

CYBERSECURITY FUNDAMENTALS

Las Vegas, Nevada | 5 – 8 December 2016

Learn to demonstrate an understanding of the principles that frame and define cyber security and the integral role of cyber security professionals in protecting enterprise data and infrastructure.

HEALTHCARE INFORMATION TECHNOLOGY

Chicago, Illinois | 10 – 13 October 2016

Obtain a deeper understanding of healthcare's regulatory issues, trends and reforms. Prepare yourself to navigate the complexities of the fast-growing industry in an era of significant reform.

INFORMATION SECURITY ESSENTIALS FOR IT AUDITORS

Miami, Florida | 12 – 15 December 2016

Keep on top of audit security essentials. Learn how to assess security risks and practices and use security frameworks and models to mitigate those risks.

TAKING THE NEXT STEP— ADVANCING YOUR IT AUDIT SKILLS

Atlanta, Georgia | 28 November – 1 December 2016

Learn how to scope, plan and manage IT audits, and identify and analyze risks associated with a broad range of infrastructure platforms and technologies.

How to Audit the Human Element and Assess Your Organization's Security Risk

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 *2016 Data Breach Investigations Report* (DBIR), Verizon's ninth annual report, revealed some grim news—the human threat vector is more dangerous than ever. The latest DBIR reaffirmed the fact that employees continued to play a major role in many of the breaches in the past year. Some 63 percent of confirmed breaches involved weak, default or stolen passwords. Worse, miscellaneous error—staff sending information to the wrong person—accounted for nearly 18 percent of breaches.[1] Despite a wealth of preventive measures, employees remain one of the costliest vectors in a number of data breaches and security incidents, which are increasing at an alarming rate.

Who is at fault? It is hard to say because although employees are clearly identified as a source of risk to the business, boards and executives are also increasingly being held responsible for risky cybersecurity practices. In fact, recent research shows that employees often want to place the blame for cyber shortcomings squarely on the shoulders of boards and executives. Twenty-nine percent of surveyed office workers and IT decision makers in the United Kingdom believe that the chief executive officer (CEO) should be responsible for a significant data breach, while 38 percent of office workers believe boards should be held accountable.[2]

Tom Pendergast, Ph.D.
Is the chief architect of MediaPro's Adaptive Awareness Framework, a vision of how to analyze, plan, train and reinforce to build a comprehensive awareness program, with the goal of building a risk-aware culture. He is the author or editor of 26 books and reference collections. Pendergast has devoted his entire career to content and curriculum design, first in print as the founder of Full Circle Editorial, then in learning solutions with MediaPro.

Também disponível em português
www.isaca.org/currentissue

Conversely, these boards and executives are looking to those in IT or information security and asking what they are doing to mitigate the risk posed by the "human element." Whether this examination of current practices is called an audit or something else, the push is on for a more rigorous way of accounting for organizational efforts to address this most vexing security risk: employees. Boards and executives want to know what exactly is being done to address the issues and whether or not these actions are getting the desired results. They want to see that there is a true awareness program in place, i.e., a program that targets meaningful changes in employee knowledge and behavior.

However, those who are asked to perform such an audit will find very little guidance on the subject. The normal sources that guide program evaluation—various documents provided by the US National Institute for Standards and Technology (NIST), the International Organization for Standardization (ISO), and the US Health Insurance Portability and Accountability Act (HIPAA), among others—provide only vague descriptions of awareness program standards and requirements. Fortunately, there is a lot of good work being done in this area that can help organizations evaluate whether they are on the right track in addressing the human threat. The best practices used in some of the world's most risk-aware companies highlight some core attributes organizations should look for (or create) as they seek to make improvements in the performance of the human element.

Although these best practices take different forms and different names, the best awareness programs do some common things: They assess and analyze the real human performance within the organization; they create a plan for sustained improvement; and they introduce a series of educational interventions (e.g., training and reinforcement) targeted at changing behavior and encouraging a risk-aware culture. Organizations that take the human problem seriously know that they must examine the current state of employee knowledge, skills and attitudes toward security (and privacy, often intertwined in the eyes of employees). This requires stepping back to take a broad look at the organization's culture, assessing all the potential ways employees are (or are not) understanding and responding to security-related risk.

> **"...Although employees are clearly identified as a source of risk to the business, boards and executives are also increasingly being held responsible for risky cybersecurity practices."**

Some of the best ways to understand a company's human risk factors are by conducting employee surveys, both pre- and post-training. These help organizations to understand what employees know today, so appropriate enhancements can be made in the future. Even if the budget is tight, there is no shortage of free industry data, such as the previously cited DBIR, to help an organization understand its specific employee risk. Only when the risk factors are understood can the organization ensure that it works to deliver the right training to the right employees.

Additionally, data from network incident reporting tools, such as security and information event management (SIEM) systems and data loss prevention (DLP) software that may already be in place, will help in understanding the prevalence of data handling issues. The concept of user and entity behavioral analytics (UEBA or UBA) is quickly emerging as a way to parse through all the information collected by SIEM, DLP and other sources, and provide prioritized trend information to the IT professionals monitoring the network. UEBA tools provide real value in identifying patterns and signs that reveal the presence of bad actors in the IT environment.

An exciting emerging use for UEBA is tying it directly to "just-in-time-training" at the spot of the foul. UEBA might identify Jane Doe saving a company document to an unapproved cloud storage site such as Dropbox, Box or Google Drive, and deliver a system-generated pop-up that reminds her of the company's policy on storing company documents in an authorized ecosystem. If Jane does it again, the system then might provide a quick video on the reasons why it is best to avoid an unapproved cloud storage system. Months later, if Jane makes the same mistake again, she might be automatically enrolled in a 15-minute course on approved cloud storage and the appropriate way to store company documents. That is a perfect example of delivering the right training to the right person at the right time.

Separate from network monitoring tools, simulated phishing and social-engineering attacks reveal what risky actions employees are most likely to take when given the opportunity. Such simulations can employ a wide variety of clever techniques to gather passwords, obtain access to sensitive information, or gain physical access through tactics as simple as an email or a phone call, tailgating, or leaving dummy USB devices in the work environment.

Enjoying this article?

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

A number of vendors offer phishing simulator programs as part of an awareness program package. But vendors that focus too heavily on phishing as the be-all, end-all of cyberthreats should be viewed with some caution. Such an approach targets only one vector of attack and does not do the work of helping employees see the multilayered nature of threats.

Another important step in improving employee performance and culture is understanding the risk specific to the organization's industry and unique business environment. For example, if an organization has a call center, its employees are going to face very different risk factors from those encountered by workers at a bank—it is just the nature of what the job entails. Understanding the risk factors in specific areas of the business allows the organization to deliver training that is tailored to its employees' specific lines of work, which is inherently more relatable and useful. (Training loses much of its effectiveness if it is not relevant.)

"Once these human-related risk factors are understood and described, the next step is to develop a plan for an awareness program that addresses the risk factors."

Recently, the US Securities and Exchange Commission (SEC) noted that cybersecurity is the biggest risk to the US financial system, with SEC Chair Mary Jo White saying, "What we found, as a general matter so far, is a lot of preparedness, a lot of awareness, but also their policies and procedures are not tailored to their particular risks."[3] A recent report by the SEC Office of Compliance Inspections and Examinations (OCIE) examined the securities industry and recommended the industry as a whole "focus on how training is tailored to specific job functions and how training is designed to encourage responsible employee and vendor behavior,"[4] lending further support for the need for training that is relatable and useful.

While there are many tools for analysis, the goal of them is the same: to come up with a list of five to 10 human-centered risk factors that can be the focal point of efforts to improve (there is no golden number, but the more effective programs limit the number to focus their efforts). Once these human-related risk factors are understood and described, the next step is to develop a plan for an awareness program that addresses the risk factors. Like anything in life, planning is key when it comes to developing a successful, comprehensive awareness program. As part of that plan, organizations should ask themselves if they have set out to implement both formal and informal educational programs. Conventional wisdom would say formal training, often web-based, is the way to go. This is largely due to the ease with which employees can be held accountable for taking training, but the education program cannot stop there if the organization really wants to reach its employees and create that ever-important change in behavior. The best programs do not rely solely on formal training; instead they rely on a variety of educational measures to communicate desired knowledge and behavior to employees.

Once an organization has a solid plan, it needs to quickly inventory whether or not it has the capacity to deliver a program and make good on its plan. For example, does the organization have the capacity to deliver educational reinforcement in the form of games, videos and posters? Are executives on board and willing to champion messages in their daily communication with employees? Are all the right people in place to support and help carry out the program? Organizational capacity to successfully deploy a program is critical to carrying out the plan and will determine whether or not it can go "all in" with an adaptive campaign of phishing, training, posters, games, animations and the like over the course of the year.

In more progressive organizations where the goal is a mind-set change, messages about information protection become part of the daily culture. This may include catchy and memorable posters on the walls, animated videos playing on lobby

TV screens, or even a game that gets people competing against one another and allows employees to show what they know about security and privacy. These types of examples are what make the difference when paired with more formal, ongoing training.

One example often cited is Microsoft because it does a great job of this. Anyone who has walked around one of its many campuses should be accustomed to seeing constantly changing messaging about security and privacy. An auditor or executive in any company should see these types of awareness-raising devices when they walk around. If they do, that is an indication of a company that has made tremendous strides in protecting company information and empowering employees to do the same.

> **"Identifying risk factors at the individual level saves time and money, as the organization likely does not need to train John and Jane equally."**

Additionally, a good program delivers training that is role-based or role-specific; employees in different roles, such as human resources (HR) and IT, should receive training tailored to their specialties. Why does this matter? IT employees do not need to know about safeguarding conversations with potential hires, but do need to be well versed in preventing unauthorized data access and use. Conversely, the HR staff need not be as concerned with education on data transmission practices, while protecting sensitive employee information is exactly in their wheelhouse.

Another way to focus education on those who need it is to deploy a means of assessing competence prior to training delivery. How? Rather than giving everyone training on a whole slew of topics—the most expensive and most time-consuming option—individuals can be trained on what they might be lacking, on a case-by-case basis. For instance, Jane Doe has received five simulated phishing attempts over the past year and has forwarded each of them to IT without clicking the link, whereas John Doe has bitten on three of those five phishing campaigns. Based on that information, one can conclude that Jane probably does not need phishing training, but John definitely does. Identifying risk factors at the individual level saves time and money, as the organization likely does not need to train John and Jane equally. As the saying goes, "time is money," and when employees are spending time being trained on things they do not need to know, they are potentially missing out on more important, job-related tasks (and coming to the conclusion that information security does not matter to them!).

Even the organization that has identified its specific risk factors, developed a plan, and is going to implement formal and informal training can do more if it wishes by assessing whether it has a culture of security. This is hard to measure, but not impossible. Information gathering at this level calls for rigorous employee knowledge assessment. A Security Culture Diagnostic Survey has been designed to identify and compare security cultures in organizations and can be found in *People-Centric Security: Transforming Your Enterprise Security Culture*.[5]

Alternatively, organizations can start by looking at what messages managers and executives are (or are not) communicating relative to security. Moreover, are the security-reinforcing systems (e.g., incident reporting, systemic security reviews) valued and utilized? Do any business units outside of information security attempt to meaningfully engage with security issues? If the answer to any of these is "no" or "do not know," the organization may not have reached the point where it has an established culture of security, which should be part of its plan to improve its awareness posture.

A truly mature organization, one that adheres to the principles of tier 3 and tier 4 in NIST's Cybersecurity Framework (CSF),[6] approaches information security as a self-reinforcing program of continuous improvement, not simply an annual event, like the required training model of old. The CSF makes it clear that there are levels to cybersecurity maturity and, in a similar way, awareness maturity. These levels of maturity are conveniently broken out into tiers:

> **"A truly mature organization... approaches information security as a self-reinforcing program of continuous improvement, not simply an annual event."**

- **Partial (tier 1)**—Risk management is *ad hoc* with limited awareness of risk and no collaboration with others.
- **Risk informed (tier 2)**—Risk management processes and programs are in place, but are not integrated enterprisewide; collaboration is understood, but the organization lacks formal capabilities.
- **Repeatable (tier 3)**—Formal policies for risk-management processes and programs are in place enterprisewide, with partial external collaboration.
- **Adaptive (tier 4)**—Risk management processes and programs are based on lessons learned and embedded in culture, with proactive collaboration.

Organizations that approach training as simply an annual event likely find themselves in tier 1 or tier 2, whereas organizations that continuously improve are more likely to be found in tier 3 or tier 4.

Whatever tier or maturity level an organization is or aspires to be, the path to understanding and improving starts with stepping back and examining existing practices. The best organizations analyze their human risk factors using a variety of different tools; they develop a plan to change behavior related to those risk factors; they align their resources to execute on that plan; and then they deliver adaptive, flexible education to the right people, when and where they need it. Threats are not slowing down and the best efforts of employees are not keeping up. Employee security awareness education must continually adapt to new and emerging threats. The best way toward this goal is through a robust, risk-aligned and adaptive awareness program.

Author's Note

The author wishes to disclose that Microsoft has done work with MediaPro in the past.

Endnotes

1 Verizon, *2016 Data Breach Investigations Report, www.verizonenterprise.com/verizon-insights-lab/dbir/2016/*
2 VMare, "The Cyber Chasm: How the Disconnect Between the C-suite and Security Endangers the Enterprise," The Economist Intelligence Unit, 2016, *www.vmware.com/radius/wp-content/uploads/2015/08/EIU-VMware-Data-Security-Briefing.pdf*
3 Lambert, L.; "SEC Says Cyber Security Biggest Risk to Financial System," Reuters, 18 May 2016, *www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4*
4 Securities and Exchange Commission, "OCIE's 2015 Cybersecurity Examination Initiative," National Exam Program Risk Alert, vol. 4, iss. 8, USA, 15 September 2015, *https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf*
5 Hayden, L.; *People-Centric Security: Transforming Your Enterprise Security Culture*, McGraw-Hill, USA, September 2015
6 National Institute of Standards and Technology, Cybersecurity Framework, USA, 2013, *www.nist.gov/cyberframework/*

Cyberinsurance: Value Generator or Cost Burden?

Também disponível em português
www.isaca.org/currentissue

The rapid advancement in technology is driving tremendous change in many industries. As a result, vast amounts of data are generated, which can be harnessed into information to facilitate and make sense of a world in constant motion. Data are now considered a wealth generator for the 21st century. Consequently, the financial costs of data loss through cyberevents can be staggering. For instance, the highly publicized attack on Target cost the retailer and financial institutions an astronomical US $348 million.[1] Another costly cyberattack was the attack on the Wyndham hotel chain, which not only lost credit card data of more than 619,000 customers, causing US $10.6 million in loss, but also subjected the company to a US government lawsuit for deceptive business practices for getting hacked on three separate occasions.[2] Another example is attacks using CryptoWall, which caused US $18 million in losses in 2014 related to ransom payments to unencrypt personal data.[3]

The focus on cybersecurity has, perhaps, never been sharper, as cybercriminals continue to push the bar higher with more sophisticated attacks supported by the Dark Web, which consists of web sites that hide their identity and are typically accessed by an encrypted network (e.g., Tor) that also conceals the user's identity, enabling a lucrative e-commerce black market of stolen data from legitimate sources. Although the short-term impact from a cyberattack can be overwhelming, the long-term implications can be quite burdensome. Some of those long-term implications include:

- Business continuity/supply chain disruptions
- Finding and fixing vulnerabilities
- Forensic accounting for lost data and record management
- Data restoration
- Notification cost to those affected by the breach
- Payment of ransom in cyberextortion
- Identity theft protection and credit monitoring
- Reissuing compromised cards
- Regulatory and civil sanctions
- Shareholder suits against board and management
- Lawyer fees during investigations and trials
- Loss in competitive advantage and markets
- Brand damage
- Loss of customers, profits and jobs

The probability of incurring one or more of these damages and the impact they have on an organization depends on a combination of factors that include, but are not limited to, the:

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.

Syed K. Ishaq, CISA, CRISC, CCISO
Is the founder of ControlPoints, a trusted strategy-through-execution information security firm. Ishaq has 15 years of audit, compliance and cybersecurity experience. He can be reached at *syed@controlpoints.com*.

- Type of attack, e.g., distributed denial of service (DDoS) vs. ransomware
- Scope of attack, e.g., the entire network offline for days vs. a social media account takeover for only a few hours
- Complexity of the attacked network, e.g., high interconnections with numerous third-party suppliers vs. impact only to telecommunications because IT is hosted on a secure cloud
- Time of attack, e.g., during sensitive merger or acquisition negotiations vs. off-peak hours
- Affected business area, e.g., mission-critical services/products downtime preventing core business activities vs. the unavailability of nonessential services/products
- Readiness capability of the affected organization, e.g., nonexistent recovery policies and procedures vs. mature incident response program

> **"Enterprises are beginning to consider cyberinsurance as a component of their risk transfer strategy."**

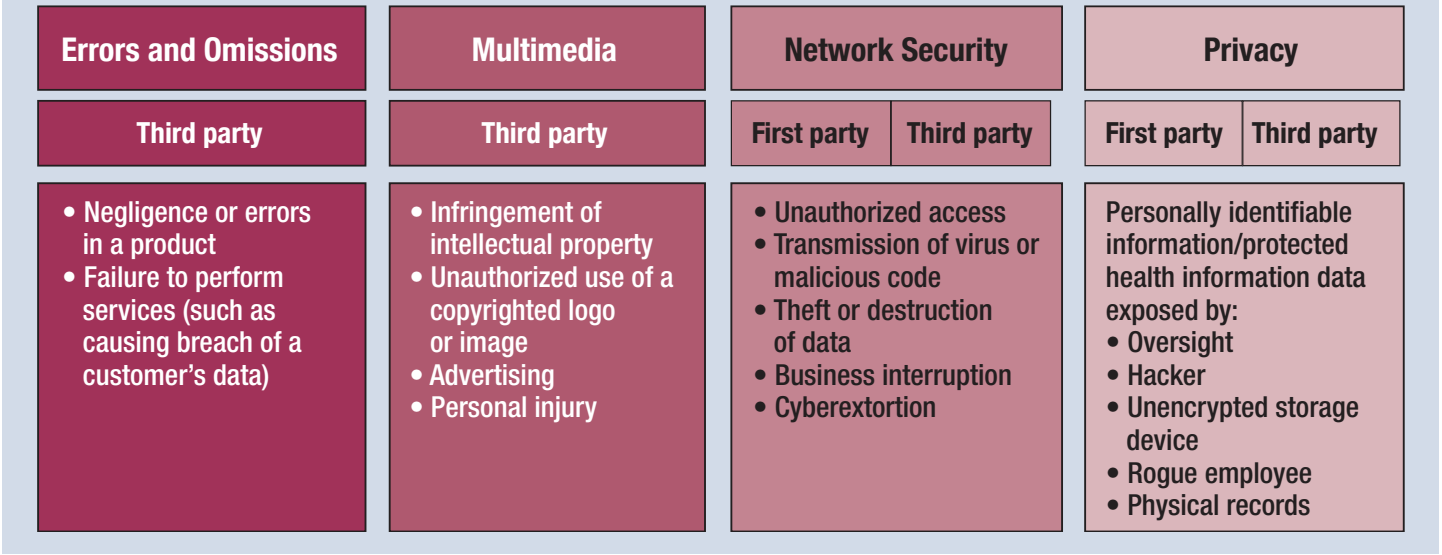
A 2016 survey found 66 percent of US, 75 percent of UK and 57 percent of German respondents were likely to stop doing business with a hacked organization.[4] Though larger companies may be better equipped to weather a cyberstorm and its aftermath, according to Experian, 60 percent of small businesses close their doors within six months after an attack,[5] making cybercrime an equal opportunity with unequal consequences. Hence, organizations would be well served to utilize the risk management strategies of avoidance, mitigation, acceptance and transference. In other words, performing all business activities manually instead of using any form of technology may help avoid cyberrisk altogether. This strategy, however, is susceptible to creating a competitive disadvantage in the modern era and is unlikely to be a viable option for most companies. Securing the network perimeter with firewalls and an intrusion prevention system, performing timely patching of vulnerabilities, and baselining configurations are methods to mitigate, or lessen, cyberrisk. Having a robust monitoring program, but making it formal policy to review audit logs on an infrequent basis due to other priorities demonstrates risk acceptance, i.e., the consented risk appetite of management. With data breaches and hacks seemingly inevitable and their detrimental impact ostensibly inescapable, enterprises are beginning to consider cyberinsurance as a component of their risk transfer strategy. In other words, organizations contractually obligate an insurer to accept part or all of their risk in the event of a cyberattack and/or breach.

Types of Policies

A traditional general liability policy only covers property damage making it insufficient to address cyber because data are intangible property. To address this shortcoming, there are approximately 50 global insurers offering cybercoverage, 35 of which are in the United States.[6] Carriers offer some combination of the following four components (**figure 1**):[7]

1. **Errors and omissions (E&O)**—E&O covers claims arising from errors in the performance of service.
2. **Multimedia liability**—Multimedia liability covers defacement of web sites, media, intellectual property rights, copyright/trademark infringement, libel and slander. Coverage here can also extend to offline content.
3. **Network security and extortion liability**—Network security liability covers the costs associated with a failure of the network to guard against a virus transmission, loss of trade secrets or patent applications, and data breaches. It includes the cost of data restoration, voluntary notification, public relations and risk management, business interruption, and crisis management. In like manner, extortion liability covers damages

Figure 1—Policy Types



Source: S. Ishaq. Reprinted with permission.

incurred from extortion, such as ransomware or distributed denial of service (DDoS) that demands payment to stop the attack.

4. **Privacy management**—Privacy includes the wrongful disclosure of personally identifiable information (PII), health and confidential information. It includes the costs for investigation, notification, credit monitoring, regulatory fees (e.g., US Federal Trade Commission [FTC] and state attorney general) and associated legal fees. Privacy can also include a loss of physical records such as improperly disposed-of files, human errors (e.g., a lost laptop, sending sensitive information to the wrong email address, a photocopier with a hard drive that contains unwiped customer records) or the wrongful collection of information.

What is unique about the network security and privacy coverages is that both first-party costs and third-party liabilities are covered. First-party coverage applies to direct costs for responding to a security failure or privacy breach. Third-party coverage applies when a company is sued, has claims made against it or has regulators demanding information.

On the other hand, what cyberinsurance does not cover is prior knowledge of issues, pending litigation, reputational harm, loss of future revenue, cost to improve internal technology systems, lost value of intellectual property, bodily injury or property damage, and effects from malicious cyberattacks. Some insurers, however, have begun making exceptions to the rule, in particular for the latter two limitations. For example, although Verizon reported a tripling of nation-/state-sponsored attacks between 2012 and 2013,[8] this type of attack source still remains uncovered due to the difficulty in attributing an attack solely to a nation/state adversary. As threats keep evolving, cyberliability brokers and insurers need to continually tailor exclusion policies.

The Fine Print

Although there are a variety of policies available, each is designed differently by individual insurers. Without careful due diligence, the insured may receive a policy that excludes most real-world threats, places unreasonable limits on others and over-covers less likely scenarios. In particular, a simple failure of timely notification to the insurer can be a common reason

Enjoying this article?

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

for denying coverage. For instance, a policy may require reporting a breach prior to or within 60 days of the policy's expiration. However, a 2015 Ponemon Institute study found that cyberattacks go undetected for an average of eight months,[9] which is more than enough time for purveyors of data to erase audit logs to impede forensic analysis and wipe out legal evidence. As a consequence, a company unaware that it has been breached until months later or until notified by a third party, e.g., its credit card processor or law enforcement, will have missed the date to file a claim.

> **"As threats keep evolving, cyberliability brokers and insurers need to continually tailor exclusion policies."**

By the same token, some policies may exclude upgrades and improvements even if a company is determined eligible for reimbursement. A payout for recovery objectives that do not include restoring the system(s) to a more resilient state than prior to the attack will only place the network back in the same predicament of being exposed to similar attack types, depending on the nature of the attack. The following case studies highlight the real-world, complex nature of cyberattacks and their impact on cyberliability insurance reimbursement many companies face.

Cottage Health System, a health care provider, had its cyberinsurance claim denied for a 2013 breach because it failed to continuously reassess its exposure to information security and privacy threats and follow minimum required practices such as encrypting medical records on a system fully accessible to anyone on the Internet.[10]

Ubiquiti Networks Inc. was subjected to an increasingly popular chief executive officer (CEO) scam in 2015. Cybercriminals spoofed (or impersonated) the CEO's email account, then sent an employee at a subsidiary company in Hong Kong instructions to transfer US $39 million to overseas accounts controlled by hackers. Since the payment was "voluntarily" wired by the employee, "the company may not be successful in obtaining any insurance coverage," explained the company in a released statement.[11]

BTC Media had its CEO's email compromised, but the breach included a social-engineering (spear-phishing) component. The compromised CEO account sent an email to a potential acquisition target's chief financial officer (CFO) with instructions to review the modifications on the proposed deal by opening an attachment, upon which the CFO's authentication credentials also became known to the hacker. The compromised CFO then instructed his CEO, in anticipation of the deal, to transfer 5,000 bitcoins valued at US $1.8 million to a spoofed holding account controlled by the hacker. Since the source of the fraud was BTC Media, the acquisition target's insurer denied its claim because the policy only covered losses from direct fraud.[12] The insurer defines "direct" to mean without any intervening steps or diverting factors.

Challenges

The aforementioned case studies raise the question: How does one go about evaluating the myriad of policies and selecting coverage that ensures timely and adequate reimbursement after an attack? Though companies are able to discuss their cyberinsurance needs with insurers, there are important issues both parties must separately overcome. For starters, brokers with a rudimentary evaluation process may rely on generic questionnaires to gauge how embedded cybersecurity is in a company's risk management strategy to set insurance premiums. Despite this, there is no standard baseline among insurance companies, thereupon insurers with less mature questionnaires may take on increased risk exposure.

For prospective insurance customers, the interpretation of questions can vary significantly, especially if technical resources are not involved in the company's internal response process. Given

that effective measures require several layers of security, if one or more layers are overlooked or misunderstood, it can result in unnecessarily higher premiums and/or greater policy restrictions. For example, a strong compliance program does not equate to an effective information security program, and *vice versa.* Moreover, an adoption of either program does not necessarily correspond to a reduction of risk. With cybersecurity dynamically evolving, if management, lawyers or brokers lack the requisite background to evaluate questions and safeguards at their disposal, then they may miss an opportunity to negotiate more favorable policy language to maximize liability protections. On the other hand, the coverage portfolio they do receive may not provide a complete measure of protection for the actual state of their organization's security posture. Furthermore, a completed insurance application detailing the controls in place may not be vetted by the insurer until after an incident occurs; henceforth, if it is found the information submitted by the business overstates the actual controls in place, it can render the entire policy useless post incident.

In the same fashion, insurers, brokers and underwriters versed solely in business and financial risk lack the requisite skills to adequately assess technology safeguards and risk. IT requires a specialized understanding, but IT security necessitates even more focused expertise because the impact of cyber transcends well beyond the IT department. Best practice in cybersecurity continues to evolve, reinforcing the notion that the solutions that work well today might become obsolete tomorrow. A point-in-time evaluation of a company's security posture in a constantly evolving threat landscape only increases the complexity of determining the appropriate scope and cost of coverage. The interconnected nature of IT means the more networks with which a single business interacts, the more risk it is subjected to. To get a clear picture of the material risk, each third-party network must also be assessed, which is no easy task for an insurer. And the emerging threats from increased adoption in end points, social media and the Internet of Things (IoT) should not be overlooked. For example, it can be difficult to conclusively tie a case of identity theft to a single attack vector because a breach could occur from a lost phone, logging onto an infected web site, data stolen in real-time transit or an IoT device connected to public Wi-Fi. Insurers must overcome this wide knowledge gap as they try to figure out the type, frequency and severity of cyberthreats facing an organization.

The early days of this hopeful industry present additional challenges worthy of consideration. For instance, government pressures to release breach details without a guarantee of immunity disincentivizes firms from sharing attack analysis data. In the same way, the negative market perception that surrounds a breach restrains companies from talking about their cyberincidents unless they absolutely must. This paradox restricts the flow of historical data and trends released into the market that insurance companies could otherwise rely on to make comparisons within and across industries. From a legal perspective, cyberinsurance language in contracts is still relatively new and not well litigated. For that reason, the lack of robust precedence compels courts to be reluctant to hear cybercases, thereby leading to disputes addressed chiefly through arbitration.

"A point-in-time evaluation of a company's security posture in a constantly evolving threat landscape only increases the complexity of determining the appropriate scope and cost of coverage."

Return on Investment

The market for cyberinsurance is relatively new, unpredictable, and lacks trending data and comprehensive coverage packages. Greater technical intricacies can lead to vague or complicated contract language and increased trepidation regarding cyberinsurance's actual value. Does cyberinsurance tangibly demonstrate that it increases security, reduces liability, and is a reliable source of relief during

and after an attack? Market sentiment is perhaps best captured in a 2015 KPMG survey, which found that 74 percent of businesses reported not having any sort of cyberliability insurance. Of those that did, only 48 percent believed their coverage would cover the actual cost of the breach.[13] And in a separate report by Reuters, for the few businesses that do get hacked, their premiums triple at renewal time.[14] Nevertheless, shareholders expect the board and management to meet their fiduciary requirements to protect company interests. On top of that, not only are regulations beginning to require cyberinsurance, but mergers and acquisitions transactions also increasingly view cyberinsurance as a means to limit liability.

> **"...the mere process of applying for cyberinsurance can encourage companies to identify best practices and tools, perform advance review, and improve communication among appropriate stakeholders."**

In simple terms, a breach can occur in the infrastructure and the information; the former is inevitable, but the latter is preventable through effective strategies that do not necessarily require costly technology purchases. Unsurprisingly, companies and boards are forced to spend money when there has been a breach or when they are facing a civil lawsuit after an incident, but proactive measures may actually help reduce the overall burden. For example, a strong security awareness program, an effective business continuity plan and an incident response plan can significantly strengthen an enterprise's preparedness and reaction to an attack and help avoid a breach.

Cyberinsurers may require the implementation of basic cybersecurity measures to avert voiding coverage. Hence, the mere process of applying for cyberinsurance can encourage companies to identify best practices and tools, perform advance review, and improve communication among appropriate stakeholders, such as legal, IT, finance and risk management teams, they may not otherwise consider. Residual benefits can include a higher chance of repelling an adversary and lower premiums, the promise of which may encourage organizations to get serious about their defenses beyond the bare minimum. In a sample of 33 companies spanning IT, health care, education, retail and financial services industries, cyberpremiums cost, on average, 1.2 percent of total revenues.[15] Premiums for health care companies cost, on average, 2.8 percent of total revenues, largely due to higher risk and increasing breaches involving patient data. In general, chief information security officers (CISOs) will be able to demonstrate a measurable net profit with their cybersecurity initiatives if the savings achieved from decreased incidents plus cyberinsurance reimbursements can be far greater than the cost of safeguards plus countermeasures.

All things considered, as this nascent industry continues to mature, it remains to be seen if cyberinsurance can demonstrate sufficient value to warrant widespread adoption as a necessary component of an overall cyberdefense strategy.

Endnotes

1 Chiarodo, J.; P., Beshara; "What Cyber Insurance Can Do for Contractors," *FCW*, 7 July 2015, *https://fcw.com/articles/2015/06/30/comment_chiarodo_beshara.aspx*

2 Northrop, S.; "Is Your Business Ready for FTC Oversight of Data Security?," IAPP, 21 September 2015, *https://iapp.org/news/a/is-your-business-ready-for-ftc-oversight-of-data-security*

3 Federal Bureau of Investigation, "Criminals Continue to Defraud and Extort Funds From Victims Using CryptoWall Ransomware Schemes," USA, *www.ic3.gov*, 23 June 2015, *www.ic3.gov/media/2015/150623.aspx*

4 Mann, B.; "Centrify Consumer Trust Survey: The Corporate Cost of Compromised Credentials," Centrify, 8 June 2016, *http://blog.centrify.com/corporate-cost-of-compromised-credentials/*

5 National Cyber Security Alliance, "3 Reasons Hackers Love Your Small Business Infographic," StaySafeOnline.org, 2015, *http://staysafeonline.org/ncsam/resources/3-reasons-hackers-love-your-small-business-infographic*

6 Kirkpatrick, K.; "Cyber Policies on the Rise," *Communications of the ACM*, vol. 58, no. 10, p. 21-23, *http://cacm.acm.org/magazines/2015/10/192376-cyber-policies-on-the-rise/fulltext*

7 Schutzer, D.; "An Assessment of Cyber Insurance," CTO Corner, February 2015, *http://fsroundtable.org/cto-corner-assessment-cyber-insurance/*

8 *Ibid*.

9 Ponemon Institute Research Report, *2015 Cost of Data Breach Study: Global Analysis*, May 2015, *www-01.ibm.com/common/ssi/cgi-bin/ialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF*

10 Greenwald, J.; "Insurer Cites Cyber Policy Exclusion to Dispute Data Breach Settlement," Business Insurance, 15 May 2015, *www.businessinsurance.com/article/20150515/NEWS06/150519893*

11 Hacker, R.; "Fraudsters Duped This Company Into Handing Over $40 Million," *Fortune*, 10 August 2015, *http://fortune.com/2015/08/10/ubiquiti-networks-email-scam-40-million/*

12 Dotson, K.; "BitPay Hacked for $1.8 Million in Bitcoin During December 2014," SiliconAngle, 17 September 2015, *http://siliconangle.com/blog/2015/09/17/bitpay-hacked-for-1-8-million-in-bitcoin-during-december-2014/*

13 Reeve, T.; "Cyber Insurance Not Trusted by Business, KPMG Claims," *SC Magazine UK*, 1 May 2015, *www.scmagazineuk.com/cyber-insurance-not-trusted-by-business-kpmg-claims/article/412535/*

14 Finkle, J.; "Cyber Insurance Premiums Rocket After High-Profile Attacks," Reuters, 12 October 2015, *www.reuters.com/article/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012*

15 Marciano, C.; "How Much Does Cyber/Data Breach Insurance Cost?," Data Breach Insurance, 1 June 2016, *https://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/*

feature

An Integrated Approach for Cyberthreat Monitoring Using Open-source Software

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.

As cyberthreats evolve each day, detecting these threats is becoming more important. Recent studies show that the time between a breach occurring and being detected is, on average, 229 days.[1] Since 229 days is a long time, an average company will not respond to an attack in a timely manner and will not mitigate its effects if there is no extra effort used for detection. This number shows there is a lack of accurate cyberthreat monitoring for most companies, and it is mostly because necessary monitoring mechanisms are not placed correctly and/or do not work seamlessly. Additionally, most companies focus on prevention rather than detection. Since prevention methods for most advanced threats fail, the need for detection is becoming more important each day. There are also security investment cost concerns for most small and medium-sized businesses (SMBs). While a not-so-skilled attacker can easily hack a corporate IT infrastructure by using a US $500 exploit that is being sold in an underground market, the cost for preventing or detecting these attacks is not proportional with this low cost when a company chooses to buy and install commercial solutions.

For these types of needs, open-source software presents numerous possibilities since it has great community support and is cost-effective, especially for SMBs. With its advantages, a company may choose to build its security infrastructure using open-source solutions.

An average breach typically consists of seven main steps (**figure 1**), as modeled by Lockheed Martin and called the Cyber Kill Chain.[2] If organizations want to adequately detect attacks, these steps are important starting points to address necessary monitoring needs.

Figure 1—Seven Steps of the Cyber Kill Chain

Steps	Example Actions
Step 1: Reconnaissance	Harvesting emails, social networking, passive search, IP addresses, port scans, etc.
Step 2: Weaponization	Developing exploits with payloads, delivery system
Step 3: Delivery	Spear phishing, man-in-the-middle attacks (MitM), universal serial bus (USB), infected web sites, etc.
Step 4: Exploitation	Exploiting a vulnerability to execute a code on victim's machine
Step 5: Installation	Installing malware on assets
Step 6: Command and Control	Command channel for remote manipulation of victim's system
Step 7: Actions on Target	Data exfiltration, expand compromise, remote "hands-on keyboard" access

Source: Lockheed Martin. Reprinted with permission.

By using this Cyber Kill Chain abstraction, there is a chance to detect an adversary if necessary detection mechanisms are in place, executed and correlated correctly for each step. For example, if a network intrusion detection system (NIDS) is monitoring the active remote connecting IPs for possible command and control (C&C) activity using threat intelligence feeds, it can easily alert the security staff for needed blocking actions. Again, if a host-based intrusion detection system (HIDS) can monitor the host activities (e.g., integrity checking for critical system files), it can alert the security team when a malicious event occurs on the host.

Network Intrusion Detection System

An NIDS performs analysis of passing traffic on the entire subnet and matches the traffic that is passed on the subnet to the library of known attacks. By using it effectively, an NIDS can help an organization be alert for attack attempts at various steps of the Cyber Kill Chain model. For example, if there is malware using malicious URLs/IPs, the NIDS will

Furkan Caliskan, CISA
Is the information security assistant manager in the Ziraat Bank A.S., the largest bank in Turkey. Before that, he worked as an IT auditor. He can be reached at *caliskanfurkan@gmail.com.*

catch it from network traffic using its signatures, relating to step 6. And if its vulnerability signature matches with current active traffic, this would be related to step 4.

Security Onion (SO) is a Linux distribution created for intrusion detection, network security monitoring and log management. It is based on Ubuntu GNU/Linux and contains well-known open-source network security software such as Snort, Suricata, Bro and Sguil in an integrated approach.[3] Since they are integrated with scripts for ease of use, it is very easy to install and start to use via its graphical user interface (GUI). It has three install options: standalone, sensor and server. If one wants to install sensor and server onto the same machine, the standalone mode can be used. For large networks, distributed installation could be the right answer for easy maintenance and central management of distributed sensors using built-in SaltStack configuration management support.

While using SO, one must use either port mirroring or network tap hardware devices to mirror all network traffic to the SO sensor machines. After the process of installation and enabling necessary settings, NIDS software components will start to see and analyze traffic against threats using built-in threat signatures.

Effective placement of the sensors in the network is also an important consideration to get a clear and accurate view of the network.

Figure 2 is an example of an NIDS alert reporting window using the Sguil application.

SO also comes with a useful log search tool called enterprise log search and archive (ELSA). It is built on syslog-ng, MySQL and Sphinx. It provides an easy-to-use, web-based query interface similar to the well-known Splunk application. It also supports email alerting, scheduled queries and graphing. Historical events queries and statistical results can be gathered using ELSA.

One of the most notable features of SO is its packet capture capability using the netsniff-ng tool. When choosing to configure the packet capture feature, whenever an intrusion detection system (IDS) alarm is generated, one can easily see and analyze the packet captures of the related event for detailed analysis. Since capturing all traffic consumes a large amount of hard disk capacity, organizations should plan carefully before installing their system. Network bandwidth value and log retention practices can be used as starting points for these plans.

Host-based Intrusion Detection Systems

HIDS is an intrusion detection system that monitors and analyzes the internals of a computing system.

Different from NIDS, HIDS monitors for host-based activities. For example, it can monitor the integrity of critical files, network connections, system logs, local firewall status, rootkit detection, brute-force attempts to the system and more.

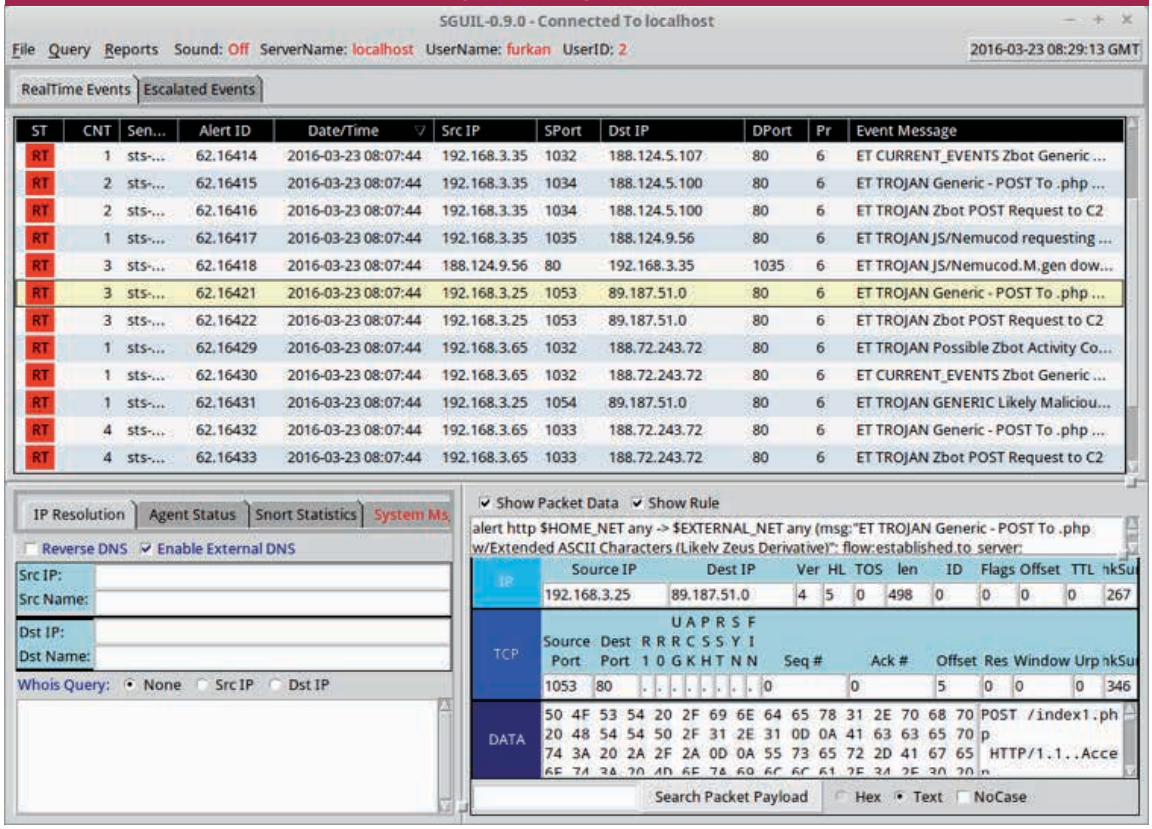
Using HIDS effectively can help an organization detect attack attempts in steps 5 and 7 in the Cyber Kill Chain. For example, step 5 uses the HIDS file integrity monitoring feature, which can detect whenever malware corrupts a system file or write itself to the registry and raise an alert.

One of the more well-known open-source HIDS projects is OSSEC[4] (**figure 3**). It supports Windows, Linux, Mac, BSD, VMware ESX systems and more.

Its capabilities include centralized management, real-time and configurable alerts, agentless monitoring, and integration with commercial security information and event management (SIEM).

It is also easy to customize since it is open source. OSSEC can be customized for purposes such as USB device white-listing and software vulnerability scanning.

Figure 2—Sguil Screen



Source: Furkan Caliskan. Reprinted with permission.

For deployment, an OSSEC server installation is needed. After this step, an agent can be installed on any host, and, given the agent key and IP information of the server, the agent will start to monitor the host it has installed and send the logs to the OSSEC server. This process can be automated for large deployments using methods such as Windows Management Instrumentation (WMI) and Puppet. There is also a project called Auto-OSSEC[5] for easy deployment.

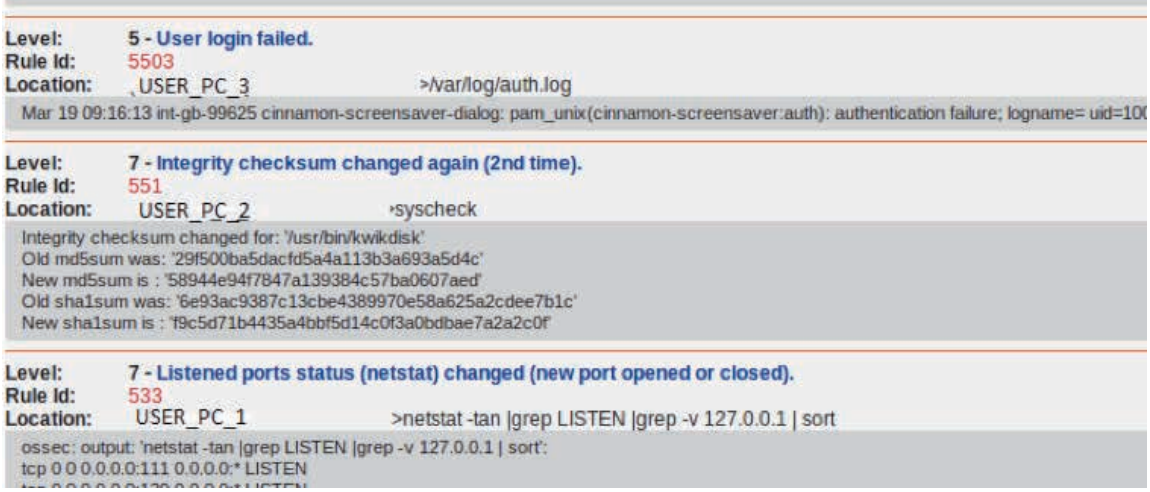
Honeypots

Many adversaries start their malicious activities by scanning external subnets and trying to exploit the weakest machine among an organization's public-facing hosts. A honeypot can be used to trick the adversary and entice him/her to try to exploit it. While an attacker is attempting a breach, honeypots report the event to the central security monitoring servers and help defend the production infrastructures.

When used effectively, honeypots can help organizations detect attack attempts in step 1 of the Cyber Kill Chain.

There is a Linux distribution called HoneyDrive, which is a bundle of honeypot software and is easy to use to get started. Another well-known open-source honeypot is Dionaea. It is a malware-capturing honeypot initially developed under The Honeynet Project's 2009 Google Summer of Code (GSoC).[6] Dionaea aims to trap malware exploiting vulnerabilities exposed by services offered over a network and, ultimately, to obtain a copy of the malware. It captures exploits offered over a network and stores details of these harmful events such as source IP, attack type and downloaded binary for later analysis. While an attacker is mounting an attack within this honeypot, the organization can launch a proactive defense using this information. By default, Dionaea supports Server Message Block

Figure 3—OSSEC Screen Shot



Source: Furkan Caliskan. Reprinted with permission.

(SMB), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Microsoft SQL Server (MSSQL) and Session Initiation Protocol (SIP).

Figure 4 shows Dionaea-captured malware and related hashes. These hashes can be submitted to *Virustotal.com* for more detailed analysis.

Figure 5 shows the malware source IPs for blocking purposes.

A major concern for honeypots is their correct placement in a network. While a public-facing honeypot is good for external attacks, extra internal honeypots for detecting lateral movements are also an effective effort.

Integrating Open-source Software and Making It All Work

One of the greatest challenges in cybersecurity is managing all security efforts centrally and making them easy to use. When an organization has numerous log sources and security systems, monitoring and managing them becomes more complex. This is a significant challenge for intrusion detection efforts, since all security logs should be carefully analyzed. If one is not able to detect an intrusion within a reasonable time frame, it can lead the entire system into a precarious situation. Therefore, using detection services effectively and in a combined manner is important for a well-protected IT infrastructure.

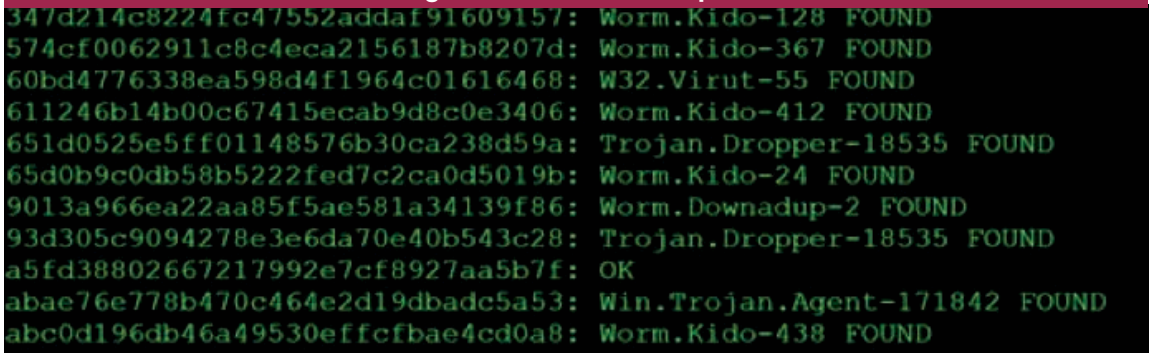
For central monitoring and dashboard purposes, ElasticSearch, Logstash and Kibana (ELK)[7] stack are well-known open-source solutions. They consist of three major components. ElasticSearch is a Lucene-based search server and it provides a distributed full-text search engine. Logstash is an easy-to-use log collection framework that works well with ElasticSearch. Kibana is the ultimate monitoring web user interface and helps visualize all the logs that come from Logstash and are indexed by ElasticSearch.

Using this stack, HIDS, NIDS and honeypot systems can send their data to ELK, and an analyst can correlate these data, create a dashboard for central monitoring and start taking quick actions (e.g., blocking attacker IPs using honeypot data, correlating HIDS and NIDS data to increase accuracy of a detected attack according to kill-chain abstraction). Unless using security data effectively, all the logging efforts are useless.

Conclusion

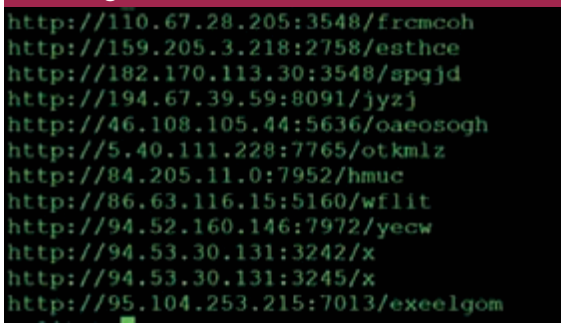
With today's fast-growing cybersecurity needs, building an effective cyberdefense infrastructure is a big challenge for many organizations. Building

Figure 4—Malware Samples



Source: Furkan Caliskan. Reprinted with permission.

Figure 5—Attacker IP Addresses



Source: Furkan Caliskan. Reprinted with permission.

a solid and accurate monitoring infrastructure will decrease the time to detect attacks since it will help gain the necessary insights from systems. A strong monitoring infrastructure will be able to correlate and use data accurately, enabling the security team to only work on important and accurate alarms.

This article provides an overview of open-source tools that can be used to deliver enhanced cyberthreat detection and defense to suit the resources of most cyberdefenders. In addition, these open-source software offerings provide significant flexibility and the benefit of a large support community. This can help to level the playing field for those tasked with guarding an organization and its "crown jewels." On the other hand, to utilize flexibility and low-budget advantages of open-source security solutions, the security team in charge of installing these solutions should know what they are doing and enjoy the open source community and culture. But open source is also a risk for companies that have small security staffs. Especially in the long term, a product that is no longer supported must be managed by the organization, resulting in unique challenges.

Endnotes

1 Mandiant, *2014 Threat Report,* M-Trends, April 2014, *https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf*
2 Lockheed Martin, Cyber Kill Chain, *http://cyber.lockheedmartin.com/solutions/cyber-kill-chain*
3 Security Onion, *http://blog.securityonion.net/*
4 OSSEC, *http://ossec.github.io/*
5 Kennedy, D.; "Tool Release: Auto-OSSEC—Automated OSSEC Deployment," Binary Defense Systems Update blog, 5 October 2015, *https://www.binarydefense.com/bds/tool-release-auto-ossec-automated-ossec-deployment/*
6 The Honeynet Project, Google Summer of Code 2009, *http://honeynet.org/gsoc2009*
7 Sissel, J.; "An Introduction to the ELK Stack," Elastic, *https://www.elastic.co/webinars/introduction-elk-stack*

Balancing the Cybersecurity Battlefield

History shows that women bring a different value to the work environment and improve overall operational effectiveness and financial results. In key financial metrics, companies with women on their boards of directors (BoDs) outperform those without women.[1] Recent research reports that if women were to have economic parity with men in the workplace, global gross domestic product (GDP) could increase by US $12 trillion by 2025.[2] When women are in leadership positions in significant numbers, "the bottom line improves—from financial success to the quality and scope of decision making."[3]

> **"People who think differently because of their gender, culture or training, attack and defend themselves differently and bring unique value to cybersecurity teams."**

Groups are collectively more intelligent than individuals—and that collective intelligence increases as the percentage of women in the group increases, as was learned when women began enrolling in the US military.[4] The military observed that "women provide a vital contribution to critical and creative thinking and decision making in the national security apparatus"[5] and that this capability is missing in many military units where currently there are no women.

Today, the cybersecurity industry is clamoring for women experts, painfully aware that only 11 percent of information security professionals are women, with about 56 percent of those women leaving this sector by mid-career.[6] Women bring specific value to the field of cybersecurity. With half the technology-consuming society being women, a strong representation of women as security practitioners would bring new and deeper insights into the social, psychological, emotional, technical and physical vulnerabilities that attackers are preying on today.

Cybersecurity, in essence, is about protecting information and systems against cyberattacks, cyberterrorism and cyberwarfare.[7] In times of war, governments utilize their entire population to overcome their enemies, often bringing in millions of women to step into roles previously done by men.[8] Excluding women in cybersecurity, where there is a severe skills shortage, is like excluding a battalion in war. It takes all resources to win a war.[9] Cybersecurity is an environment that is about staying ahead of the adversary, protecting assets more quickly than the threat vectors can exploit them, outpacing attackers and applying counterintelligence. Cybersecurity is a battleground of sorts. In war, everything that a country possesses is an asset and used to its own advantage, including the diversity of intelligence, skills and strategy. Women are able to reach the same results as their male counterparts if they get the same rights, privileges and possibilities.[10]

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.

Daksha Bhasker, CISM, CISSP
Has more than a decade of experience in the telecommunications industry working in various roles including business intelligence, strategy planning, business management operations and controls, governance, Sarbanes-Oxley Act compliance, complex technical solutions, security architecture, risk management, and cybersecurity. She is a senior network security architect with the network technology development team at Bell Canada and focuses on the security of emerging technologies.

Women should be seen as critical contributors to the cybersecurity industry. Cybersecurity hinges on the three pillars of people, process and technology, all of which can be exploited by attackers. People can be hacked easier than technology. People who think differently because of their gender, culture or training, attack and defend themselves differently and bring unique value to cybersecurity teams. Certain nation-states that are earning reputations as spawning grounds for hackers are not looking for the latest security credential, the most reputed academic degree or a professional licensure to practice in the field. These nation-states are willing to recruit and cross-train on the job. The counterresponse needs to be just as flexible, diverse and prolific. Nontraditional skills are important to the cybersecurity industry. For example, a political scientist may have insights into the agenda of nation-states and strategies that can be augmented to understand the motive and means of an attack. Similarly, a psychologist can offer threat intelligence that is based on human behavior and analysis. In cybersecurity, diversity brings value and expands the strength of the team.

“As career participation and advancement becomes a challenge, dissatisfied women tend to opt out of cybersecurity mid-career.”

Women can face numerous barriers to entry into the cybersecurity arena. Security industry opportunities that are commonly denied to women include:

- Inclusion in the cybersecurity community
- Equal opportunities for training and skills development
- Peer acceptance
- Acceptance as leaders
- Acceptance as engineering and technical experts
- Career advancement opportunities within the security industry

The present community of security professionals is a well-established, predominantly male community.[11] It takes extraordinary grit and effort for newcomers, especially women, to penetrate these networks. They face reluctant inclusion as they strive for acceptance by the community and hope that, at some point, their security careers will flourish. They seek equal participation opportunities, acceptance and integration. This is reflected in the meager 10 percent of information security leadership roles that are occupied by women today.[12] Cybersecurity is unique because it is a community of secrets, secret knowledge, classified information, association with dark hacker communities, trust circles and other secret resources. Security intelligence organizations around the world extol secrecy as their primary strength. A secret, by definition, is the exclusion of others in information sharing. Exclusion in the cybersecurity community can happen to anyone who does not fit the typical profile, including women.[13] Government security clearances do little in advancing women into security information professional circles, even when working around security communities in security organizations. This lack of advancement results in a high percentage of women being relegated to security-related essential, yet ancillary, functions such as administration, project or program management, business development, and marketing or communications. Because women often work in these roles, some may never quite penetrate to core security roles.[14] As career participation and advancement becomes a challenge, dissatisfied women tend to opt out of cybersecurity mid-career to areas where upward mobility is more accessible.[15]

Security professionals are rarely the most popular experts in a company regardless of gender. Most projects and initiatives consider security requirements to be impediments or necessary and painful overhead. Security professional expertise, opinions and budget requirements invariably experience responses of aggressive scrutiny and rigorous uproars, often by nonsecurity professionals.[16] Women have a tendency to overcompensate for being in a male-dominated field, a phenomenon referred to as the Madame Curie effect, meaning that women believe they must become more qualified and develop exceptional ability to compete with men in male-dominated science.”[17] This tendency, combined with the previously mentioned roadblocks, is especially taxing and has an effect on women who are developing new skills and working up a cybersecurity career path.

When work-related social events are male-dominant events, despite the best of intentions, women can continue to feel marginalized and struggle to bond with their cybersecurity colleagues. These situations can alienate and isolate a woman cybersecurity professional who does not have stereotypical male interests.

Aside from the very basic requirements of work-life balance and equal pay, there are a host of things that can be done to support, encourage and retain women in cybersecurity. The following efforts can help encourage women to participate in cybersecurity and advance toward leadership positions:

- Invitations and welcomes for women as professionals and allies into the field
- Open information sharing
- Training
- Career coaching
- Support
- Respecting differences in opinion based on professional background
- Partnership with mentors

The following steps can help to better incorporate women into the cybersecurity workforce:

- Make clear attempts to diminish the male-dominated stereotype of the cybersecurity industry. Both men and women are needed to win the cybersecurity fight. The image of cybersecurity professionals is predominantly male in the media. Overhaul such widespread imaging from hoodie-clad, keyboard pounding, acrobatic male ninjas to one of professional business etiquette, elegance and standards. Ensure a similar professional work climate where women can thrive in work-related social events as much as their male counterparts.
- In the workplace, welcome women as they develop subject matter expertise in core cybersecurity roles. Ensure a space of respect among all employees, especially those who do not have a history of working with women as peers and leaders.
- Encourage women by taking an active interest in their cybersecurity careers. Offer equal access to training and help eliminate barriers where women wish to pursue and sustain careers in cybersecurity. Provide access to professional networks and mentoring. Develop a discipline-specific mentor match program for women and offer established industry mentors for as long as this support is needed. Be aware of the Madam Curie effect and utilize mentoring as a channel to reduce this tendency. Encourage women, especially leaders in technology and engineering, to nurture newer entrants in the cybersecurity domain.
- Incentivize women to achieve leadership roles in cybersecurity and set clear paths of promotion for women employees. Enterprises can begin by maintaining transparent statistics on gender distribution in cybersecurity, tracking them against desired benchmarks. Communicating these statistics openly, while measuring them annually for progress, increases awareness of the gender-distribution gap and spurs desire for remediation. Reward women with financial incentives or incorporate recognition for attempting a nontraditional career in cybersecurity, and monitor their progress year after year. Create pro-women cybersecurity interest groups, networks and forums to enable women to have easy access to support, guidance and information. Establish exit interviews for women who choose to leave the field to understand and address identified shortcomings. Engage managers in attracting and retaining women employees.

Enjoying this article?

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

- Manage the culture of secret intelligence and required nondisclosures that is prevalent in the security industry with as much openness and transparency as possible. Help to prevent the misuse of information classification systems to prevent unnecessary exclusion of newcomers to the cybersecurity field. Create a mechanism that challenges such exclusion and openly discuss how to prevent this exclusion. Promote the need for training in the workplace to overcome unconscious biases against women in this industry.

Collectively, the goal of cybersecurity professionals is to win the cybersecurity war against attackers. Let women in the arena know that cybersecurity is their fight, too. Women on the cybersecurity battlefield are an asset.

Acknowledgement

The author would like to thank Tyson Macaulay, chief security strategist and vice president of security services at Fortinet, for many years of mentorship, guidance and shared insights.

Author's Note

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

Endnotes

1 International Labour Organization, "Women at Work: Trends 2016," International Labour Office, Geneva, 2016, *www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/---publ/documents/publication/wcms_457317.pdf*
2 Woetzel, J.; A. Madgavkar; K. Ellingrud; E. Labaye; S. Devillard; E. Kutcher; J. Manyika; R. Dobbs; M. Krishnan; "The Power of Parity: How Advancing Women's Equality Can Add $12 Trillion to Global Growth," McKinsey Global Institute, McKinsey & Company, September 2015, *www.mckinsey.com/global-themes/employment-and-growth/how-advancing-womens-equality-can-add-12-trillion-to-global-growth*
3 Seliger, S.; S. L. Shames; *The White House Project Report: Benchmarking Women's Leadership*, White House Project, USA, 2009
4 Haring, E. L.; "Women in Battle: What Women Bring to the Fight," *Parameters*, vol. 43, iss. 2, 2013, p. 27
5 *Ibid.*
6 Frost & Sullivan, "Agents of Change: Women in the Information Security Profession, The (ISC)^2 Global Information Security Workforce Subreport," *www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/Women-in-the-Information-Security-Profession-GISWS-Subreport.pdf*
7 Palo Alto Networks, Inc.; "What is Cyber Security," 2016, *www.paloaltonetworks.com/documentation/glossary/what-is-cyber-security*
8 Kabanenko, I.; *The Importance of Effective Utilization of Women at Arms*, Naval Postgraduate School, USA, March 2015
9 Online Highways LLC, "Rosie the Riveter," u-s-history.com, *www.u-s-history.com/pages/h1656.html.*
10 Rayman, N.; "Female Chess Legend: 'We Are Capable of the Same Fight as Any Other Man'," *TIME*, UK, 20 April 2015, *http://time.com/3828676/chess-judit-polgar-nigel-short-sexism/*
11 *Op cit,* Frost & Sullivan
12 *Ibid.*
13 D'Hondt, K; *Women in Cybersecurity*, Harvard Kennedy School, USA, 2016
14 *Op cit,* Frost & Sullivan
15 Morbin, T.; "RSA: Women Breaking the Glass Firewall," *SC Magazine UK*, 21 April 2015, *www.scmagazineuk.com/rsa-women-breaking-the-glass-firewall/article/410089/*
16 Sethi, R.; "Managing Security Requirements in Agile Projects," *InfoQ*, 4 June 2012, *https://www.infoq.com/articles/managing-security-requirements-in-agile-projects*
17 Natural Sciences and Engineering Research Council of Canada, "Women in Science and Engineering in Canada," November 2010, *http://publications.gc.ca/collections/collection_2012/rsgc-serc/NS3-46-2010-eng.pdf*

feature

Planning for Information Security Testing—A Practical Approach

Once approval to perform an information security audit and, most likely, a penetration test (pen-test) of an organization's networks and systems has been obtained, then what? Where to start? Planning it requires a great deal of thought and consideration and, for first timers, this task can be quite daunting. Poor planning can have serious consequences for the network, causing unwanted business disruption and, in the worst-case scenario, permanent harm. Depending on the risk appetite of the organization, the scope of the pen-test could be drastically different.

The first thing one needs to understand is that information security auditing is not a one-size-fits-all type of engagement. It is reasonable to start small and slowly progress to more complex engagements. It is also important to note that different networks and applications can progress in different stages.

For example, if an organization has a supervisory control and data acquisition (SCADA) system that has never been tested, nor even scanned for vulnerabilities, one might want to consider not starting the information security testing by deploying a full-blown pen-test. It would be prudent to start with a vulnerability assessment to test the waters and use the results to harden the system for a future pen-test.

The model in **figure 1** proposes a guideline for maturing testing activities by correlating different combinations of the "rules of engagement," which will be covered in detail in this article, with risk tolerance. These preset combinations can be used as a starting point.

Before considering the rules of engagement, it is important to know the types of information security testing:

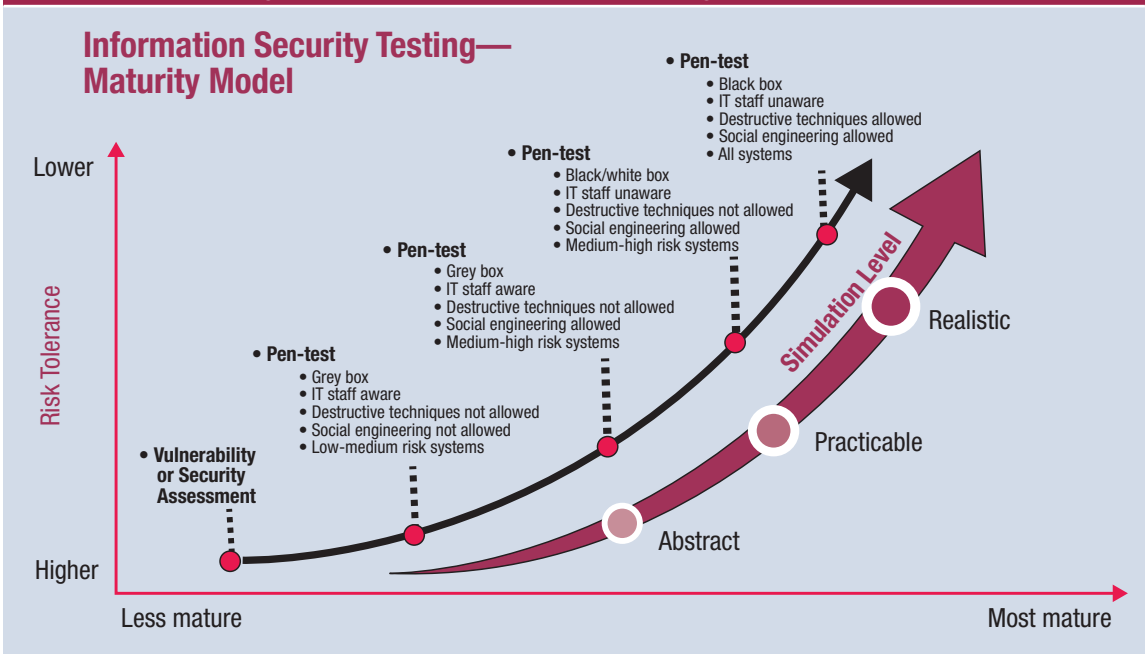
- **Vulnerability scan**—This scan examines the security of individual computers, network devices or applications for known vulnerabilities. Vulnerabilities are identified by running a scanner, sniffers, reviewing configurations, etc. Vulnerabilities identified are never exploited. This test tends to be less disruptive and also inexpensive when outsourced.
- **Security assessment**—This builds upon the vulnerability assessment by adding manual verification of controls to confirm exposure by reviewing settings, policies and procedures. It has a broader coverage. Assessment of physical security safeguards would be covered here.
- **Penetration test**—This happens one step ahead of a vulnerability assessment. It takes advantage of the known and unknown (e.g., zero-day attacks) vulnerabilities. It also makes use of social engineering techniques to exploit the human component of cybersecurity. Note that vulnerability assessment is included in pen-testing. Vulnerability assessment is the starting activity that would be scheduled to look for vulnerabilities. It is called the discovery phase (or reconnaissance) of the test cycle. Penetration testers must run a vulnerability scan to identify weak points to be exploited.
- **Social engineering**—Although social engineering is actually a pen-test technique, many companies not yet ready for a pen-test might opt to only deploy a phishing email campaign, for example, to verify how many of their users are vulnerable to this technique and require further training. Results

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.

Karina Korpela, CISA, CISM, CRISC, CISSP, PMP
Is the IT audit manager at AltaLink, a Berkshire Hathaway Energy Company and Alberta, Canada's largest transmission provider. Korpela has more than 15 years of international experience with IT audits, cybersecurity assessments, performing data analytics and developing continuous controls monitoring applications for many different business processes. She began her career at Coopers & Lybrand as a system administrator and she was later invited to join its Computer Audit Assistance Group (CAAG) as an IT auditor. She can be reached at *karina.korpela@altalink.ca.*

Paul Weatherhead, CISSP
Is the vice president and chief technology officer at Digital Boundary Group, an information technology security assurance services firm serving clients throughout North America. He is frequently called upon to advise North American clients in the financial services, law enforcement, municipal and provincial government, utilities, and professional services sectors on corporate IT security and network intrusion investigations. Over the past 17 years, Weatherhead has focused on network security and threat management consulting, having performed more than 400 IT security assessments in Canada, the United States and the United Kingdom. He regularly conducts network security training courses and has instructed at the Canadian Police College.

Figure 1—Information Security Testing Maturity Model



Source: K. Korpela. Reprinted with permission.

are reported, but information gathered is never used to penetrate the network.

> **"Ideally, pen-tests can be run just once a year while vulnerability assessments should be performed more frequently."**

An assessment is not better than a pen-test or *vice versa*. They provide different outcomes and value. Their applicability will depend on the organization's risk tolerance, systems' sensitivity and the security infrastructure maturity. But, ideally, pen-tests can be run just once a year while vulnerability assessments should be performed more frequently. Both the vulnerability scan and pen-tests can be performed against the internal and external systems and network devices. They both can be general in scope or focused on specific areas. **Figure 2** shows areas of focus and their applicability.

Rules of Engagement

These rules should be thought of as the sound adjustment knobs in a home theater system. One combination might be better for a smaller room in which cable TV is being watched, while another combination might be better for a bigger room where a DVD is being played. Once these rules are understood, it gets easier to decide the objectives and scope for testing.

A different set of combinations can be applied to each system within the scope. In one highly sensitive network, one may only run a vulnerability scan and in other, more robust networks, one might run a more realistic pen-test. Or, the sound can be tuned as the

Figure 2—Focus Areas				
Focus Areas/Types	Vulnerability Scan	Security Assessment	Pen-test	Social Engineering
Routers and switches	I	I	I	-
Firewall	I	I	I	I
Intrusion detection system (IDS); intrusion prevention system (IPS)	I	I	I	I
Wireless network	I	I	I	-
Denial of service (DoS)	O	O	O	-
Password cracking	-	O	I	-
Social engineering	-	O	I	I
Stolen mobile devices	-	I	I	-
Application	I	I	I	-
Physical	I	I	I	I
Database	I	I	I	-
Voice Over Internet Protocol (VoIP)	O	I	I	-
Virtual private network (VPN)	I	I	I	-
Email security	I	I	I	I
Security patches	I	I	I	-
Data leakage	-	I	I	I
Telecommunication and broadband communication	I	I	I	-
I = Included | O = Optional | - = Generally not included				

Source: K. Korpela and P. Weatherhead. Reprinted with permission.

testing occurs. For example, when the tester does not succeed in penetrating the first line of defense, the test can be considered completed or additional information, or even access, can be provided to enable the tester to bypass it and restart testing from there. In this way, additional vulnerabilities can be identified should a future attacker manage to breach the first level of defense.

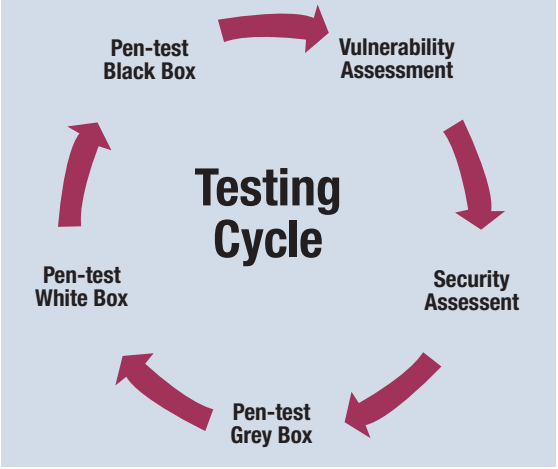
The combination chosen depends on the risk tolerance and the maturity of a company's cybersecurity processes. Nevertheless, these rules allow for flexibility in adjusting the test plan according to the systems and networks in scope.

It is important to keep in mind that in the always-evolving world of information security, reaching the highest maturity level and, as a consequence, becoming complacent can be dangerous.

Even though a higher maturity level is required to perform the most realistic testing, it comes with a price as it can give a false sense of security. A full-blown black box allows the tester to assess only the first line of defense at the time of testing. But what if a zero-day attack that exploits vulnerabilities behind that first line of defense occurs? How would the internal systems respond? Andy Grove's quote on complacency is very much applicable to information security: "Success breeds complacency. Complacency breeds failure. Only the paranoid survive."[1]

It is essential to apply a cyclical approach to information security testing as suggested in **figure 3**.

Figure 3—Testing Cycle



Source: K. Korpela. Reprinted with permission.

Strategy: Internal vs. External

The strategy determines whether testing should be performed from outside of the network such as from the Internet, or from inside the network or both.

> **"Not announcing pen-testing helps the organization to check the security threats that arise due to human errors and ignorance."**

- **External**—This is, perhaps, the most widely-used form of pen-testing. It addresses the ability of a remote attacker to get to the internal network. The goal of the pen-test is to access specific servers and the "crown jewels" within the internal network by exploiting externally exposed servers, clients and people.
- **Internal**—Contrary to what management usually thinks this is, it is not a strategy applicable to vulnerability assessment work only. Pen-tests can be run internally when the goal is to simulate what would happen if a company's own employee attempted to carry out an attack from within or if an attacker managed to gain access to a network. The target is typically the same as external pen-testing, but the major differentiator is the "attacker" either has some sort of authorized access or is starting from a point within the internal network. Internal testing can help businesses identify weaknesses in their second or third lines of defense, as an insider attack will bypass perimeter safeguards altogether. Internal testing can answer questions such as, "How well segregated is the network?" "Is the patching management effective?" If the attacker is in a network segment, internal testing can determine whether he/she can see any other segments, what he/she might see on those other segments, and what activities he/she can carry out.

Announcement: Covert vs. Not Covert

This section of the rules of engagement is used to document whether or not tests will be announced.

- **Not covert**—These pen-tests are those performed with the knowledge and consent of IT staff and, of course, upper management. The next decision is whether to defend the network against testers. This option, also known as the Blue Team vs. Red Team approach, can cut the test short as the defending team could just shut down the network once it has detected the testers. In order to maximize the pen-test, it is recommended that specific instructions be given that no action to stop the testers is to be taken in response to the pen-test at the time and duration arranged. This can be a great opportunity for the defending team to learn how to think like hackers by monitoring the attack and documenting which systems and sensors trigger alerts during the exercise.
- **Covert**—This option is also known as Red Team, and it involves performing a pen-test without the knowledge of IT staff, but with consent from upper management. Not announcing pen-testing helps the organization to check the security threats that

arise due to human errors and ignorance. It also examines the agility of the security infrastructure and the responsiveness of the IT staff.

Type: Grey vs. White vs. Black Box

Organizations must decide whether to share information about the system and networks with the assessing organization (tester). Those decisions are typed as:

- **Black box**—No information is shared with the testers. This simulates an external attack where testers will spend more time in the reconnaissance phase and, because of that, it tends to take more time and be more expensive.
- **Grey box**—Some information is provided to the testers—that which hackers would, perhaps, obtain when using reconnaissance tools or after obtaining access to local area networks (LANs). This decreases the time spent by the testers and, therefore, cost as well. Information given does not compromise the pen-test's validity. Examples of such information would be a list of out-of-scope hosts or a lighter version of network topology.
- **White box**—All information that testers need to exploit vulnerabilities is provided. This option is preferable when:
  - The scoping task is left to the testers to determine
  - A complete audit of its security is taking place
  - Organizations want to simulate an attack from an inside threat, such as a disgruntled IT employee who would already have access to such information

There is no right or wrong type, and all options can be done with or without the knowledge of IT staff. Black box offers a more realistic test from the outside hacker perspective, but white box has the potential to be more devastating because the testers will have the knowledge of what is important within a network and where it is located—something that external attackers do not usually know from the start. An internal attack approach will not always require a white-box type

Figure 4—NDT vs. DT Techniques

Nondestructive Techniques (NDT)	Potentially Destructive/Disruptive Techniques (DT)
• Passive research, including employees' social media accounts • URL spoofing and phishing • Physical/on-site social engineering • Remote/logical social engineering • Read corporate emails • Network mapping and operating system (OS) fingerprinting • Caller identification (ID) and email address spoofing • Network sniffing • **Vulnerability scanning*** • Network monitoring tools • Ping tools • Promiscuous mode detection tools • Cryptography tools • Domain Name System (DNS) tools • IP spoofing • **Port scanners*** • Firewall tools • Man-in-the-middle attacks • File manipulation • Poisoning of file-share networks • Investigation of personnel backgrounds • Scenario analysis	• ICMP flood (Smurf attack, Ping flood and Ping of death) • Teardrop • Application level floods • Distributed, reflected, degradation of service • Unintentional, DoS level II • Blind DoS • Tampering with system logs with the intent of deleting/ disguising trails • DoS attacks • Buffer overflow • Forced reinstall and restart • Brute-force attack • Structured Query Language (SQL) injection

*Vulnerability and port scanners are, by nature, nondestructive if configured appropriately.

Source: K. Korpela and P. Weatherhead. Reprinted with permission.

Enjoying this article?

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

of testing. For example, if the objective is to test what a hacker could do if he/she just walked into the company's office and plugged in a computer, then an internal testing strategy with a black-box testing type could be selected.

Technique: Nondestructive vs. Destructive

It is import to inform the testers which techniques will be allowed during the engagement. When nondestructive (NDT) methods are selected, testers will set up their tools to avoid causing a denial-of-service (DoS), for example, or any other attack that could disrupt normal business operations. NDT provides a proof of concept, but does not prove it. **Figure 4** lists commonly used techniques. These techniques should be discussed with the testers in advance when the organization notifies the testers which tests may be used during the engagement. Regardless of the technique selected, it is recommended to explicitly state which tools and techniques will be allowed and which will not. For example, there are attacks and tools that can be destructive by nature, but can be "tuned down" by the tester so that they will not cause a DoS, buffer overflow or any system to shut down.

> **"It is recommended to explicitly state which tools and techniques will be allowed and which will not."**

A very valid point to be addressed here is the use of open source and in-house developed tools by the tester for vulnerability assessments and pen-tests. Both types of software come with risk and benefits.

Open source means that the source code is available to all potential users, and they are free to use, modify and redistribute the source code. Considering that the source code is accessible, testers can often tweak the software, plug exploits and remove unnecessary features. This can improve efficiency, speed and security. The most commonly used open source software for information security testing is Linux Backtrack and Kali, which comes with a large community supporting it and, therefore, developing enhancements and versatile add-ons.

As for in-house developed tools, it is very likely that most experienced testers develop tools themselves to cover the gap between commercial and open source. An example would be the development of a tool to scan the network without locking Structured Query Language (SQL) accounts, which may happen when using a commercial scanner.

The risk of these tools disrupting business or causing a propagation of malware could be controlled by:

- Not allowing installation on the target systems
- Running the tool(s) against nonproduction systems or test systems first
- Ascertaining that the tester acquired open source tools from trusted sites and performed a Secure Hash Algorithm 2 (SHA2) checksum to verify integrity
- Ascertaining that the tester has used a valid software development framework, which could include peer review, for in-house software
- Ascertaining that the tester has appropriately patched and upgraded software

And for social engineering techniques such as Caller ID and email address spoofing, one may choose to allow it to be deployed passively, that is, only for the purpose of gathering information during the reconnaissance phase. Other considerations include whether testers will be allowed to break into the company's premises, break into employees' homes and/or hack employees' social media accounts.

These tools and techniques can be flagged as allowed only with prior consent and can be handled on a case-by-case basis.

Statement of Work

Aside from assigning well-skilled and experienced professionals to perform the test and knowing the rules of engagement, it is also essential that a test plan be developed to establish the parameters such as objective, scope, assumptions and risk.

Using a template as shown in **figure 5** provides the tester with clear expectations for the testing and transparency and outlines the plan in a nontechnical way in order for upper management to approve it.

Background

When developing the test, it is critical to keep in mind that it will require approval from upper management (senior executive level is preferable) and, therefore, the background should provide them with context by detailing the need for performing this type of work, a summary of previous tests, the rationale for the objective and scope selected, changes made to the IT environment, new threats, and so on. Here is where the justification for using a third-party assessing organization could be provided.

Goals

What will be the area of focus (refer to **figure 2**) for the test? Or, will it be general? Is there a particular threat against which the company needs to test its controls? For example, an organization may choose to test against one particular vulnerability such as the Heartbleed bug, or it may choose to test if it is possible for hackers or a disgruntled employee to obtain unauthorized access to the enterprise resource planning (ERP) systems and wire money to an off-shore bank account. But for most companies, good starting goals could simply be: Is the organization secure? Is the organization compliant?

To ensure that the testing adds value to the organization, it is crucial to identify and understand the areas of risk and/or the potential weakest

Figure 5—Pen-test Plan Template

BACKGROUND:
GOALS:

B1. Objective

A. SCOPE:
- In scope
- Out of scope

Rules of Behavior

B. STRATEGY:
C. TEAMING:
D. TYPE:
E. ANALYSIS TECHNIQUE:
F. SUCCESS FACTORS:

B2. Objective

A. SCOPE:
- In scope
- Out of scope

Rules of Behavior

B. STRATEGY:
C. TEAMING:
D. TYPE:
E. ANALYSIS TECHNIQUE:
F. SUCCESS FACTORS:

SCHEDULE
RISK AND CONTINGENCIES
ASSUMPTIONS
DELIVERABLES
CONTACTS
APPROVALS
ADDENDUMS

Source: K. Korpela and P. Weatherhead. Reprinted with permission.

link in fending off cyberattacks. Risk assessment frameworks can be helpful in identifying the goals for testing. Organizations that have performed a business impact analysis could use this as input into identifying specific areas of business risk and adjusting the testing accordingly. For example, an organization that identifies research and development data as its most important assets could develop a test plan that includes attempts to gain unauthorized access to the data. Organizations may wish to involve the third-party testers in this phase, as they may be able to suggest current industry trends.

Objective

It is advisable to provide testers with specific objectives. What should testers do once they obtain access to the network? Should they leave crumbs? Should testers find a specific application and create user accounts? Those objectives will become clear and easy to define as the organization gets familiar with its systems and cyberrisk. A good place to start is to define objectives related to the first and/or second lines of defense such as firewalls.

Scope/Out of Scope

The testing criteria can be either a full-scale test for the entire network and systems or a more narrowly defined test for target devices such as web servers, routers, SCADA, firewalls, DNS servers, mail servers and file transfer protocol (FTP) servers as listed in **figure 2**. To determine the extent to which the testing should be done, these questions should be asked:

- What will be tested?
- In the case of social engineering only, which employees are in scope?
- From where it will be tested?
- When should the test not be performed?
- Are production systems out of scope?
- Which hosts are out of scope/restricted?
- By whom will it be tested?

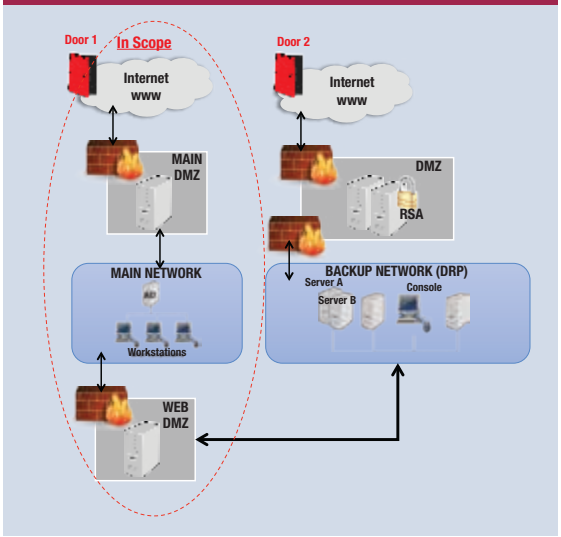
Most assessing organizations will use the number of hosts, users, external IPs and locations in scope to calculate the engagement's cost.

It is helpful to have a nontechnical diagram that shows the networks in scope and testing starting points (doors) (**figure 6**). It will provide upper management with additional context and visual understanding of the scope.

Success Factors

When will the test be considered a success? Is it when the tester breaks into the network or when a breach is not possible? Is penetrating the network enough proof of the need for stiffening controls?

Figure 6—Example of Nontechnical Network Diagram



Source: K. Korpela and P. Weatherhead. Reprinted with permission.

The measurements defined in the Goals section of this article could be repeated here to determine, in detail, which activities must be performed by the assessing organization or even by the IT staff to consider the test successful.

Schedule

If the issue of timing is not resolved properly, it can be catastrophic to an organization. It is easy to imagine the uproar if a DoS test was performed on a university on the day its students are scheduled to take their online examinations. This is an example of poor timing as well as lack of communication between the penetration testers and the university. Good planning and preparation will help avoid such bad practices.

A pen-test does not last forever and, therefore, it is important to be explicit in the plan of a finite period for testing. The plan should also request that testers notify organization stakeholders when testing has begun on the day it was agreed to commence.

Contacts

A contacts list should be developed to identify all the key people (including their names, roles, email addresses and telephone numbers) participating in the planning, coordination and execution of tests. Those who should be contacted first in case of concerns, changes and emergencies should be clearly identified. The list should not include staff that is not meant to know about the testing; their inclusion might confuse the assessing organization.

Risk and Contingencies

All the possible risk factors and their likelihood of occurring during the test period must be specified. An example of a risk might be that the testing activities may inadvertently shut down the network causing interruption of daily business functionalities. Once risk factors have been listed, a table can be prepared with the preventive controls and mitigation strategies in case the risk materializes (**figure 7**).

Deliverables

It is critical to provide context and background to the results. For example, if the number of vulnerabilities reported has doubled from last year, it is important to add the total number of end points scanned to the results.

Reporting to management must be part of the pen-test engagement. Testers will often put together a detailed and very technical presentation summarizing the test results. Best practice is to have one technical, detailed presentation for the IT team (chief information officer [CIO] and key managers) and a separate, shorter presentation for the executives that summarizes the tests and focuses on business risk impact and mitigation plans. Best practice is to have the executive summary created by internal audit.

> **“Risk assessment frameworks can be helpful in identifying the goals for testing.”**

Examples of deliverables to be considered include:

- A detailed technical report on the vulnerabilities of the system explained in a way that is understandable by senior management. This report should also include, but is not limited to:
  - Outcome of the test in technical risk terms
  - Indication of the skills necessary to exploit the vulnerabilities (script kiddies, worm/virus writers, security researchers, professional hackers or hacktivists)

Figure 7—Example of a Risk and Contingency Plan

Risk	Risk Tolerance	Preventive Controls	Probability (%)	Mitigation Strategy	Residual Risk
Testing activities may inadvertently shut down the network causing interruption of daily business functions.	Medium	Attacks that could cause the network to shut down and hosts that could be sensitive to logical tempering are disclaimed as out of scope.	10%	Invoke the business resumption plan.	Low

Source: K. Korpela and P. Weatherhead. Reprinted with permission.

  - Explanation of false positives
  - Short-term (tactical) recommendations
  - Root-cause, long-term (strategic) recommendations
  - Security improvement action plan
- A report listing the cybersecurity controls (processes and/or technologies) currently in place that are working effectively and their categorization against industry best practices (weak, moderate, strong)
- A report showing the social-engineering methods used and the success rates at the company being assessed

Approvals

Obtaining consent from upper management before conducting a pen-test is vital. Depending upon organizational legal requirements, a separate release and authorization form may be required (in addition to the rules of engagement) that states that the assessing organization will be held harmless and not criminally liable for unintentional interruptions and loss or damage to equipment.

> **"It is critical to provide context and background to the results."**

Other Considerations

It is also recommended that plans explicitly state details regarding the following issues:

- **Scope**—Employees/locations out of scope for social-engineering activities
- **Report sanitization**—There is risk involved in the potential circulation of an unsanitized version of the report that includes the company's IP addresses and other important information. Organizations may want to consider having two versions of the report for different audiences and distribution methods.
- **Distribution method**—Organizations may want to consider using only secure methods to communicate unsanitized plans and other information being provided about the systems and networks.
- **Confidentiality**—The assessing organization must be made to understand that any information or data obtained during the pen-tests will be treated as confidential and will be returned or destroyed accordingly after the tests.

References

EC-Council ECSA, *LPT Courseware Manual*, v4, vol. 2

Scarfone, K.; M. Souppaya; A. Cody; A. Orebaugh; *Technical Guide to Information Security Testing and Assessment*, National Institute of Standards and Technology, NIST Special Publication 800-115, USA, September 2008, *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf*

Tipton, H. F.; M., Krause; *Information Security Management Handbook, 6th Edition*, CRC Press, USA, 2007

Chan Tuck Wai, "Conducting a Penetration Test on an Organization," SANS Institute InfoSec Reading Room, 2002, *https://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67*

SANS Institute, "Guidelines for Developing Penetration Rules of Behavior," InfoSec Reading Room, 2001, *https://www.sans.org/reading-room/whitepapers/testing/guidelines-developing-penetration-rules-behavior-259*

SANS Institute, "Security Concerns in Using Open Source Software for Enterprise Requirements," InfoSec Reading Room, 2009, *https://www.sans.org/reading-room/whitepapers/awareness/security-concerns-open-source-software-enterprise-requirements-1305*

Endnotes

1 Grove, A. S.; *Only the Paranoid Survive: How to Exploit the Crisis Points That Challenge Every Company*, Crown Business, USA, 1999

A Critical Perspective on Safeguard Selection Processes

Safeguards have become an essential part of every IT environment. As companies become more reliant on modern technology, they also have to face more vulnerabilities that must be handled efficiently. However, the selection of an appropriate safeguard can be challenging.

The various attributes and as much preliminary information as possible should be considered in the selection process. A systematic process of review and decision-making techniques helps to avoid inopportune justifications that are based on hastiness and poor preparation. Stakeholders should be aware of possible problems that can occur during the selection process, including any general shortcomings in the decision-making techniques employed. The selection process can also be affected by unforeseen cost, time and quality issues.

During the preparation, execution and quality assurance of the safeguard selection, a critical perspective should be used for pointing out possible problems.

Motives

Sometimes, the selection of a safeguard is based on faulty justifications. The causes of those justifications are often fear, uncertainty and doubt. Some unethical product representatives may even enhance these conditions to increase their sales through the use of comprehensive and often subtle and subliminal disinformation. Neutral sources are often referred to, but the significance of the reference is greatly exaggerated or presented in the wrong context. The result can be an expensive and inadequate investment in a suboptimal safeguard.

On the other hand, hastiness and poor preparation can also lead to faulty justification. If managers must react quickly because of severe threats, they may not have the opportunity to consult with appropriate experts prior to the investment decision. In cases such as this, poor decisions are very common. Subsequently, the expenses are high without generating the expected security enhancement.

The best way to avoid poor justification is a well-thought-out safeguard selection process that involves experts. To find the most appropriate safeguard, the decision maker must be able to evaluate several safeguards and identify and select the best one. The selection of a safeguard is based on the evaluation of multiple qualitative or quantitative attributes. Therefore, a process should cover the comparison of these attributes and the evaluation of the existing safeguards. The attributes are weighted so that the evaluation of the safeguards can be performed considering the specific situation and characteristics of the company.

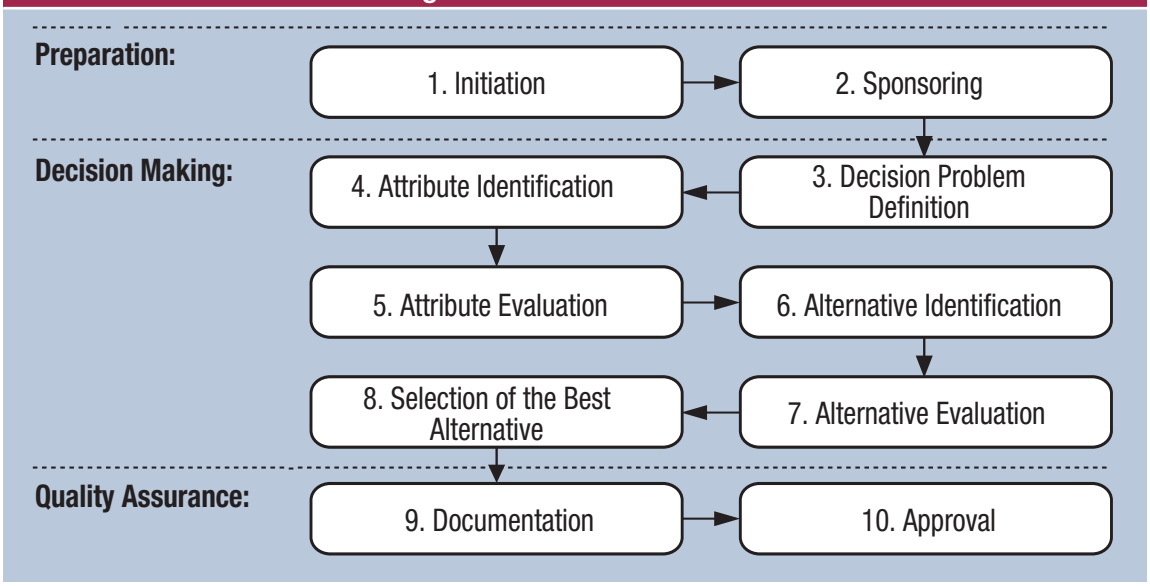
The advantages of using a structured process over an unsystematic process include the following:

- The problem to be addressed must be defined before actually starting the evaluation.

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.

Stefan Beissel, Ph.D., CISA, CISSP, PMP
Is a senior information security expert who has worked at international companies in the finance, banking and commerce sectors for nearly 15 years. He is the author of multiple books and journal articles and has trained and lectured professionals, undergraduate and graduate students on information security and related topics.

Figure 1—Selection Process



Source: S. Beissel. Reprinted with permission.

- The identification and use of attributes facilitate the consideration of different perspectives within the evaluation.
- The selection process is organized with transparent steps and it is divided into aggregated subparts.

How the safeguard selection process is composed in detail depends on the company that develops and uses the process. In general, a structured process includes the preparation of the selection, the narrowing of the decision making and the activities for quality assurance (**figure 1**).

Each phase in the selection process can be further described as follows:

1. The initiation should be based on a solid reason for a specific safeguard selection with consideration of the stakeholders' perception of information security.
2. The sponsoring phase is used to get acceptance and support from executive management and select an appropriate sponsor.
3. The first step of decision making—defining the problem to be solved via the decision—aims to gain a thorough understanding of important elements (e.g., strategy, scope, assets, risk, protection, stakeholders) that will factor into the decision-making process.
4. During attribute identification, the decision maker must consider all relevant attributes that will be used for evaluating the safeguard alternatives.
5. Afterward, the decision maker must also determine how important each attribute is by performing an attribute evaluation.
6. Alternative identification is a crucial step and its outcome depends on the information that can be gathered about available alternatives via research of external knowledge.
7. The alternative evaluation is needed to evaluate the alternatives with regard to the relevant attributes and to create a subsequent ranking.

8. Based on the ranking, the best alternative (the alternative with the highest rank) can be identified.
9. Documentation ensures that the decision-making process can be understood by third parties, who can then use it to gain insights into the substeps and to gather indications about the substeps' correctness and completeness.
10. A separate approval, mostly by senior management, allows an additional quality check so that the results are not used thoughtlessly.

Decision-making Techniques

When faced with selecting among alternatives that have multiple attributes, the most common decision-making techniques are simple additive weighting (SAW)[1] and the analytic hierarchy process (AHP).[2] Both techniques are based on the same general sequence:

- Define the decision problem.
- Identify and evaluate the attributes.
- Identify and evaluate the alternatives.
- Select the best alternative.

The differences lie in the calculations of the evaluations. SAW uses calculations that are based on independent evaluations of separate attributes and alternatives, while AHP uses pairwise comparisons of two attributes or alternatives at a time. Since these different techniques include different calculation methods, the same alternatives can lead to dissimilar results, e.g., an alternative could be the most appropriate when using SAW, but only a second choice when using AHP. Evaluation results with alternative scores that are close to each other can lead to this situation.

There are also other decision-making techniques in the scientific field, e.g., the analytic network process (ANP), the technique for order preference by similarity to ideal solution (TOPSIS) and data envelopment analysis (DEA). However, SAW and AHP provide the best balance between an ease of understanding and thoughtful application for practical use in the enterprise sector.
Like most multi-attribute decision-making techniques, SAW and AHP also come with potential disadvantages that should be known and, if possible, avoided including:

> **"SAW and AHP provide the best balance between an ease of understanding and thoughtful application for practical use in the enterprise sector."**

- The techniques can be manipulated in many possible ways. Because precise figures and calculation methods are used, objectivity can be faked. Due to the general subjectivity in the weighting and evaluation of attributes, the result can be significantly affected by undetected manipulation. Although the subjectivity can be reduced by including experts, it cannot be eliminated. In addition, the decision maker has the freedom of choice regarding the attribute selection.
- The addition of the subscores implies the independence of the attributes. However, dependencies between attributes, such as competitive or complementary relationships, often cannot be completely avoided. For example, the protection level and vendor support of a safeguard are often closely related. Consequently, there is a

risk that strongly dependent attributes lead to an unintentional over- or undervaluation of alternatives.

- The aforementioned addition also leads to a possible substitutability of the subscores. In particular, subscores that are derived from very bad characteristics of an alternative can be substituted with subscores from very good characteristics. Therefore, single attributes might be neglected. Even if the attributes are divided into exclusion and comparison attributes, this problem can be only partially eliminated. The comparison attributes are still affected by a possible substitutability.
- The overall result can be subject to leveling. In this case, it is likely that the weaknesses or strengths of the best alternative are no longer recognizable in the result. The more attributes considered, the more likely the results are positioned in the middle region of the range of the possible overall scores.
- Due to the assessment of alternatives with individual attributes, the overall problem will be broken down into many single problems. This decomposition is questionable because, first, the overall problem is no longer clear and, second, there is a risk that the assessments of many single problems lead to an undesirable overall assessment. If the attributes are in a competitive relationship to each other, the improvement of a subscore regarding a single attribute can lead to the evaluation of a competing attribute resulting in a lower subscore. For example, the reduction of false positive events in biometric access control systems often leads to an increase of false-negative events.

In addition to the disadvantages of the particular decision-making technique, general difficulties can occur during the selection of a safeguard. The company can be influenced by cost, time and quality aspects while making the decision. For example, the company might focus on the safeguard costs and neglect the costs of the selection process. Various events or activities might slow down the selection process for unforeseen reasons and delay the planned selection. Errors and overlooked information might cause quality issues in the selection results.

Problem Identification

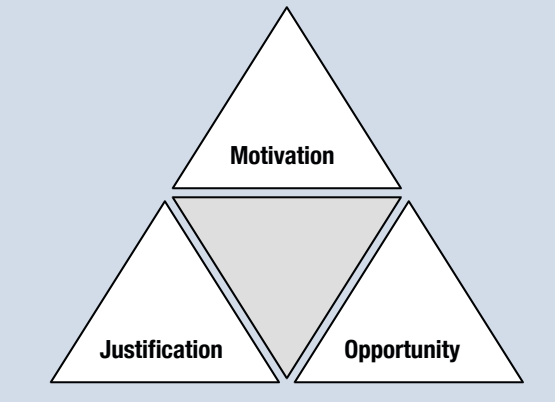
The result from the selection process should be checked critically for any indication that implies potential problems in the process. Only results that are free of obvious errors and doubts should be approved and used for acquiring and implementing the selected safeguard. Among other things, the following scenarios can indicate problems in the selection process:

- The decision problem, including the strategy and protection requirements, has changed during the process or it was not analyzed sufficiently from the beginning. Therefore, senior management has to assume that the result does not completely meet the underlying problem.

> **“The safeguard selection process is crucial and should not be based on faulty justifications.”**

- Internal conditions (e.g., resources and schedules) have been overlooked or changed so that the recommended solution would actually not be the best solution. Unfavorable internal conditions can also lead to major problems in implementation.
- External conditions (e.g., laws, standards, market conditions) have changed so that the initial decision-making process is not accurate anymore. Certain environmental factors can lead to new requirements in the planning or potential problems in the acquisition, implementation and operation of the safeguard.

Figure 2—Fraud Triangle



Source: S. Beissel. Reprinted with permission.

- The decision-making process was incorrect or incomplete, resulting in errors that can significantly influence the evaluation results. If an error happens to be related to a critical attribute or evaluation, the ranking of the alternatives can even be changed. In this case, the selected alternative would not be the best alternative.
- The documentation of the decision-making process is not sufficient in regard to scope and quality. If the documentation is insufficient or missing, senior management can reject the result of the selection process.
- Abuse of power might have influenced the decision-making process. Often, this abuse can legally be categorized as fraud, which is generally caused by motivation, justification and opportunity, as described in the fraud triangle (**figure 2**).[3] The attribute evaluation is one of a number of activities that might have been exploited with abuse. Senior management should be aware of potential weaknesses or missing control measures in the safeguard selection process. Indications for abuse should be taken seriously. If abuse seems to have impacted the result, senior management should reject it. Common indications for abuse are discrepancies in records, conflicting or missing evidence, and problematic or unusual relationships between involved parties.[4]

Conclusion

Every company is interested in finding the most appropriate safeguards to protect the company appropriately and cost-effectively. Therefore, the safeguard selection process is crucial and should not be based on faulty justifications. A structured process that allows handling multiple attributes is preferable to unsystematic activities.

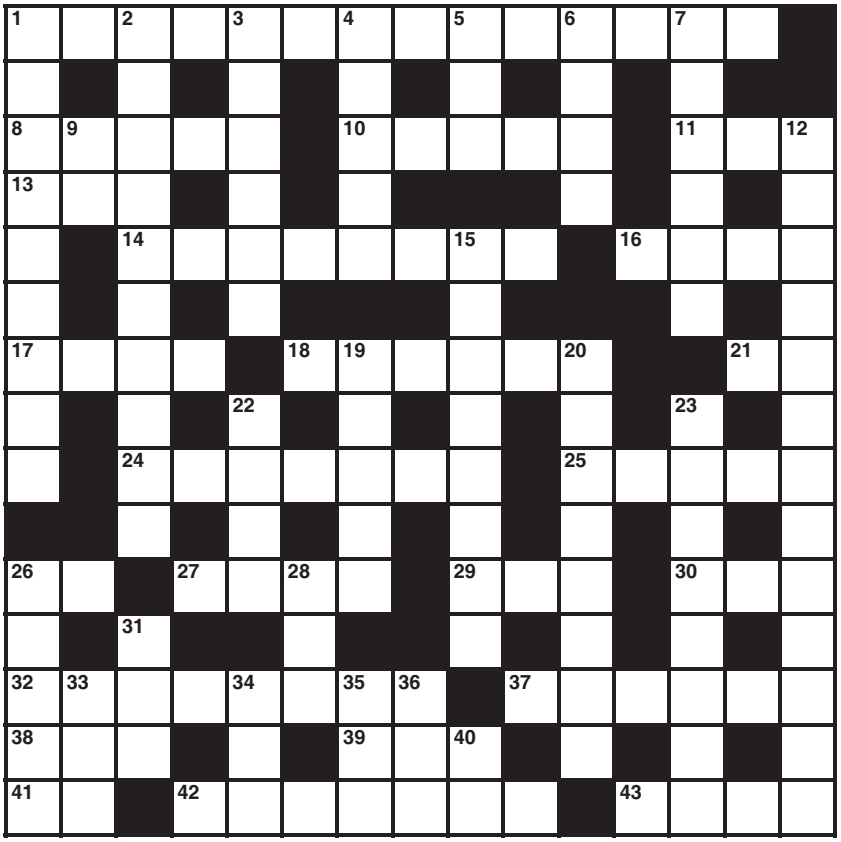
This process should also be supported with a decision-making technique that is manageable and delivers transparent and understandable results. However, common disadvantages such as substitutability, leveling, and over- or undervaluation, should be considered. The overall selection process can be characterized by various problems, which cannot always be avoided and, therefore, should be considered continually, especially when checking the result of the process. Indications of these problems are, among other things, major changes in the decision problem as well as changed internal or external conditions, errors, insufficient documentation, and possible fraudulent activities. Mostly, the safeguard selection of a company can be greatly improved by focusing not only on evaluating the safeguard alternatives, but also on critically examining the selection process itself.

Endnotes

1 Fishburn, P. C.; "Additive Utilities With Incomplete Product Set: Applications to Priorities and Assignments," *Operations Research*, vol. 15, iss. 3, April 1967, p. 537–542
2 Saaty, T. L.; "How to Make a Decision: The Analytic Hierarchy Process," *Interfaces*, vol. 24, December 1994, p. 19–43
3 Nimwegen, S.; *Prevention and Identification of Fraud: Possibilities of Internal Corporate Governance Elements*, dissertation, University of Münster, Westfalen, Germany, 2009
4 American Institute of Certified Public Accountants, "AU Section 316—Consideration of Fraud in a Financial Statement Audit," USA, 2002, *www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00316.pdf*

crossword puzzle

by Myles Mellor
www.themecrosswords.com



ACROSS

1 Primary task of a DBA, 3 words
8 Gains access to
10 Conforming to a perfect standard
11 Unprocessed, as data
13 Voice, as a grievance
14 Elaborate overall plan for the future
16 Half
17 Point on an agenda
18 Rental company caught up in moral issues relating to tax withholding
21 Technical department
24 Relating to favoritism to relatives, especially in promotions or job placements
25 Interval in which repeating sequences of actions occur
26 Weight measure, for short
27 Indication of damage
29 Not using up-to-date technologies
30 Zilch
32 Tools to visually lay out the concepts relating to a project, negotiation, etc., 2 words
37 Temporarily obtain
38 "Patience ___ virtue" 2 words
39 Boundary
41 Trademark, abbr.
42 "Immorality of ____," unwillingness to speak up against unethical actions
43 Time period

DOWN

1 Tending to control a situation rather than waiting for something to happen
2 Watching over and directing
3 Verify
4 Tarnish ethically
5 Color
6 In the proper manner
7 Goal to be obtained
9 Transcendental number
12 One who alerts on unethical activities within a company for which the person is working
15 Promise and then renege, 3 words
19 Between, prefix
20 What a hacker often uses to gain access, 2 words
22 Details of a project
23 Situation
26 Confine
28 __ __ rule (usually)
31 Kind of fingerprint
33 Doctrine
34 1006 in Roman terms
35 Before, prefix
36 Transgression
40 Event controller, abbr.

Answers on page 58

quiz#168

Based on Volume 3, 2016—Data Privacy
Value—1 Hour of CISA/CISM/CGEIT/CRISC Continuing Professional Education (CPE) Credit

TRUE OR FALSE

VANDERPOOL ARTICLE

1 One prominent feature of the General Data Protection Regulations (GDRP) 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.

2 The right to know you have been hacked is a popular component of the GDPR and requires organizations to report to a central authority as soon as possible any data breaches that pose a risk to data owners.

3 Although many medical researchers are not content with the latest changes to the GDPR's wording, there are no stakeholders caught in the crosshairs of the GDPR.

4 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.

STOLBIKOVA ARTICLE

5 Studies show that the time different processors take to encrypt and/or decrypt data can be 200 times slower for ECC than for an equivalent RSA length.

6 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.

7 Grover attacks make factoring easier by creating a variable superposition over all possible inputs, destructively interfering states that are invalid and, consequently, finding inputs that satisfy a given function.

8 ECC will be easier to break than RSA cryptosystems due to a lower qubits (quantum equivalents of traditional bits) requirement.

9 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.

THARAKAN ARTICLE

10 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.

11 The CISO should collect feedback based on the compliance metrics and report to the CEO on the effectiveness of the information security program.

12 Outsourcing security operations is a good choice for large-sized organizations, as it helps them reduce the hassles of maintaining an always-functioning environment.

SERRANO ARTICLE

13 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.

14 In the SMART approach, the first step is to collect and manage data, then analyze them, draw insight with that analysis and, finally, make decisions based on the analysis performed.

15 Organizations from nonfinancial services did not consider regulatory requirements a key risk, whereas organizations from the financial sector did.

16 Data governance policies, procedures and controls should be implemented in order to obtain the appropriate data quality levels.

CPE quiz

Prepared by
Smita Totade,
Ph.D., CISA, CISM, CGEIT, CRISC

Take the quiz online

CPE quiz #167

THE ANSWER FORM

Based on Volume 3, 2016

TRUE OR FALSE

VANDERPOOL ARTICLE

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

STOLBIKOVA ARTICLE

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

THARAKAN ARTICLE

10. _____
11. _____
12. _____

SERRANO ARTICLE

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

Name _____

PLEASE PRINT OR TYPE

Address _____

CISA, CISM, CGEIT or CRISC # _____

Answers: Crossword by Myles Mellor
See page 56 for the puzzle.

1P	R	O	T	E	C	T	T	H	E	D	A	T	A
R		V		N		A		U		U		A	
O	P	E	N	S		I	D	E	A	L		R	A
A	I	R		U		N				Y		G	
C		S	T	R	A	T	E	G	Y		S	E	M
T		E		E				O			T		S
I	T	E	M		A	I	R	B	N	B			I
V		I		S		N		A		A		S	
E		N	E	P	O	T	I	C		C	Y	C	L
		G		E		E		K		K		E	
L	B		S	C	A	R		O	L	D		N	I
I		D			S			N		O		A	
M	I	N	D	M	A	P	S		B	O	R	R	O
I	S	A		V		R	I	M		R		I	
T	M		S	I	L	E	N	C	E		H	O	U

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.

standards guidelines tools and techniques

ISACA Member and Certification Holder Compliance

The specialized 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 mobilization, 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 guidelines are effective 1 September 2014.

General
1001 Audit Charter
1002 Organizational 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 categorization as the standards (also divided into three categories):

- General guidelines (2000 series)
- Performance guidelines (2200 series)
- Reporting guidelines (2400 series)

Please note that the guidelines are effective 1 September 2014.

General
2001 Audit Charter
2002 Organizational 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

leaders and supporters

ISACA®
Trust in, and value from, information systems

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

www.isaca.org/bookstore

NEW!

CISA, CISM, CGEIT and CRISC Review Manuals Are Now Available as eBooks!

ISACA® Review Manuals in secure eBook format are compatible with any EPUB 3 reader such as Adobe Digital Editions or Bluefire Reader. These manuals will conveniently travel with you on your laptop, tablet or phone.

- Searchable content for greater ease-of-use
- Time-saving internal and external hyperlinks
- Interactive features within the table of contents
- Available for immediate download after purchase—with no waiting and no shipping cost anywhere in the world!

CISA® CISM® CGEIT® CRISC™

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

NEW! COBIT 5 for Business Benefits Realization by ISACA

by ISACA

PRINT
Product Code: CB5BBR
Member/Nonmember:
$35.00/$80.00

WEB DOWNLOAD
Product Code: WCB5BBR
Member/Nonmember:
$35.00/$75.00

Enterprises make technology-enabled investments as a matter of daily operations. The need for business benefits realization from those investments is always present-from the time that the assets from such investments are being planned, until they are retired from use. Business benefits realization is a requirement from stakeholders and governance bodies to ensure that IT-business activity achieves the benefits that are envisioned when key investment decisions are made. One business benefits realization expert asserts: the only valid reason for investing in technology-enabled change is to generate benefits. Technology-enabled investments will undoubtedly play an ever-increasing role in our information-based society.

SPECIAL DISCOUNT OFFER:

Members: Add the PDF for just $15.00! When you purchase both the print and PDF versions of this title, you can save over 50%. Please add both this product and the PDF of *COBIT 5 for Business Benefits Realization* to your shopping cart and checkout in order to take advantage of this special offer.

Nonmembers: Add the PDF for just $30.00! When you purchase both the print and PDF versions of this title, you can save over 75%. Please add both this product and the PDF of *COBIT 5 for Business Benefits Realization* to your shopping cart and checkout in order to take advantage of this special offer.

CSX Cybersecurity Fundamentals Study Guide
NEW EDITION NOW AVAILABLE IN SPANISH!!

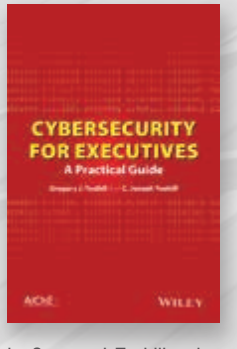
by ISACA

PRINT
English Product Code: CSXG1
Spanish Product Code: CSXG1S
Member/Nonmember:
$45.00/$55.00

WEB DOWNLOAD
English Product Code:
WCSXG1
Spanish Product Code:
WCSXG1S
Member/Nonmember:
$45.00/$55.00

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

Cybersecurity for Executives: A Practical Guide



by Gregory J. Touhill and
C. Joseph Touhill

PRINT
Product Code: 120WCS
Member/Nonmember:
$75.00/$85.00

Practical guide that can be used by executives to make well-informed decisions on cybersecurity issues to better protect their business

- Emphasizes, in a direct and uncomplicated way, how executives can identify, understand, assess, and mitigate risks associated with cybersecurity issues
- Covers 'What to Do When You Get Hacked?' including Business Continuity and Disaster Recovery planning, Public Relations, Legal and Regulatory issues, and Notifications and Disclosures
- Provides steps for integrating cybersecurity into Strategy; Policy and Guidelines; Change Management and Personnel Management
- Identifies cybersecurity best practices that executives can and should use both in the office and at home to protect their vital information

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

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

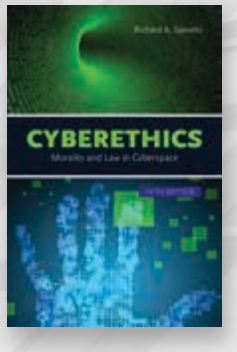
by John Sileo

PRINT
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. By interlacing his personal experience with cutting-edge research and unforgettable stories, John not only inspires change inside of your organization, but outlines a simple framework with which to build a Culture of Privacy. This book is a must-read for any individual with a Social Security Number and any business leader who doesn't want the negative publicity, customer flight, legal battles and stock depreciation resulting from data breach.

Cyberethics—Morality and Law in Cyberspace, 5th Edition



by Richard Spinello

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

The Internet and widespread use of blogging, email, social media and e-commerce have foregrounded new, complex moral issues and dilemmas. Likewise, modern technologies and social networks have brought numerous challenges to legal systems, which have difficulty keeping up with borderless global information technologies. The fully revised and updated Fifth Edition of *Cyberethics: Morality and Law in Cyberspace* offers an in-depth and comprehensive examination of the social costs and moral issues emerging from ever-expanding use of the Internet and new information technologies. Focusing heavily on content control, free speech, intellectual property, and security, *Cyberethics: Morality and Law in Cyberspace* provides legal and philosophical discussions of these critical issues.

Transforming Cybersecurity

by ISACA

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

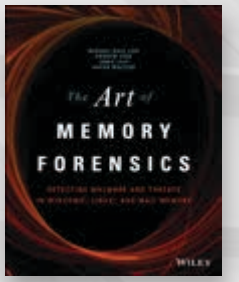
WEB DOWNLOAD
Product Code: WCB5TC1
Member/Nonmember:
Free/$60.00

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

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

This publication gives practical guidance on transforming cybersecurity in a systemic way. First, the impacts of cybercrime and cyberwarfare on business and society are illustrated and put in context. This section shows the rise in cost and frequency of security incidents, including APT attacks and other threats with a critical impact and high intensity. Second, the transformation addresses security governance, security management and security assurance. In accordance with the lens concept within COBIT 5, these sections cover all elements of the systemic transformation and cybersecurity improvements.

The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory



Michael Hale Ligh, Andrew Case, Jamie Levy, Aaron Walters

PRINT
Product Code: 122WAM
Member/Nonmember: $55.00/$65.00

Memory forensics is the art of analyzing computer memory (RAM) to solve digital crimes. As a follow-up to the best seller Malware Analyst's Cookbook, experts in the fields of malware, security, and digital forensics bring you a step-by-step guide to memory forensics—now the most sought after skill in the digital forensics and incident response fields.

Beginning with introductory concepts and moving toward the advanced, *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory* is based on a five day training course that the authors have presented to hundreds of students. It is the only book on the market that focuses exclusively on memory forensics and how to deploy such techniques properly.

Responding to Targeted Cyberattacks

by ISACA

PRINT
Product Code: RTC
Member/Nonmember: $35.00/$59.00

WEB DOWNLOAD
Product Code: WRTC
Member/Nonmember: FREE/$59.00

A Breach WILL Eventually Occur!
Is your enterprise prepared!

The threat environment had radically changed over the last decade. Most enterprises have not kept pace and lack the necessary fundamentals required to prepare and plan against cyberattacks.

To successfully expel attackers, the enterprise must be able to:
- Conduct an investigation
- Feed threat intelligence into a detailed remediation/eradication plan
- Execute the remediation/eradication plan

This publication covers a few of the basic concepts that will help answer the key questions posed by a new outlook that a breach WILL eventually occur.

A Practical Guide to PCI DSS

by ISACA

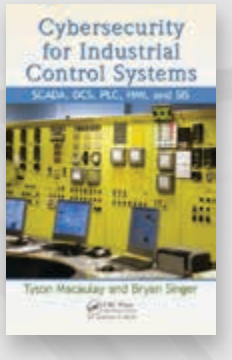
PRINT
Product Code: APG
Member/Nonmember: $35.00/$60.00

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 additional valued information.

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



by ISACA

PRINT
Product Code: 60CRC
Member/Nonmember: $84.00/$94.00

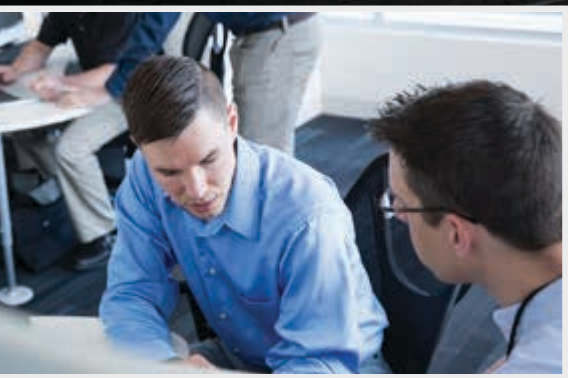
As industrial control systems (ICS), including SCADA, DCS, and other process control networks, become Internet-facing, they expose crucial services to attack. Threats like Duqu, a sophisticated worm found in the wild that appeared to share portions of its code with the Stuxnet worm, emerge with increasing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

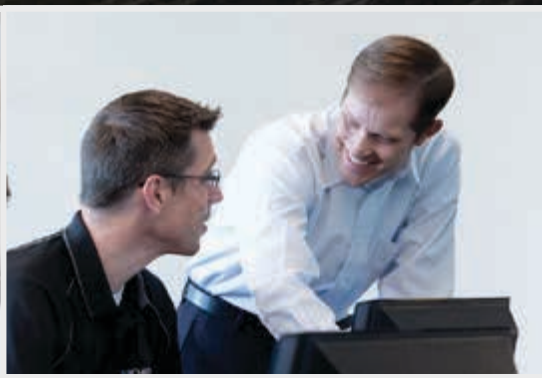
2 EASY WAYS TO ORDER:

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

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