Volume 5, 2015

ISACA® Journal

CYBERSECURITY

360-Degree Vision

Featured articles:

Addressing Cybersecurity Vulnerabilities

The Underground Threat

Preparing for a Cyberattack by Extending BCM into the C-suite

And more...

ISACA®

Trust in, and value from, information systems

WWW.ISACA.ORG

MEMBER GET A MEMBER 2015

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**

Receive a passport wallet with RFID blocking technology.

*RECRUIT 4–5 NEW MEMBERS**

Receive a pair of high quality, name brand, 10x42 binoculars that feature 10-power multicoated lenses and 42mm objectives.

*RECRUIT 6–7 NEW MEMBERS**

receive a high quality 10" fan that is quiet, powerful and has no blades. This innovative design from a leading manufacturer makes it easy to clean and very quiet.

*RECRUIT 8–9 NEW MEMBERS**

Receive a high-performance action camera for photos and video. Waterproof to 131' (40m). Features 1080p60 and 720p120 video. 12MP photos up to 30 frames per second, with built-in WI-FI and Bluetooth® capabilities.

*RECRUIT 10 OR MORE NEW MEMBERS**

Receive a high quality smartwatch, an incredibly precise timepiece that allows you new ways to connect. It is also a comprehensive health and fitness companion. It creates a new way for you to relate with technology designed for personal living.

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

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

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.

FOLLOW YOUR PASSION.
FIND YOUR PLACE.

with a

CYBERSECURITY MASTERS DEGREE

from Missouri State

AACSB ACCREDITED

100% ONLINE

Become A Leader In A Leading Industry

- Our Masters degree in Cybersecurity is a full thirty hour degree program that is appropriate for professionals who either wish to, or currently are, working full time in the field of Cybersecurity.

- With classes ranging from Hacker Tools and Techniques, to Organizational Behavior, students will equip themselves for positions ranging from Security Analysts, to Chief Information Security Officer.

Unbeatable Value

- Tuition rates lower than state and national averages.

Missouri State™ UNIVERSITY

cybersecurity.missouristate.edu

EO/AA/M/F/VETERANS/DISABILITY

VOLUME 5, 2015

ISACA® Journal

Columns

Features

Plus

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

Online-exclusive Features

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

Online Features
The following is a sample of the upcoming features planned for September and October.

Auditors and Large Software Projects: Can Auditors Prevent Project Failure? Part 2
Ed Gelbstein, Ph.D.

Book Review: Computer Security Handbook, 6th Edition
Reviewed by Dino Ippoliti, CISA, CISM,

Book Review: Governance, Risk Management and Compliance: It Can't Happen to Us—Avoiding Corporate Disaster While Driving Success
Reviewed by Maria Patricia Prandini, CISA, CRISC

Book Review: IT Auditing and Application Controls for Small and Mid-sized Enterprises: Revenue, Expenditure, Inventory, Payroll, and More
Reviewed by A. Krista Kivisild, CISA, CA, CPA

Vulnerability of Login Credentials at the Heart of Cyberhacks and Data Breaches
Jeff Maynard

Read more from these *Journal* authors...

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

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

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

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

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

ISACA®
Trust in, and value from, information systems
3701 Algonquin Road, Suite 1010
Rolling Meadows, Illinois 60008 USA
Telephone +1.847.253.1545
Fax +1.847.253.1443
www.isaca.org

THERE'S NO SHORTAGE OF
CYBER SECURITY THREATS

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

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

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

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

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

ANSWER THE CALL. START TODAY. **CAPELLA.EDU/ISACA** OR **1.866.933.5836**

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

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

Capella University

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.*

Stanley Baldwin's Bomber

Stanley Baldwin was a British politician who won numerous national elections in the 1920s and 1930s. He was also one of Britain's worst prime ministers, leading His Majesty's government through the Depression and the rise of fascism with inaction that amounted to catatonia. Winston Churchill referred to him as "no better than an epileptic corpse."[1] He is largely forgotten today, but is remembered (somewhat) for one quote. In the early 1930s, explaining why military action would be futile, he said, "The bomber will always get through."[2]

Now let us move forward more than 80 years to a conversation I had with the chief information officer (CIO) of a major law firm. He told me that there was no sense in building protections against cyberattacks because, "if the Freedonian Army wants my data, I can't stop them."[3] He was, in effect, uttering an updated version of Baldwin's evasion. But Baldwin was wrong. In World War II, some bombers, alas, got through, but not all. Stout-hearted airmen and fast fighter planes stopped many of them. The cost and difficulty of attack were raised to a point that proved unbearable for the aggressors. And people crawled into shelters to mitigate their risk when a bomber did manage to drop its load. The same counterarguments, in my opinion, apply to cyberattacks and even to cyberwar.

If—which I do not for a moment believe—but if it were true that cyberattackers can penetrate any system, steal any information and subvert any safeguard, then there are certain things prudent businesspeople would do. Let us accept that dismal assumption for the sake of discussion and explore a few ideas of what you should do if the unstoppable bombers are on their way.

GET YOUR FIGHTER PLANES READY

Every organization should make certain that it has intrusion detection systems (IDS) and intrusion prevention systems (IPS) located at every entry point into its network. Having said this, it is probably impossible, since entry points are now every personal computer and, increasingly, every mobile device. Therefore, traffic from all of these should be directed to secure gateways, with IDS/IPS there looking for bombers on the horizon.

And right behind them should be well-managed firewalls and virus filters. It is a sad fact that this should need to be pointed out this late into the war, but too many firewalls are lowered too often to allow seemingly benign traffic to pass through; even the vendors have admitted that virus filters can be beaten.[4] There is a new generation of firewalls[5] that simply provides a higher level of security. Sure, they cost money, but so does getting bombed, which we have presumed here to be inevitable.

TRAIN YOUR FIGHTER PILOTS

Just as in physical warfare, the best safeguards need people to make them work. It is essential that every organization have personnel who can implement controls to prevent and deter attacks, detect them when they occur, and recover from them if a bomber does get through. I have previously referred to this cadre of specialists as a CyberCERT.[6]

Repelling cyberattacks is not an innate skill, but people can be trained to do it. If you want to have enough airmen on your side when the bomber approaches, you cannot wait until then to start their training. You need to build your air force before the battle is fought.

MAKE COPIES OF IMPORTANT STUFF

In a war, if you think the Ministry will be bombed, you make copies of critical documents and store them somewhere else. Well, we are in a war with cyberattackers, declared or not. So it is important to have backup copies[7] of critical data.

This applies even more so to software. As I have mentioned in several articles,[8] a trusted image of software is the bedrock on which cyberrecovery must be built. Cyberattacks occur because programs are penetrated, although there are exceptions to this statement.[9] Therefore, just as with data, it is critical to have copies of

software that is known not to have been infected. This may necessitate saving many generations of copies, potentially back to software releases.

HARDEN YOUR TARGETS

At a recent conference, Dennis Wenk of Seagate stated that, in his opinion, downtime attributed to hardware and software that were beyond their end of life caused more damage than that caused by cyberattacks.[10] I cannot say whether I agree or not about the relative impact today, but it is evident that you cannot shoot down a bomber with a pop gun. It is imperative that applications and the platforms they run on be up to date. They need to have not only the latest security safeguards, but also be as free of flaws as possible.

To pick only one example, Microsoft has published a list of 91 significant security vulnerabilities in Windows 2003,[11] which was taken off support in 2010. I have personally seen production systems running on this operating system since that time. Running outdated software on antiquated equipment is akin to waving a bright banner at a cyberattacker that says, "Drop bombs here."

HIDE THE CROWN JEWELS

Keeping in mind that the Freedonian Army cannot be stopped in its never-ending quest to penetrate your systems, it only makes sense to make certain it cannot get to your most sensitive information. There are some files that, if disclosed, would cause significant and irreparable harm to your organization. Therefore, they should not be accessible remotely nor ever be copied to portable media, including laptop computers. Note: This approach may be considered extreme.

> "Minimize your risk as much as you can and prepare to recover when the attack occurs."

Alternatively, and more practically, all sensitive data should be encrypted—at rest, in transit and in use. In terms of cost and difficulty, this may actually be more onerous than the previously suggested, if unrealistic, approach, but it is more likely to be put into practice.

PREPARE FOR WAR

In summary, if you think that successful cyberattacks are inevitable, you should minimize your risk as much as you can and prepare to recover when the attack occurs. Come to think of it, that is a pretty good strategy even if you do not think the bomber will always get through.

If you think of cyberattacks as war, which it is in both the figurative and literal senses, make yourself ready to win it. Do not just accept defeat before the big battles begin.

ENDNOTES

1 Halle, Kay; *Irrepressible Churchill*, World Publishing Company, USA, 1966, p. 131

2 Hansard, Official Report, 10 November 1932, United Kingdom, col. 632, vol. 270, *http://hansard.millbanksystems.com/commons/1932/nov/10/international-affairs#column_632*

3 He actually referred to an army other than that of Freedonia, a small, imaginary country with an economy based largely on poultry, which considers all other nations to be sworn enemies.

4 See my previous column, "Barbarians at the Ramparts," *ISACA Journal*, vol. 3, 2013.

5 See the article by my colleague, Eric Beck, "How Zero-trust Network Security Can Enable Recovery From Cyberattacks," *ISACA Journal*, vol. 6, 2014.

6 *ISACA Journal*, vol. 5, 2014

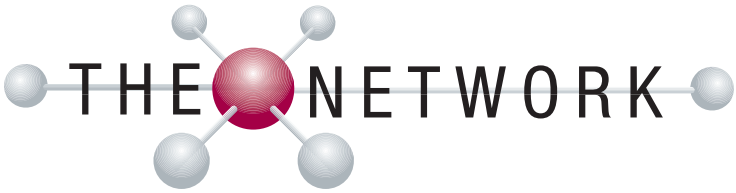
7 Note that I said "backup copies" and not "replicated files." It is still important to have portable copies of data that have integrity (or at least as much integrity as usual) so that files can be restored to a known, trusted point. Replication provides a file that is current, but it does not preserve a trail of what it was, notably prior to being attacked.

8 See most recently my column, "Cyberrecovery Preparation," *ISACA Journal*, vol. 3, 2014.

9 Grimes, Roger A.; "Should You Worry About Memory-only Malware?" *InfoWorld*, 4 February 2014, *www.infoworld.com/article/2608848/security/should-you-worry-about-memory-only-malware-.html*. See also a comment made by Mr. Erik Taavila in regard to one of my previous articles, "CyberCERT," vol. 5, 2014, *www.isaca.org/Journal/archives/2014/Volume-5/Pages/CyberCERT.aspx#comments.*

10 Continuity Insights Management Conference, "Information Technology Risk: What You Need to Know," Scottsdale, Arizona, USA, 22-24 April 2105

11 I am not picking on Microsoft. It is only that Windows' security flaws are well documented. See *www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-107/cvssscoremin-5/cvssscoremax-5.99/Microsoft-Windows-2000.html.*



Daniela Gschwend

Daniela Gschwend, CISA, CGEIT, CRISC, after studying information management at the University of St. Gall (Switzerland), began in the IT audit department of Credit Suisse (CS), a global leading financial services company with headquarters in Zurich, Switzerland, as part of the infrastructure audit team. Four years later, she had the opportunity to head up the IT audit team of one of the CS companies, based in London, England, UK. Moving back to Switzerland after three years in the UK, Gschwend joined Swiss Re, the second largest reinsurance company in the world, as global head of internal IT audit. After four years in this role, she "switched sides," becoming an auditee, and moved into various governance of enterprise IT roles over the past 13 years.

Q: *As a governance of enterprise IT (GEIT) professional, how do you believe your background in IT audit has supported and guided your career to date?*

A: My background as an auditor has helped me to understand what auditors are looking for; identifying gaps and improvement opportunities is one side, but convincing management to implement these before they become issues can be very challenging when one is in the same department. We continue to emphasize that gaps have to be addressed for risk mitigation purposes, not because audit wanted something.

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

A: Global companies receive (too) many and different requirements from all over the world, coming in via various channels and time lines. A GEIT professional must be able to communicate and work with a variety of experts across the globe, speaking their and management's language and creating transparency and a consistent approach to addressing the key risk areas. Overall, networking, communicating and "translating" requirements into deliverables are essential.

Q: *How do you see the role of GEIT changing in the long term?*

A: Unfortunately, I believe we still need to work on some basic elements to make sure that top-level management and the board assume their GEIT responsibilities. Also, the gap between the business and the IT worlds in companies has not been properly addressed and closed yet. With the technological developments, decision makers tend to misjudge the risk and the efforts behind their decisions and forget the potential implications on today's IT environment and their past decisions.

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

A: When I started as an auditor, we had to figure out how IT and the processes worked and what controls we expected to see together in our team and with experts. There were hardly any audit programs available, self-written scripts had to be run or we accessed the systems on the operating system level to get the respective data. The efforts were high, but they allowed us to think carefully about what we really needed, why we needed it and how we could get it at a low price. Therefore, my advice: Do not become a checklist auditor. Always think about the big picture, that which is behind the scenes; challenge programs; and assess what makes sense and what does not. Have an opinion on what you do—the auditee and management will see the benefits.

Q: *How has your volunteering with a leading industry association, such as ISACA®, especially your work as president of your local ISACA chapter, helped and advanced your career and professional life?*

A: Joining the board of the ISACA Switzerland Chapter immediately provided opportunities within the chapter and then later internationally. People recognized me (sometimes also in interviews when hiring) and members provided feedback and turned to me (and other board members) for support. The companies I have worked for have supported my engagement as it also demonstrates initiative and engagement beyond the organization's boundaries. Interactions with people outside the company and global networking capabilities have helped me to gain access to experts at all levels and use these resources to solve difficulties. Being the president has also improved my leadership skills. There have been many situations and problems that I have had to address that have, in turn, helped me in my professional life.

Do you have something to say about this article?

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

Go directly to the article:

WHAT HAS BEEN, OR DO YOU ANTICIPATE BEING, THE BIGGEST COMPLIANCE CHALLENGE IN 2015?
Balancing the benefits from technological capabilities with the many and changing regulatory and client requirements that are often in contradiction with technological trends

WHAT ARE YOUR THREE GOALS FOR 2015?
1. Continue the journey to change the perception of governance, risk management and compliance (GRC) into a more enabling topic (different marketing).
2. Achieve more with combined efforts globally—more effective load balancing.
3. Stay fit and become a better pinball player.

WHAT IS ON YOUR DESK RIGHT NOW?
My big iMac, jelly bellies and still too many documents

WHO ARE YOU FOLLOWING ON TWITTER?
The top DJs in the world and a few companies in the financial and consultancy industry

WHAT IS YOUR NUMBER ONE PIECE OF ADVICE FOR OTHER GEIT PROFESSIONALS?
Keep calm and maintain oversight.

WHAT IS YOUR FAVORITE BENEFIT OF YOUR ISACA MEMBERSHIP?
COBIT®. But, a close second is the networking, especially that which I gain as a board member with other chapter leaders around the globe.

WHAT DO YOU DO WHEN YOU ARE NOT AT WORK?
Eat, sleep, celebrate (there's always something), repeat.

Auditors and Large Software Projects, Part 1

Can Auditors Prevent Project Failure?

Ed Gelbstein, Ph.D., 1940 – 2015, worked in IS/IT in the private and public sectors in various countries for more than 50 years. Gelbstein did analog and digital development in the 1960s, incorporated digital computers in the control systems for continuous process in the late '60s and early '70s, and managed projects of increasing size and complexity until the early 1990s. In the 1990s, he became an executive at the preprivatized British Railways and then the United Nations global computing and data communications provider. Following his (semi) retirement from the UN, he joined the audit teams of the UN Board of Auditors and the French National Audit Office. Gelbstein also taught postgraduate courses on business management of information systems.

Large software projects have been notorious because of:

- Their large budget and timescale overruns
- Failing to deliver the promised benefits
- Being accredited to production before they are ready (insufficient testing, inadequate documentation and everything in between)

How can this happen, given that this has been known for many years and there are many methodologies and sources of guidance available to software developers and project managers? Examples include PRINCE 2,[1] the Project Management Body of Knowledge (PMBOK)[2] and the Software Engineering Body of Knowledge (SWEBOK).[3] Moreover, many of the professionals involved in this work hold certifications from the Project Management Institute and/or the SWEBOK certificate.

Auditors also have many sources of good practices and guidance such as ISACA's own *Systems Development and Project Management Audit/Assurance Program*[4] and the guidelines for auditing IT project management published by The Institute of Internal Auditors.[5] There is also a worthwhile *ISACA® Journal* article on project risk management.[6]

Even though many projects have been "audited to death," the problem persists to the extent that the Working Group on IT Audit of the International Organization of Supreme Audit Institutions (INTOSAI) dedicated an issue of its journal to the topic of "Why IT projects fail,"[7] and more articles on this theme continue to appear. The catalog of failed projects is huge. "Failure" is a flexible word that can mean different things to different people, e.g., a three-month delay to a project may not be considered a failure in some cases, yet is an absolute disaster in others.

HOW CORPORATE LIFE CONSPIRES TO CAUSE AN IT PROJECT TO FAIL

Having participated in a few successful large projects years ago and also witnessed (and in some cases audited) projects that failed, some were abandoned when management had the opportunity and courage to do so. However, this is not always the case, and money and people can continue to be thrown into a failing project's black hole.

This column explores some of the realities surrounding failed projects. The sections and findings presented are a composite of findings from several projects over many years (and they keep turning up). No identities or details of the project owners are given because of nondisclosure agreements signed to protect their confidentiality.

The Business Case

Large projects fall in two categories:

- Replacements or major enhancements to an existing system (which is, therefore, known and understood)
- Innovative solutions that create opportunities for change and, therefore, are somewhat speculative

The auditor should always request and study the business case.

The business case for the first category would be based on the shortcomings of the existing system and how these would be overcome by

Editor's Note

On 19 July, 2015, Ed Gelbstein, Ph.D., passed away after a lengthy illness. He was a prolific writer and contributor to the ISACA Journal *and a valued and admired colleague. His work will continue to be published in the* ISACA Journal *posthumously.*

the proposed project. The auditor could consider reviewing the technical risk of a system that may not be properly documented or may be fragile because of other reasons.

This may not be all that hard to do, except for the limited ability to predict costs with reasonable confidence. Such estimates do not have a particularly good track record.

Innovative solutions are more of a crystal-ball-gazing exercise, and estimated costs and benefits may be inaccurate at the time of doing the business case.

One example of where this proved to be problematic involved a large database for sensitive personal information. Consultants were engaged to estimate the benefits that could be expected and produced a series of glossy reports with impressive numbers.

The audit finding: The reported estimates were suspiciously accurate—down to 1 euro in zillions and years away from being achieved. The reports did not include the assumptions made to support the benefits and presented only a best-case scenario. There was no mention of a most likely or worst-case scenario. The costs were a guess, not even an educated one. The sponsor was not happy with the auditor's observations but decided to shelve the project.

The Project Risk Analysis

The auditor should request and study reports that define business risk, project risk and technical risk, assuming these definitions have been created (not always the case), and determine if the risk assessments are based on a proper methodology.[8]

Many years ago, a large project was launched without any risk analysis created and it went off the rails within a short time. The client believed that the vendor would be responsible for the management of the project. The vendor was, but only as far as its responsibilities extended. The client did not think it was necessary to have a project manager. It took two years to put the project back on track.

An often-ignored project risk is assuming that the project manager could be guaranteed to be there for the many years of a project. Wrong. Some gave up (see the upcoming part 2 of this article, to be released in vol. 3, 2016); others were offered a better job elsewhere and left. Finding a person capable of taking over once the project has started and leading it to a successful conclusion may be harder than it looks.

Other easy-to-ignore technical risk relates to the rapid obsolescence of the technologies initially selected, plus limited knowledge of the products that replace those technologies; the disappearance of a supplier because of bankruptcy, mergers and acquisitions; or, less frequently, the supplier's decision that the product is no longer viable.

This happened to the biggest civilian IT scheme attempted for the UK National Health Service. The project had been in disarray since it missed its first deadlines in 2007. The project had been beset by changing specifications, technical challenges and clashes with suppliers, which left it years behind schedule and well over budget. Accenture, the largest contractor involved, walked out on contracts worth £2 billion in 2006.[9]

The Requirements Definition

The auditor should review the stages through which the functionality and features that the system should deliver were developed and report the appropriate findings. What should go into a requirements definition is well defined elsewhere, but this does not mean it actually happens. Nonetheless, the auditor should give particular attention to the sections in the requirements definition that address key system controls, such as measures to ensure segregation of duties (SoD); the methods for granting and controlling privileges including role-based access controls; and management of superuser rights, logs, and audit trails.

Beyond this point, the auditor should consider recommending that any changed or additional requirements once the system design and estimates have been frozen should be allowed only if there is an overwhelming reason for doing so, and then, strict change control should be applied.

CONCLUSIONS

This column, the first of three, focused primarily on those aspects of project management of large software developments that, if not done well enough, contribute to budget and timescale overruns or, at worst, the failure of the project.

Smaller projects, such as those classed as "end-user computing" rarely get the benefit of an audit, even when they consist of sophisticated spreadsheets that are, in fact, a complex software project and are used for critical analyses. It is not uncommon for these to be undocumented and poorly tested, perhaps an issue for a future column, as is the whole topic of software quality.

ENDNOTES

[1] AXELOS Ltd., Prince2, *www.prince-officialsite.com/*

[2] Project Management Institute, Project Management Body of Knowledge (PMBOK), *www.pmi.org/PMBOK-Guide-and-Standards.aspx*

[3] IEEE Computer Society, *Guide to the Software Engineering Body of Knowledge, www.computer.org/portal/web/swebok*

[4] ISACA, *Systems Development and Project Management Audit/Assurance Program*, 2009, *www.isaca.org/auditprograms*

[5] Mookhey, K. K.; "Auditing IT Project Management," The Institute of Internal Auditors (The IIA), 1 May 2008, *https://iaonline.theiia.org/auditing-it-project-management*

[6] Singleton, Tommie; "What Every IT Auditor Should Know About Project Risk Management," *ISACA Journal*, vol. 3, 2004, *www.isaca.org/archives*

[7] INTOSAI, "Why IT projects fail," *The IntoIT Journal*, iss. 26, May 2008, *www.intosaiitaudit.org/publication_and_resources/1*

[8] *Op cit*, Singleton

[9] Wright, Oliver; "NHS Pulls the Plug on Its £11bn IT System," *The Independent*, 3 August 2011, *www.independent.co.uk/life-style/health-and-families/health-news/nhs-pulls-the-plug-on-its-11bn-it-system-2330906.html*

Monitoring Morality

Is Assurance of Information Ethics Feasible?

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.*

My honest thought about monitoring is: I do not like being monitored! I am not alone. A large majority of individuals and organizations would assert that they do not like being monitored. And yet, it has benefits, such as the potential for corrective action, behavior modification and improvement in performance. Monitoring, including self-monitoring, helps gain and maintain others' trust as well. If monitoring can be digested as a palatable thought, the next question is: Can we—should we—monitor morality in organizations?

Why monitor morality? As John Rosthorn said, "The more serious survival issue for top managers and investors is not competition, but the enemies within the corporation."[1] The "enemy within" has to do with actions of someone (or a group of people) influential in the enterprise breaching the trust of its stakeholders. Organizations—whether for-profit or otherwise—thrive on their stakeholders' trust in them. All legitimate organizations need to protect and manage this trust in order to guarantee their continued viability and prosperity. People both within and outside the enterprise have expectations and trust that the organization will deliver on its promises. Any cracks in this trust, often a consequence of poor risk management, result in a crisis of confidence in the organization. Consequently, a perfectly running organization may face extinction if the trust gap widens. As an example, consider the recent introduction of a new generic top-level domain (gTLD) name, *.sucks*, by Icann, the traffic cop of the Internet. Icann's approval of the .sucks domain rested on hearing no objections from anyone, hardly a responsible justification, given the global influence Icann holds.[2] This has engendered a crisis of confidence in Icann, for the new domain could prove to be predatory, exploitative or coercive. Consequently, subscribers, regulators and erstwhile users of the global network wonder if Icann will maintain its historic path of integrity and objectivity.

So there is a need for the enterprise to nurture and maintain trust, which, in turn, depends on how well it fulfills its duties rather than how aggressively it chases its rights. The normative ideas of trust and duty need to be put into practice to observe and assess an organization's behavior within the context of ethics. For this, we must recognize two related dimensions:

1. Stakeholders of the organization
2. The organization's performance

STAKEHOLDERS

Any entity that involves people will have to face separate concerns for each of its stakeholders (e.g., investors, employees, the community) in addition to dealing with its overarching need to harmonize these into a broader set of values embedded in a common vision and a code of ethics. The diversity of stakeholder groups' needs should be built into and coordinated within the overall ethical climate of the organization. An IT training school, for example, should offer its students information security skills that their prospective employers can use, while at the same time striving to ensure that it does not graduate "raw" hackers with little or no ethical sensitivity.

Finally, whereas duty toward each stakeholder must be addressed, it is equally important that a balance be achieved among all of the duties toward a stakeholder group and between the expectations of various competing stakeholder groups. For example, passenger safety concerns of a railroad should not be relegated only to buying casualty insurance, and the decision on energy use should not disregard environmental issues while minimizing train operating costs.

PERFORMANCE

Trust of stakeholders is sourced in three key categories of influence and accountability of a business: economic, social and environmental.[3] Of the three, the concept of economic accountability has been developed well over the past several centuries. There are metrics in

place, such as the general-purpose financial statements that provide insights into the financial health of the business. Also, regulatory requirements have attempted to enforce the need for trustworthy information. This, in turn, permits the business's stakeholders to assess how well the company has delivered on its promise to generate a return on investment (ROI) in the company. The accountability and reporting issues in social and environmental categories are being more aggressively examined recently, although there is still a great deal of room for further development and maturation. One idea is to develop an integrated, multidimensional reporting of enterprise performance, called the "triple bottom line" (3BL), an accountability framework with three parts—social, environmental and financial—often considered the three pillars of sustainability. Besides each dimension representing a separate domain, it is equally important to recognize trade-offs across the three dimensions. For example, financial results of a particular period or periods may be improved by marginalizing environmental objectives or killing the community involvement of the organization.

The idea of trust across these performance categories accompanies the stakeholders' concern as to how well the organization will measure up to it. After all, an entity's actions could run counter to its promises and expected behavior. Because businesses are agents of their principals, such as the shareholders, there is a need for assurance that the results reported are audited by an independent, competent professional with integrity and objectivity. Whether a single bottom line or triple bottom line, key performance reports to stakeholders deserve an endorsement of assurance by an independent party.

Any attempt to assess organizational performance should examine all intersecting cells, between stakeholder groups on one side of the table and the three dimensions of performance—financial, social and environmental—on the other. To illustrate, take the example of privacy as an issue. Privacy issues can be represented as a subcategory of the social dimension of Google. Because Google has vast influence on privacy of user data, it has been asked by the US Federal Trade Commission (FTC)—as have others—to have a privacy audit conducted. In this case, the stakeholder group is the user (including, perhaps, the regulator) and the category of the organizational dimension is the social aspect. Depending on the nature of the organization, its business model and its strategy, intersecting cells would likely vary in terms of criticality and relevance. Privacy issues, for example, may not be as critical to a home builder as they would be to a business such as LinkedIn.

ETHICS AUDIT

The term "ethics audit" or, preferably, the "assurance of ethics" is not widely used in literature and is sometimes confused with ethical auditing. In essence, an ethics audit is a systematic review of the expressed or implicit ethical obligations of an enterprise to assess how well this portfolio of moral obligations was met by the leadership of the enterprise during the period of time examined. The following propositions seem to articulate well the idea of assurance of ethics:[4]

- An organization is, at its core, a social institution.
- The organization conducts itself within the bounds of a set of basic values.
- Management's actions and behavior are essential expressions of these values over time.

To illustrate, Amtrak (USA) endows an important social dimension as it serves millions of passengers. One of its values has to do with passenger safety. A recent northbound train near Philadelphia, Pennsylvania, USA, was speeding at over 100 miles per hour, more than twice the speed limit, and became derailed. Several lives were lost and many passengers were injured. The automatic train control (ATC) technology currently in place is limited in comparison to the more sophisticated positive train control (PTC) technology, and the use of ATC has been put forth as a key reason for the tragedy. Presumably, the true reasons may be evident in the allocation of resources toward this duty; deferment of decisions to address high levels of risk in certain track areas; poor employee training; or the lack of awareness of or low sensitivity to passenger safety as an organizational objective. Only an in-depth investigation of the incident will reveal the exact nature of causes leading to the disaster.

LEADERSHIP

Across the three dimensions—economic, social and environmental—of a business, one thing that is common is leadership. The top leaders craft the internal environment and nurture and support the overall accountability of the entity to its stakeholders. Management's commitment to the

written word of conduct is crucial to the ethical expression in everything that management decides and every way it leads the organization.[5] Trustworthy behavior has the underlying element of risk management; that is, how well does the company manage the risk of doing business in a morally responsible way?

If we were to look for one indicator of moral threads that bind leadership in a business, it would probably be the tone at the top. The external auditors consider it important to review the client company's tone at the top as an overarching fraud risk factor.[6] If the tone is poor, chances are leadership behavior may fall short in its resolve to do the right thing. Take the case of Tianjin University in China. Six individuals, including three professors from China, while on sabbatical at a US university, allegedly swiped secrets from US companies relating to how to filter out unwanted signals in wireless devices. Upon their return to China, Tianjin University collaborated with the professors to form a start-up to produce and sell equipment using the technology.[7] The bottom line: Tianjin University appears to have failed to uphold its integrity.

In contrast, continuing the example of transportation safety, look at the case of the Union Pacific Corporation (UP). UP is mostly in the business of moving freight. However, it places utmost importance on the safety of its people, customers and communities at large. The company lives by its promise to protect people from potential harm as it drives its economic agenda. And UP makes resource allocations to ensure that safer, more current and sophisticated PTC technologies are in place to ensure safety: a key moral commitment of the corporation.

IS ASSURANCE OF INFORMATION ETHICS FEASIBLE?

I am quite optimistic about the prospects of assurance of information ethics. Yes, there is a great deal of work that needs to be done to develop models and paradigms that will permit a clear articulation of the *how* portion of the assurance process. Perhaps the three broad propositions noted in this column will provide a basis for further analysis and design.

How does an assurance of ethics differ from an assurance of information ethics? The two certainly seem to overlap a great deal. However, the emphasis in the assurance of information ethics should be on information objectives, technologies, platforms and processes, and outputs—all examined from the perspective of ethical conduct by the organization. One possibility is to extend COBIT® 5 to a specific and clear mapping of information ethics.

As is becoming well known, ethical dilemmas from fast-paced innovation in the IT-enabled environment are emerging and will have to be addressed. For example, Amazon, among others, will have to find ethically responsible ways to deploy drones, and Google will have to continue to wrestle with privacy issues while working on global and fair access to information. Mobile devices and the Internet of Things (IoT) will make life exciting, but even before harnessing the good, abuses of technology could overwhelm the IT professional. In this increasingly complex environment, a disciplined approach to account for information ethics should prove worthwhile.

ENDNOTES

[1] Rosthorn, John; "Business Ethics Auditing—More Than a Stakeholder's Toy," *Journal of Business Ethics*, 27: 9-19, 2000, p. 9

[2] Elder, Jeff; "A Debate Over the Domain '.sucks,'" Digits: Tech News & Analysis From the WSJ, 29 May 2015, *http://blogs.wsj.com/digits/2015/05/19/new-domain-sparks-icann-debate/*

[3] Garcia-Marza, D.; "Trust and Dialogue: Theoretical Approaches to Ethics Auditing," *Journal of Business Ethics*, 57: 209-219, 2005

[4] *Op cit*, Garcia-Marza, p. 215

[5] For example, the recent disclosures of the alleged bribery scandals at the Federation of International Football Associations (FIFA) suggest a weak tone at the top, despite elaborate documentation of enforcement requirements of ethical practices of the sport.

[6] See, for example, Apostolou, B. A.; J. H. Hassell; S. A. Weber; G. E. Sumners; "The Relative Importance of Fraud Risk Factors," *Behavioral Research in Accounting*, 13: 1-24, 2001.

[7] *The Wall Street Journal*, "U.S. Says Chinese Professors Stole Tech," 20 May 2015, p. A1

Reviewed by Larry Marks, CISA, CISM, CGEIT, CRISC, CFE, CISSP, CSTE, ITIL, PMP, who has extensive experience in implementing IT processes, policies and technology regarding internal controls and information security in the financial services, insurance, health care and telecommunications industries.

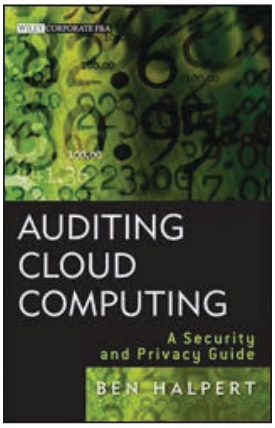
Auditing Cloud Computing: A Security and Privacy Guide

Auditing Cloud Computing offers an independent supplement to *Security Considerations for Cloud Computing*, part of ISACA's Cloud Computing Vision Series, which provides guidance to the auditor on how to help IT and business professionals who are considering the possibility of moving to the cloud.

Besides the generic approach to minimizing risk to the organization through a careful review of the contract, supporting appendices and service level agreements (SLAs), and white papers published by the cloud provider, *Auditing Cloud Computing* recommends that the auditor supplement the review by first identifying the type of cloud that is being contracted. The author suggests that the auditor's approach cover:

- Cloud-based governance of enterprise IT (GEIT)
- Cloud-based IT service delivery and support
- System and infrastructure life cycle management for the cloud
- Global regulation and cloud computing
- Business continuity and disaster recovery

Specifically, *Auditing Cloud Computing* points to risk related to cloud computing, which enables readers to do a deep dive on business continuity processing for the application. The book further emphasizes the importance of questions on where the data are located, given that business is of a global nature and many countries have their own data privacy requirements. The book recommends that the auditor not shy away from hard questions and ask the questions that matter (e.g., Does the provider regularly back up all data to tape and store it offsite? Can the customer approve any maintenance, updates or changes?). There are usage scenarios to be considered within the context of the cloud that the auditor has to ask as part of due diligence (e.g., When the organization wants to move away from this cloud service, how does it deprovision and transition assets out of the cloud vendor to another location for another context?).



By Ben Halpert

The auditor needs to view the venture and IT risk from a business point of view, not just as boxes on a checklist. Some questions to ask are obvious, such as those regarding the risk to the enterprise if the vendor were to go bankrupt or not be able to continue servicing the client. But high-level business and control questions grouped around categories of governance need to be asked as well. The book also recommends that the checklist the auditor uses to guide the review not be locked in to a style of cloud, deployment model or type of customer. The auditor must have the vision and perform due diligence to ask questions that may not have an answer, and enterprises should be cautious of the questions for which there is no answer.

The book provides an overview of cloud deployment models and other cloud concepts so that the reader has a proper foundation on cloud basics. It does not require that readers have an understanding of cloud computing concepts. The book also provides real-life scenarios that auditors may encounter. *Auditing Cloud Computing* serves as a practical guide that can apply to other cloud possibilities that any employer may consider.

EDITOR'S NOTE

Auditing Cloud Computing: A Security and Privacy Guide is available from the ISACA® Bookstore. For more information, visit *www.isaca.org/bookstore*, email *bookstore@isaca.org* or telephone +1.847.660.5650.

Do you have something to say about this article?

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

Go directly to the article:

Cybersecurity in the Quantum World

Michele Mosca, Ph.D., is one of the world's leading researchers in quantum computing and quantum cryptography. Mosca is cofounder of the Institute for Quantum Computing at the University of Waterloo (Ontario, Canada) and a founding faculty member at Perimeter Institute for Theoretical Physics. He cofounded CryptoWorks21, a training program in quantum-safe cryptography funded by the Canadian government. In 2015, Mosca cofounded evolutionQ Inc., where he serves as chief executive officer and president with chief technology officer Norbert Lütkenhaus, a pioneer and leader in quantum cryptography, to support organizations as they evolve their quantum-vulnerable systems and practices to quantum-safe ones.

Also available in Korean
한국어로도 가능

Most people probably lock their doors when they are not at home. They trust that the things they value—family photographs, artwork, financial information and medical files—will be protected, thanks to steel deadbolts that can be unlocked only with their own key.

But what if we learned that, one day soon, someone would invent a universal lock pick that could instantly and easily open any locked door?

Most would likely investigate whether a new kind of lock might be impervious to the universal lock pick. And, most likely, people would not wait until after a first break-in to change the locks. Instead, one would want to do it before burglars had a chance to test their new tool in one's neighborhood.

MODERN CRYPTOGRAPHY

In the Information Age, many of one's most valuable belongings—finances, medical histories and, to a large extent, identities—are kept safe behind digital deadbolts.

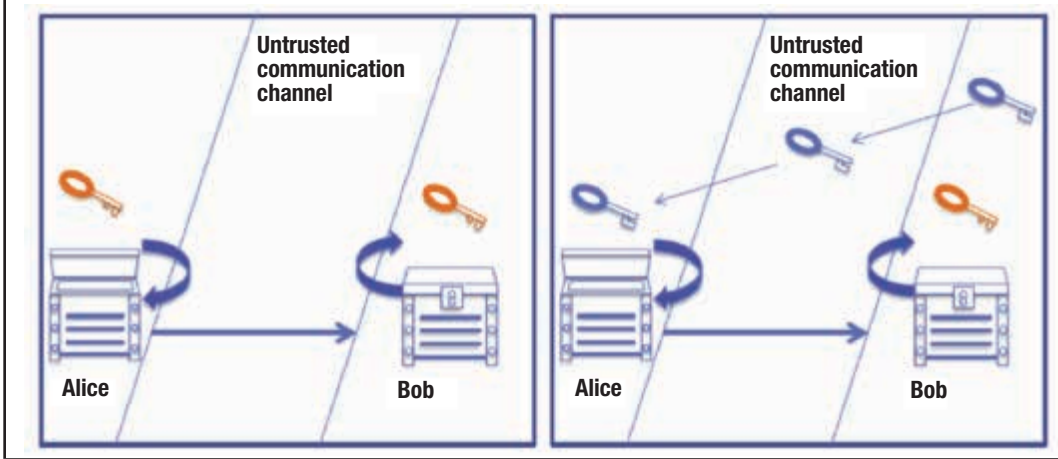
The reason people can safely make money transfers and buy products online, and why major institutions and governments can exchange vast amounts of private data, is that information is protected by the complex "keys" of cryptography.

Present-day cybersecurity, like the lock on a front door, is reliable because the key used for an online transmission is digitally unique from countless other possible keys—and it is practically impossible for a cybercriminal to guess which one will unlock the door to private data. Online, keys are typically based on mathematical problems that are too difficult for even the most powerful computers to crack. One can trust that an online mortgage payment, for example, cannot be intercepted and stolen because a unique cryptographic key is shared between the payer and the bank, and the safety of that key is assured by the mathematical problem on which it is based.

Figure 1 illustrates that in symmetric key cryptography (left), two parties, typically referred to as Alice and Bob, share the same private key (illustrated in orange). For example, Alice may encrypt a message with the key, send the ciphertext through an untrusted channel, and Bob may decrypt the message with the same key.

In public key cryptography (right), each party, say Bob, has its own private key (again, illustrated in orange) that it shouldn't share with anyone, and a public key (blue) that may be

Figure 1—Symmetric and Public Key Cryptography



Source: Michele Mosca. Reprinted with permission.

freely disseminated to anyone interested in communicating with Bob. Any party, say Alice, may, for example, encrypt a message with Bob's (nonsecret) public key and send the ciphertext to Bob through an untrusted channel, and only Bob can decrypt the message. Public key cryptography may also be used to confirm the authenticity of the origin of information received and its integrity (e.g., during automatic software updates in order to confirm the updates are not malware).

The impact of quantum computers on symmetric key cryptography is serious; however, doubling key lengths protects against the currently known quantum attacks. In contrast, quantum cryptanalysis will fundamentally break RSA and elliptic curve cryptography (ECC)-based cryptography, as well as any other system, based on the difficulty of factoring large integers or finding discrete logarithms. Longer key lengths will not suffice, and fundamentally new methods for establishing keys in a public key setting will be needed.

But what if it was found that a kind of universal digital lock pick is on the horizon—one that could efficiently solve such mathematical problems? Would users seek a new kind of lock?

This once might have been a purely hypothetical question, but not anymore. It is a question that every person and, crucially, every organization needs to ask before it is too late.

It is the question of cybersecurity in the Quantum Age.

QUANTUM TECHNOLOGIES

Quantum computers are machines that harness and control the phenomena of the quantum world, the world of atoms, electrons, photons and nature's other building blocks, to process information in a radically different way than present-day computers.

Whereas today's computers perform operations by manipulating binary bits of ones and zeros, quantum computers process information with quantum bits (qubits), which behave in profoundly different ways than classical bits.

The laws of quantum mechanics, a pillar of modern physics, alongside Einstein's general relativity, allow quantum particles to be in a superposition of states. An oversimplified, but not entirely inaccurate, way to think of superposition is that a quantum particle can be in two different places, or states, at the same time.

It is a counterintuitive idea because human intuition has evolved in the bigger, messier world where quantum effects are not directly evident.

But the everyday world and the quantum world are converging. Computers, which just a half century ago filled an entire room, now fit in pockets and are extraordinarily powerful. Engineers have perpetually found new ways to make transistors, the on/off switches that enable computing, smaller and smaller, thereby allowing more to be crammed onto every microchip and increasing their efficiency and power.

This miniaturization of transistors is quickly nearing a threshold, however. Before long, transistors will shrink to the size of atoms and the rules governing their behavior will flip from classical to quantum. This threshold was long considered a kind of dead end for innovation in computing, until some scientists (the famous Richard Feynman among them) wondered if the switch from classical to quantum could somehow be turned into an advantage. The superposition principle, they argued, could mean that a qubit in a quantum computer could be not only a "one" or "zero," but both simultaneously, leading to a special form of parallel computation and a drastic, even exponential, increase in power.

QUANTUM CRYPTANALYSIS

Until recent decades, though, quantum computing sounded like the stuff of science fiction. Even if it were possible, and most people doubted that given how tiny and difficult to control quantum particles are, it was unclear for what it might be useful.

That changed almost overnight when applied mathematician Peter Shor demonstrated an algorithm that, if run by a quantum computer, could do something it was believed no classical computer could efficiently achieve: the mathematical feat of factoring very large numbers.

This is exactly the mathematical problem on which much of today's cybersecurity is based.

Quantum computers are still in the research and development stage. The science behind them is extremely complex, but working prototypes are emerging from research groups around the world.

Once the question was if quantum computers would become a reality. Now the question being asked is: "When will they become a reality?"

MANAGING QUANTUM RISK

An even more urgent question, especially for people and organizations that rely on cybersecurity, is whether they will be ready for the threat that quantum computers will pose to their ability to protect data from cyberattack.

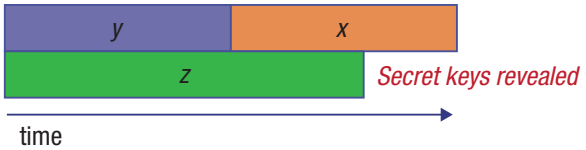
Although the digital burglars are not yet in the neighborhood, so to speak, updating cybersecurity to be quantum safe is much more complicated and time-consuming than changing the deadbolt on a front door.

What organizations need to begin thinking about now is not an immediate, drastic overhaul of their security infrastructure, but rather an "ounce of prevention" as quantum technologies begin to take shape on the horizon. It is better to evolve in pace with technologies rather than react reflexively to a major disruption; it is the more strategic, efficient and, ultimately, cost-effective approach.

Most cybersecurity infrastructures are extremely complex, particularly for large organizations, institutions and governments with varying security demands, and no two systems are exactly alike, so there is no one-size-fits-all solution for quantum readiness.

If powerful quantum computers become available, say, 10 years from now, but it takes a given organization 11 years to retool its infrastructure to become quantum safe, it is already too late for that organization to be impervious to the quantum threat. Furthermore, to protect against the compromise of information that was communicated a certain number of years in the past, the changeover to quantum-safe techniques must happen at least that many years before quantum computers are available (**figure 2**).

Figure 2—Will Your Secrets Be Revealed?



Source: Michele Mosca. Reprinted with permission.

Even if one is able to deploy quantum-safe tools before the quantum threat is realized, organizations responsible for keeping information confidential for some number of years, say x, must be sure that they are utilizing quantum-safe tools and practices at least x years before the quantum threat is at their doorstep. In other words, if it takes y years to quantum-proof their tools and systems, and z years for the quantum threat to become reality, then it is critical that x+y<z. Otherwise, the confidentiality guarantees will be compromised.[1] For example, if 5 (x) years of confidentiality are required and the quantum threat is 15 (z) years away, then the organization must quantum-proof its systems in under 10 (y) years.

It is impossible to predict exactly when full-scale quantum computers will be available, but the pace of research and innovation is accelerating every day.[2, 3]

Quantum computing research is well motivated and well funded at research facilities around the world, and the potential benefits of quantum computing are great. But the double-edged sword of quantum computing is the threat it poses to information security if it is used for the wrong reasons. For the advent of quantum computers to be a positive milestone in human history, the cyberinfrastructure must be quantum-proofed in time.

QUANTUM-SAFE OPTIONS

Thankfully, quantum technologies also make possible one solution to that threat. Quantum cryptography capitalizes on quantum phenomena to protect private information in ways that even a quantum computer cannot crack. It is based on the law of quantum mechanics that says that observing quantum data necessarily disturbs them; this means that any eavesdropping on a quantum transmission used for key establishment can be instantly detected before any data can possibly be compromised. Such quantum key distribution (QKD) is already commercially available and has been used to protect important bank transfers and other communications.

There are also forms of postquantum cryptography, which are not themselves based on quantum techniques. Like today's public key methods, they use conventional technologies and rely on assumptions about the infeasibility of some mathematical computations; however, they are secure against all currently known forms of quantum or conventional cryptanalytic attacks.

Determining which of these approaches, or what combination of them, is required for an organization to face the coming quantum threat to cybersecurity is something that needs to be determined on a case-by-case basis.

For many organizations, the urgency lies not in drastically overhauling cybersecurity infrastructure today, but in analyzing the potential vulnerabilities and laying the groundwork so that a transition can be undertaken if/when the need becomes imminent.

Assessing those vulnerabilities and determining what is needed to remedy them is the essential first step in charting a course toward quantum readiness.

The consequences of unpreparedness are potentially enormous: the compromise and potential collapse of financial systems, energy grids, e-commerce, stock markets and other essential digital infrastructures on which society relies. Those consequences vastly outweigh the relatively small investments required to make those infrastructures quantum-ready.

It may not yet be necessary to install a new digital deadbolt. But for the sake of what is most valuable, the time is now for organizations to look carefully at their current security systems to ensure that the threat, when it arrives, will not get past the front door.

REFERENCES

Pecen, Mark; *et al.; Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges*, white paper, European Telecommunications Standards Institute, October 2014

Menezes, A. J.; P. C. van Oorschot; S. A. Vanstone; *Handbook of Applied Cryptography, (Discrete Mathematics and Its Applications)*, CRC Press, England, 1996

ENDNOTES

[1] Mosca, Michele; "Setting the Scene for the ETSI Quantum-safe Cryptography Workshop," e-proceedings of 1st Quantum-Safe-Crypto Workshop, Sophia Antipolis, 26-27 September 2013

[2] Steffen, M.; D. P. DiVincenzo; J. M. Chow; T. N. Theis; M. B. Ketchen; "Quantum Computing: An IBM Perspective," *IBM Journal of Research and Development*, vol. 55, no. 5, paper 13, September/October 2011

[3] Devoret, M. H.; R. J. Schoelkopf; "Superconducting Circuits for Quantum Information: An Outlook," *Science*, vol. 339, no. 6124, 8 March 2013, p. 1169-1174

Addressing Cybersecurity Vulnerabilities

Omar Y. Sharkasi, CBCP, CFE, CRP, is a retired lead IT bank examiner at the State of Illinois (USA) Department of Financial and Professional Regulation-Banking Division (IDFPR). His significant work experience includes regulatory compliance in the fields of information security, risk management, business continuity, Payment Card Industry Data Security Standard (PCI DSS), fraud prevention/detection strategies, data loss prevention system implementation, and policy enforcement. Prior to the IDFPR, he worked in diverse industries in the field of accounting and finance.

Today's IT leaders face many challenges and rapid changes with respect to Internet security. IT leaders must increase cybersecurity public awareness and coordination across the subset of federal governments, all while having to do more with less. They have to protect enterprise, customer, citizen, member and employee data, while thwarting attacks from cybercriminals. The problem is that much of the legislation worldwide addresses regulatory compliance and fails in advising organizations on the ins and outs of information security. That is to say, following regulatory guidelines may ensure compliance but not necessarily offer system security. This leaves many enterprises scrambling to understand their information security infrastructure and obligations. Conducting secure transactions across the Internet relies on a number of factors, not the least of which is government guidelines.

The Internet contains a virtual encyclopedia of information. It is also touted as the platform upon which the majority of business and consumer transactions takes place. This responsibility is being thrust upon a network on which reports of security violations (e.g., cyberhacking, exploitable holes) are on the rise at the same time that fortifying any system requires daily diligence on the part of network administrators. The Internet has provided terrorists and other criminals with a deadly, sophisticated new weapon in their arsenal. Yet the full potential of secure Internet connections has not been realized. Until recently, service providers, government organizations and private enterprises have been unable to benefit from the cost savings and flexibility of choosing the right security tools to mitigate the risk of deliberately intercepted, stolen or corrupted sensitive data.

> "Much of the legislation worldwide addresses regulatory compliance and fails in advising organizations on the ins and outs of information security."

The point is, with all of the weapons and adversaries present—threats, malicious intruders, thieves, disgruntled employees, industrial espionage and so on—security professionals should be able to detect, prevent and address security incidents and, if needed, provide information to help prosecute computer crimes.

Knowing who has access to critical data and making users take proper precautions to safeguard their files, workstations and mobile devices are basic steps all businesses should take. It is vitally important for financial, legal and health care operations to overhaul their information security processes and require IT positions to be filled by qualified staff who have undergone thorough background checks. Thus, organizations should consider the US Patriot Act and legislation such as the US Gramm-Leach-Bliley Act (GLBA), US Health Insurance Portability and Accountability Act (HIPAA), US Identity Theft Act, the new press releases from the Federal Financial Institutions Examination Council (FFIEC), Financial Crimes Enforcement Network's (FinCEN) Executive Alert, the US National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), and universally accepted standards and frameworks such as the ISO 27000 series, COBIT® and Industrial Automation Systems technologies.

This article examines the key areas in security programs that need attention now. This, in turn, helps create a framework to assist in meeting regulatory and security requirements, ensure corrective actionable recommendations for new processes and upgraded techniques, and enable security teams to face today's issues and prepare for tomorrow's. While much of this article is based on US legislation and US business, the analysis is applicable to many other nations.

Naturally, IT issues, whether intentional or unintentional, and unchecked cybersecurity 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 choose the Comments tab to share your thoughts.

Go directly to the article:

factors are the major cause of weak security of any business technology innovation. Not everyone is comfortable discussing them publicly, and many are still working on the fix. Quite often, unchecked IT cybersecurity risk factors that remain unmitigated for too long—something that happens in almost all businesses—are the cause for unexpected cyberattacks. The following are necessary areas for improvement.

AREA FOR IMPROVEMENT 1—INVENTORY OF ASSETS/DATA CLASSIFICATION

The data resource is as important as capital or personnel. Because of their value, data must be managed and controlled carefully. As noted in the preceding section, in addition to personally identifiable data, every business has other, highly proprietary information that it must protect (e.g., intellectual property, marketing plans, new product plans, investor information, financial information). These are all valuable assets of the business, deserving of protection. However, most enterprises' assets are not clearly and appropriately accounted for to an established inventory scheme. If information/physical assets are not clearly and appropriately labeled and documented, the efficacy of the asset inventory and data classification programs is greatly diminished. Without assigning ownership for specific assets, it becomes difficult to ensure that assets will be appropriately protected on a continuous basis. Asset inventory and associated data classification degrees of protection must be determined and applied to all information. Deciding which assets need protection is half the battle. Focusing on those critical and sensitive business processes is a crucial step in defending against cyberattacks.

A strongly established data function or active and consistently applied data management principles can help ensure data integrity and security. No matter how big or small the information security budget is, the key to security is prioritizing the effort to protect data.

Securing data must begin with data classification. To help ensure the integrity of data and the application of sound data administration practices, security managers must address issues that affect the credibility and security of the data being used. Security managers can ask the following questions to assess the credibility and security of their data:

1. Is there a centralized asset management team? If not, set one up as soon as possible.
2. Does the team complete regular or, at minimum, spot reviews of the various analyses? Does it regularly work with data owners to update and add new data resources?
3. What data do users need to access?
4. Where are the data located?
5. Do the team and the data owners have established or defined rules by which particular information classes of instances must be stored, transmitted, archived, transported and destroyed?
6. How much sensitive/critical information is available on the Internet?
7. Does the team know the cyberrisk protection their vendors and other relevant third parties have in place?

Ultimately, various business owners and the IT department must decide on what technologies and risk they are willing to live with, since most of them will have to maintain and administer the controls in some form. An understanding of user needs and existing systems is necessary to strike a balance between asset productivity and security.

AREA FOR IMPROVEMENT 2—EMERGING TECHNOLOGY RISK

Assessing and minimizing the risk of emerging technology security are the first things enterprises do before using Internet of Things (IoT) technologies to manage IT systems, building equipment, smartphones and other web-enabled intelligent systems. These first steps ensure that these technologies have adequate safeguards to fend off hackers. Many such technologies are vulnerable to attacks that could disrupt building operations and, worse, give hackers access to enterprise systems.

> "Auditors should play a significant role in IT projects and be part of the monitoring processes."

IoT increases the security complexity by promoting the use of web services, multitiered applications, distrusted databases, security zones and getting into a virtualization rut. For instance, enterprises began server virtualization in 2009 and chose virtualization hastily without appropriate risk assessment and with total reliance on vendors, hoping to learn from them and thinking of private cloud services as a safe choice. Typically, new technology initiatives are deployed without a detailed risk assessment in place. In fact, innovation often happens only after putting

new IT projects in employees' hands without proper risk assessment, security, accountability and proper IT audit.

To reduce risk, enterprises should pay more attention to newly proposed technology initiatives, ensure involvement of IT auditors in the early stages of any IT project, and extend the audit scope to include new technologies and management systems. Additionally, the performance of postimplementation review should be considered or viewed as a value-added audit project by the audit team. The audit team needs to have the right level of support and sponsorship to engage in the early stage of any IT projects. Auditors should play a significant role in IT projects and be part of the monitoring processes to ensure quality inputs and the merits of the project, rather than simply being involved with the outcome.

> "When security is not represented during due diligence, problems can go undetected and may be costly to fix at later stages of project implementation."

New technology brings more ways to access new types of devices and alternatives to the traditional personal computer (PC) or mainframe platforms. However, many new technology initiatives lack proper controls due to the issue of not assessing and addressing security problems on time and ignoring their warnings. It is always best for enterprises to do a security review before completing due diligence. When security is not represented during due diligence, problems can go undetected and may be costly to fix at later stages of project implementation. Security experts suggest that the following steps should be taken in order to best protect new technology initiatives:

- Integrate security at the beginning of the software development life cycle. Risk and threat assessments should be built in up front rather than bolted on later.
- Integrate security into the maintenance process, such as ensuring that all applications are patched regularly. Mobile device applications and bring your own device (BYOD) policies need to be included in the maintenance process so that these devices do not become vulnerable.
- Develop best practices for protecting legacy applications that might require special handling, such as building segmented networks and deploying any additional defenses that might be required for protecting legacy software.
- Make sure that security devices (e.g., security default settings) are configured correctly and the engineering team understands what the alerts mean.

AREA FOR IMPROVEMENT 3—THE SHEER SIZE OF THE RISK ASSESSMENT MODULES

The conventional model for risk assessment is questionnaires and onsite audits, with results recorded in documents and updated annually. As a result, a large number of risk assessment modules and methodologies have been created. Organizations use numerous risk assessment matrices that vary from department to department, identifying variations in risk and mitigation strategies across different assets, business processes and applications. Point-in-time, piecemeal assessments are no longer sufficient. Discovering this insufficiency led to the belief that IT risk assessment processes may be practiced in an *ad hoc* manner, without following defined processes or policies. As a result, IT risk processes are today considered ineffective, inconsistent, fragmented and not robust enough to provide tools to secure the IT environment and the related enterprise functions. Furthermore, the responsibilities for continuous risk assessment processes are informal and have limited authority. Risk mitigation strategies are a top concern for the board, senior executives, the chief financial officer (CFO) and risk managers. And despite the need for rapid change and a robust risk assessment program, the challenge remains for implementing an integrated approach that can be ingrained in an organization and its management practices. Without a coordinated risk management strategy, organizations will continue to

struggle with repeated policy iterations before risk-handling procedures and controls are efficiently aligned. Simply put, enterprises must get a handle on risk management. It is a key link to instilling more customer confidence, higher profitability and company longevity.

For example, many enterprises actively hedge their IT portfolio risk to immunize against asset/liability mismatches. Others focus on building a tangible asset portfolio, which does not include intangible assets, securitized and managed by specialists. Depending on its strategy, an enterprise can now more effectively decide what market risk it wishes to manage or assume. Risk that falls outside these parameters is avoided by transferring it to a third party. An enterprise risk dashboard brings together all of the key risk exposures—operational risk, reputational risk and more. With this dashboard, management can review changes in exposure and evaluate the potential impact on capital allocation throughout the operations. Drilling down into the risk management decision areas gives management additional insight into inherent Internet risk (e.g., loss events, loss of data or reputational risk assessments) and into the methods of responding to risk (e.g., avoidance, reduction, sharing, acceptance).

> "These valuable business benefits of cloud computing cannot be utilized without addressing the new data security challenges posed by it."

AREA FOR IMPROVEMENT 4—DATA RESIDENCY/CLOUD COMPUTING RISK

Data residency violation is considered a major contributor to cyberattack risk, and it can cause massive data breaches and regulatory compliance issues. Corporate data are stored by utilizing cloud computing services. There are numerous cloud providers headquartered in every corner of the globe, with data centers equally distributed, and the typical end users may not think to question where the corporate data they upload will be stored. Unfortunately, in some cases, that *where* is critical to remaining in compliance with data privacy and data residency regulations. The revelation that employees have been storing data where they should not is one that can end up involving not only data breaches, but also legal risk.

The major cloud application providers tend to offer robust security, but the same cannot always be said of smaller or more niche providers. In fact, some providers do not even offer basic transport layer security such as Secure Sockets Layer (SSL) to protect data while in transit to their servers. Employees uploading sensitive documents on unencrypted connections is an issue that must be addressed.

Enterprises increasingly recognize cloud computing's compelling economic and operational benefits. Virtualizing and pooling IT resources in the cloud enables organizations to realize significant cost savings and accelerate the deployment of new applications. However, these valuable business benefits of cloud computing cannot be utilized without addressing the new data security challenges posed by it. Deploying confidential information and critical IT resources in the cloud raises concerns about vulnerability to attack, especially because of the anonymous, multitenant nature of cloud computing. Applications and storage volumes often reside next to potentially hostile virtual environments, leaving information at risk to theft, unauthorized exposure or malicious manipulation. Moreover, it is possible for data to remain present when consumers vacate cloud volumes, but vendors may not recycle storage devices securely. Governmental regulations on data privacy and location present the additional concern of significant legal and financial consequences if data confidentiality is breached or if cloud providers inadvertently move regulated data across national borders. As enterprises make plans to deploy applications in private and public cloud environments, new security challenges need to be addressed.

Optimal cloud security practices should include encryption of sensitive data used by cloud-based virtual machines, centralized key management that allows the user (and not the cloud provider) to control cloud data, and an assurance that cloud data are accessible according to established enterprise policies. A key component of an IT cloud development strategy is conditioning the IT vendor infrastructure for cloud delivery. This may include virtualizing and automating existing systems and adding the vendor service management capabilities requisite for cloud computing. It is advisable to get a security assessment from a neutral third party before committing to a cloud vendor.[1]

AREA FOR IMPROVEMENT 5—MIND THE INTERNAL THREAT

While the majority of enterprises use networks as the backbone for secure data exchange transactions, standard encryption and firewall technologies can provide some measure of protection from outside attacks and theft by competitors, hackers or mercenaries. But what about the internal threat committed by the enterprise's employees armed with computer access and passwords? The employee element is commonly overlooked. In fact, one of the most common bugs exploited by hackers to gain access to the inner workings of equipment is using default passwords. Default passwords are, from a manufacturing point of view, a convenient way of ensuring that its engineers can get into the company's own computers when carrying out maintenance. Too often, security administration is overwhelmed with the task of trying to do it all (e.g., managing operating systems, applications, network, mobile devices, physical security). Security administration must segregate duties and define and deploy a security policy for one area before moving on to another hot spot.

In conjunction with preventing internal irregularities, segregation of duties (SoD) should be applied so that the person responsible for assessing users' level of access authorization is not the same person who implements the access controls. Traditionally, SoD has been used to prevent any one individual from having sufficient power to perpetrate a fraud or as a check on the correct performance of one person's duties by other personnel. This principle of internal control is fairly easy to follow for simple systems, which have well-defined processes and few interfaces with other systems. However, as systems become more complex, the number of interfaces among subsystems increases, as does the risk of error in the communication process. In this case, the SoD can increase risk rather than prevent control problems.

Besides the control problems that can result from improper SoD, two other security aspects represent direct threats to data integrity. First, the existence of the privileged user role partially violates the traditional control principle of SoD. Second, the privileged user has available tools that, though necessary for the performance of various functions, can be used to override established controls. For example, tools exist to establish various levels of access and update authorization, crack and find user passwords, restructure the databases, and manipulate programs and files.

The privileged user can assign to a program a level of access, modify the web design and update authorization that can override all other controls. Furthermore, access paths can be eliminated to remove records from audit trails. For these reasons, database or security tools must be used only for their intended purposes.

The primary emphasis must be placed on administrative controls. Several remedial steps can be undertaken to increase controls and reduce the risk of internal threats. And the requirement to meet compliance demands, mitigate insider risk, and manage access and privileges of temporary workers, contractors and third parties is driving the requirement for least-privilege security across the Windows operating system (OS) environment and beyond to UNIX and Linux systems, regardless where these systems run (on the premises or in the cloud).

Poor password security and the "too much privilege" problem need to be addressed by delegating security administration and limiting what administrators can do to the tasks and resources required for their job roles, while enabling a fast, simple method of privilege elevation when required. A wide range of roles and rights are available in the Windows OS to implement least-privileged access for any user in the environment, while flexible and granular secure delegation using common sense allows for simplified management of roles and rights.

AREA FOR IMPROVEMENT 6—END-POINT SECURITY

Unfortunately, the issue of end-point security is being ignored by a significant number of enterprises. But the growing number and variety of threats to end points, in addition to the threats that use end points as a vector, have made end-point security a relevant topic to cybersecurity. Common end points are laptops, desktops, PCs and mobile devices. Most of these devices are not under the control of an organization, and one of the main concerns is management controls. As technologies continue to expand to meet the challenges of components' integration and data sharing, and as mobile workforces continue to grow and more people access corporate resources over structured public networks, the challenge becomes controlling what data should be allowed to reside on those end points or mobile devices and, when allowed, securing the data while at rest and in transit. Security administration should always weigh the security advantages of totally locking

down an end point so no applications can be loaded, no port is active and no unauthorized communications can occur vs. the productivity gains of allowing people to use the technology being offered. To be effective, end-point security must balance the security risk with the productivity benefits. The right approach must also address the IT challenges faced by business today—mainly regulatory compliance and overburdened and understaffed IT departments. The solution sometimes requires compromise and relies heavily on solution tools that could manage, assess or control security at the end point. End-point protection should be focused on tools that deliver a centrally managed, web-based, easy-to-use, fully integrated management interface that delivers a full suite of protection to end points.

Clearly, no end point is truly secure without an integrated and embedded multilayered security approach throughout. End-point security tools should also be supported by a management dashboard that provides real-time security posture reporting over all managed end points.

A product of layering insecurity may take years to develop, deploy and implement once configurations have been created. Furthermore, as the number of connections to business partners increases, the amount of remote access grows, and the variety of services offered to customers rises. The originally reasonable set of security layers in network architecture can turn into a complex tangle of security mechanisms that may not be effective and may introduce more system vulnerabilities. The key to making the most of security layers remains in segregating sensitive data into separate zones. Also, the security designer must conduct a full analysis of the enterprise's layered security every year and repeat the assessment with every major addition to the enterprise's network environment. All of these factors—and many more—must be evaluated before selecting any sort of end-point security solution.

AREA FOR IMPROVEMENT 7—STRUGGLING TO DEAL WITH LEGACY SYSTEMS

Now that Microsoft has pulled the support plug for Windows XP, financial institutions (FIs) and companies that have not switched to Windows 7 need to explore their options. For FIs, this means upgrades to Windows 7 and Agilis 3 are required to keep up with the latest patches and maintain Payment Card Industry Data Security Standard (PCI DSS) compliance. Most FIs began a legacy system replacement early in 2014. But some FIs failed to truly understand the complexity of management reporting they had developed internally over the years, not to mention integrating multiple systems from different vendors. Specifically, neglecting the reliance on numerous system features or databases that tied to the old system required processing and culture changes to switch software and get off of those old functions. For these reasons, FIs felt that they needed a more comprehensive compliance plan before jumping in with upgrades. As a best practice, many FIs found it possible to get by with a special contract with Microsoft in which they could keep Windows XP and get the necessary security patches to remain compliant until they are ready to upgrade in conjunction with other planned changes.[2] Now that the Windows XP transition deadline has passed, continuing to ignore the upgrade puts FIs at risk. And because other requirements are coming, it makes sense to create a plan that addresses not only a Windows 7 upgrade, but future needs as well.

In addition to the Windows 7 requirement, FIs must address Europay/MasterCard/Visa (EMV) liability changes, which are a series of updates that will shift the liability for card counterfeiting losses from card issuers to transaction acquirers that do not enable EMV transactions.[3] These shifts began in 2015. In addition, PCI DSS 3.0 and 3.1 guidelines state that an updated version of the Encrypting PIN Pad (EPP7) will be required to maintain compliance on automated teller machines (ATMs) purchased, installed or moved after April 2014. ATM compliance and technology changes focus on EMV and EPP7.[4] Of these two, EMV requirements are more involved, with implications for ATM hardware, software and network systems.

> "Data must be available anytime, on time and anywhere in the organization, whether IT approves of it or not."

Fraud-prevention advocates welcome EMV technology. The adoption of EMV technology, which replaces traditional magnetic stripe payment cards with more secure chip cards, could eliminate up to 30 percent of the US $8.6 billion in annual fraud losses by card issuers and merchants in the US.[5] Generally, card fraud drops in areas where EMV is in place, so the long-term gains are worth the short-term pain of transition. EMV cards are replacing current magnetic cards

or non-EMV chip cards. Adoption of EMV depends on the region. Adoption was first seen in Europe, followed by Asia-Pacific, Latin America and Canada. While EMV adoption is not mandatory, it will be necessary in order to accept EMV chip cards. The US is one of the last countries to migrate to EMV. In 2011 and 2012, American Express, Discover, MasterCard and Visa all announced their plans for moving to an EMV-based payments infrastructure in the US.[6]

AREA FOR IMPROVEMENT 8—FILE-SHARING APPLICATIONS

Effective file sharing is a necessity in knowledge-intensive organizations. Today's knowledge workers want and demand access to their files whenever and wherever they need them. Data must be available anytime, on time and anywhere in the organization, whether IT approves of it or not. Employees are bridging the established enterprise infrastructure into their preferred work environment using solutions that corporate IT departments do not, cannot or are slow to approve. In short, knowledge workers are willing to look at tools outside of the paradigm offered by corporate IT to meet their needs.

As such, some organizations have users accessing hundreds of unsanctioned cloud applications, of which half or more are often file sharing. There are two problems with free or cheap consumer-facing file-sharing cloud applications: There are a lot of them, and not all of them are equally secure. As they have become more ubiquitous, file-sharing applications have become a significant concern for IT departments, especially in security-sensitive industries such as financial services. IT departments have to decide how strict the regulation of these applications will be and enforce compliance with these regulations. IT can outright prevent the installation of the application on workplace desktops and laptops through administrative lockdown (at the expense of the freedom of end users to customize their workstation). Access to web-based file-sharing services can also be restricted by blocking specific domains. But IT will have a harder time preventing information from leaking through mobile device sharing. As with most personal unmanaged applications (PUAs), file-sharing applications may be used with or without IT consent.

Documentcentric team collaboration is required for producing a variety of outputs, including internal-facing planning documents and external-facing deliverables. IT teams need adequate tools to collaborate around work-related documents. Collaboration platforms (e.g., Microsoft SharePoint) offer content repositories for working with documents, but many IT departments have set these tools up in a restrictive, cumbersome and unintuitive manner. It is important to establish strict, enforceable policies that are frequently communicated while still allowing users enough freedom to operate and manage their data comfortably.

AREA FOR IMPROVEMENT 9—SECURITY MATURITY AND REMOTE ACCESS

User systems are only as effective as the data they use. Data administration protects data from corruption and promotes the effective use of data. However, there are still a large number of enterprises that do not have a good grasp of control characteristics, classifications and requirements. Management needs to understand control requirements before assessing control strengths and weaknesses. In other words, there should be a basis or baselines in place (e.g., standards, guidelines, benchmarks) prior to control measurement and assessment.

> "No doubt, virtualized systems make it harder to manage risk, but sensible common sense security practices still apply."

Remote access is on the increase and telecommuting (working from home)/telepresence (video and audio communications for meetings) technology is becoming more prevalent as enterprises move to capitalize on its benefits, including gains in productivity and worker satisfaction. But administrators still have to master security best practices regarding these technologies.

Remote users can access corporate network services and resources with the same efficiency and functionality as if they were in the office. Business partners can connect to each other's networks, allowing for sharing proprietary information on joint projects.

The problem for many organizations is finding an efficient, affordable, scalable means of authenticating virtual private network (VPN) users. While there are many authentication solutions on the market, not all provide the best authentication and security solutions. Organizations want their VPN connections secure, but realize the security is only as strong as its ability to deploy a system, maintain it and have users consistently employ it.

No doubt virtualized systems make it harder to manage risk, but sensible security practices still apply. The key is deciding when to use tunnel vision technologies such as Internet Protocol Security (IPSec) VPNs and when to use SSL VPNs. Both IPSec and SSL VPNs can provide enterprise-level secure

remote access, but they do so in fundamentally different ways. Before choosing to deploy either, or both, an enterprise should know how IPSec and SSL VPNs stack up in terms of security and what the cost is for that security administrative overhead. Security is built on standards and products that implement those standards, but it ultimately depends on appropriate deployment and sound policy definition. It is not always that simple, of course. Vendors promise to deliver secure access, but are SSL VPNs as secure and reliable as IPSec?

VPN vendors point out three essential security requirements:

1. **Authentication and access controls**—Each VPN type presents different options for user authentication with clear implications for security. The fundamental difference in how SSL and IPSec VPNs implement access control is an important consideration in where and how each technology is best applied.
2. **Defense against attack**—Strong data configuration and integrity and resistance to message replay and other attacks are essential to make a VPN secure.
3. **Client security**—The tunnel cannot be secure if the host client is compromised. VPN client computers need strong authentication and firewall protection, and administrators need a way to check on the health of those systems.

While most organizations acknowledge the need for some sort of security, it is quite another matter to implement it. Yet it seems too many of these policies fail to create an effective IT security platform to handle the scale and complexity of managing cybersecurity risk for an enterprise today. However, the purpose of developing policies is to ensure prevention rather than detection. Prevention is deemed to be proactive. Detection is reactive. When dealing with flaws, detective controls are considered inefficient when compared to preventive techniques. Preventive measures stop flaws up front rather than finding and fixing them once found, which may be too late and costly to address. Knowing security controls up front allows development teams to build cost estimates and prioritize security issues alongside other priorities at project or iteration inception. Implementing upfront controls is most effective, and only then can application owners decide to accept the risk or mitigate the risk at the planning stage rather than at a later stage.

Clearly, at the very least, companies should adhere to a recognized standard (e.g., ISO 17799) and place a high priority on educating and communicating with employees about the risk of Internet communication and the threat of cyberspace landscaping. Security threats are growing more complex and more sophisticated, so businesses' weapons against them need to be more sophisticated as well.

AREA FOR IMPROVEMENT 10—CYBERSECURITY TEST TOOLS

Cyberattacks on enterprises and banks worldwide reflect a frightening new era in cyberwarfare. As many security experts say, "You cannot hack or protect what you cannot see." Traditional network security strategies have become increasingly complex and costly, yet they do not deliver the level of reliability that modern mission-critical computing environments require. The solution is moving to a deeper, inside-out software-based approach that greatly reduces the number of vulnerabilities that hackers and cybercriminals can exploit. Cybersecurity stealth tools do exactly this and are an innovative, software-based approach to security that saves money, increases security, and is an agile component that adapts to changes in critical business networks and rapidly evolving regulatory requirements. Enterprises need to understand the threat landscape and engage in basic cyberhygiene to be able to mitigate a broad range of cyberrisk. This includes knowing all the devices connected to the network, what software tools are being used, how to hide data, and who has administrative permission to change or bypass/override system configurations and reducing that number to only those who need those privileges. To that end, it is good to see developers starting to introduce security tools that bring together maintenance and help-desk products with the security system. Security professionals should become familiar with the tools, techniques and weapons used in attacking their security infrastructure. Then they will be prepared to make a number of wise acquisitions, bringing in the best-of-breed products.

> "The solution is moving to a deeper, inside-out software-based approach that greatly reduces the number of vulnerabilities that hackers and cybercriminals can exploit."

Often, cyberattacks such as identity theft, account takeovers and mass disruption might have been prevented if the enterprise had been aware that their network was being accessed via cybersecurity tools. Security experts agree that nothing can be done to prevent cybersecurity criminals from using The Onion Router (Tor) without raising the risk to legitimate users.

Tor is software designed to allow someone to remain anonymous when accessing the Internet. It has been around

for some time, but for many years it was used mainly by experts and enthusiasts. Tor's hidden services and anonymous browsing enables cybercriminals to cover their operations and provides a hosting platform to sell stolen information using bitcoins as currency. Tor is also dual-use software. For instance, it can be used by security professionals to hide data from cybercriminals and intruders, but it can also be used by criminals to hack into an Internet network and compromise its security. The key is to target those who would misuse the technology, and not the technology itself.

In addition to Tor, tools called botnets are emerging and are being installed on the compromised systems to attack the victims by controlling them from a remote location. The word "bot" (from robot) refers to automated software programs that perform specific tasks on a network of computers with some degree of autonomy. Typically, computers become bots when attackers illicitly install malware that secretly connects the computer to a botnet. These tools, among others, are readily identifiable through open-source research.

Another way of looking at security products is to look at the risk of free and open-source software (FOSS). FOSS refers to software tools that users are allowed to run, study, modify and redistribute without paying a license fee.[7]

There are benefits to using FOSS. FOSS offers the ability to create new applications quickly, reliably and economically. The desire to save money, develop quality and solid pieces of code, and reduce dependence on one or more vendors are the key reasons why enterprises of all sizes are taking FOSS seriously. Thus, FOSS products are gaining broad acceptance in organizations around the world and are moving into the cloud.

Drawn by similar competitive advantages, enterprises are beginning to merge open-source applications with the cloud. Increasingly, the building blocks of Software as a Service (SaaS) applications, cloud platforms (Platform as a Service [PaaS]) and cloud infrastructure (Infrastructure as a Service [IaaS]) are composed of open-source components. These versatile technologies provide vital competitive advantages, but they can also introduce risk when employed without adequate precautions. Recent evidence suggests that the presence of application vulnerabilities in open-source software is a far more pervasive problem than most people realize. Nevertheless, the use of FOSS does pose a risk, and generally FOSS tools are permitted to access the source code or allowed to redistribute programs. The risk comes from integration tools and a lack of technical skills or support to manage open-source efforts. FOSS redistribution access may be permitted due to concerns about security and licensing. FOSS adoption and usage necessitates the ability to enforce security policies, ensure SoD and protect an enterprise's intellectual property and programming integrity. When it comes to applications, security must be as pervasive as software codes themselves and the continuously evolving threats against applications.

Firms may benefit immediately from a heightened awareness of security tools and incorporating their knowledge into their transaction monitoring efforts to prevent unauthorized intrusion and/or hide sensitive data from possible intruders. What can security tools do for a company?

- Keep Internet users from becoming Internet abusers.
- Guard against network-draining viruses, spam and chain email.
- Crack weak passwords for policy enforcement and controls.
- Mitigate legal, compliance and reputational risk.
- Protect and prevent intellectual property or confidential information leaks.
- Improve logging management capabilities, facilitate incident investigation and provide an accurate audit trail.

WHAT CAN BE DONE?

It is evident that there is no simple solution to securing an enterprise's critical infrastructure. The process takes a lot of time and effort and some careful planning. A combination of three strategies—policy and technologies designed for cybersecurity, best practices, and a focused effort—are effective in mitigating the risk of attacks on enterprise systems.

In 2014, NIST[8] and FFIEC[9, 10] announced that they would build strategic security safeguards to help cyberspace users escape an emergency and devise and implement effective cyberrisk management and security policies to reduce cybersecurity threats and keep business and other organizations safe. At this point, sharing knowledge of vulnerability, threats, incidents and security safeguards used by others is highly encouraged to mitigate cybersecurity risk.

To get started on this track, enterprises of all kinds are trying to protect themselves against advanced persistent threats (APTs) by relying on firewalls and other traditional signature-based antivirus defenses. In addition to antivirus and firewall technologies, IT security practitioners need a mix of tools as cited in frameworks such as the Cybersecurity Framework or the FFIEC announcements and guidelines.

They should begin by implementing well-understood best practices, starting with end-point hardening to remove existing malware and to close and manage vulnerabilities. Even then,

they ought to have a plan for detection and a response strategy if a breach should occur. Here are three key tools to maintain and consider when mitigating cybersecurity risk:

1. The NIST Cybersecurity Framework encourages network equipment manufacturers, enterprises, service providers, government agencies and federal integrators to take an active role in risk management, with the goal of improving the security posture and defending the IT critical infrastructures from cyberattackers and intruders. The NIST framework's approach to risk assessment is best described as a life cycle of activities based on five core functions that organize cybersecurity activities at their highest level. The framework consists of three parts: the framework core, the framework profile and the framework implementation tiers. The most important thing to remember is that risk is evolutionary, which means these activities must be continuously repeated and refined. This is NIST's first attempt at improving cybersecurity infrastructure, so this framework only scratches the surface of the activities involved in the risk life cycle. Each of these steps seems intuitive, but few organizations effectively execute all of these steps at any given time. The security chain is only as strong as the weakest link.[11]
2. FFIEC announced and introduced a cybersecurity assessment summary on its web site.[12, 13, 14] This initial round of assessments focuses on five key components of cybersecurity preparedness: risk management and oversight, threat intelligence and collaboration, cybersecurity controls, external dependency management, and cyberincident management and resilience. Per FFIEC guidance, FIs should think like hackers and develop a risk-based approach to security activities to mitigate increasing cyberthreats. To implement this type of holistic approach, security professionals must practice a variety of defense techniques (e.g., configuring access controls, addressing distributed denial-of-service [DDoS] readiness, assessing the capabilities of universal serial bus [USB] ports, enhancing BYOD security, and focusing on procedures such as penetration testing and ethical hacking). More specifically, each FI is expected to monitor incoming traffic to its public web site, activate incident response plans if it suspects that a DDoS attack is occurring, and ensure sufficient staffing for the duration of the attack, including leveraging next-generation test tools to assess and manage cybersecurity risk.

   Implementing NIST and/or FFIEC holistic approaches requires intensive training while developing a risk-based approach to security. Just as vital, though, is the need for cybersecurity education for all security experts. They must also learn how to properly use cybersecurity tools and conduct an organizational security audit to identify security breaches and other problems.
3. It is advantageous to strengthen IT relationships and categorize best business practices. Proactively managing cybersecurity risk is a must. From this perspective it is possible to broaden the sphere of knowledge to the risk landscape, beyond what has traditionally been an IT-based discipline. Being prepared to detect and respond to attacks and attempted attacks starts with knowing the computer environment. This should include having a cyberattack contingency plan. Having a business resilience plan that includes cyberattacks will not only save money on impacting events, it will also allow business to resume much sooner than if data are lost or compromised.

CONCLUSION

Attackers need to find only one weakness to get into an enterprise system and spread their reach. Defenders need to plan for the inevitable breach and have a plan in place. If enterprises run out of options to deal with a cyberattack, they are done. Enterprises need to make sure that they are managing cybersecurity as they go.

Security professionals are going to have to make the correct investment in security infrastructure based on a sound cybersecurity plan that leverages industry standards and extends beyond traditional security standards to ensure strong preventive measures, more rapid detection, response and recovery (should a breach occur). For now, decision makers within the government and private sectors need to exert more efforts to that end, invent new and creative ways to protect IT infrastructures, adopt the best security practices, and educate the end user with a formally defined security policy to minimize data leaks.

ENDNOTES

[1] Gartner Group, "Assessing the Security Risks of Cloud Computing," June 2014, *www.gartner.com/doc/685308*

[2] Stewart, D.; "Outlook for ATMs After Windows XP," *BAI Banking Strategies*, 16 April 2014, *www.bai.org/bankingstrategies/Distribution-Channels/ATM/Outlook-for-ATMs-after-Windows-XP?utm_source=BSO_Daily_041714&utm_medium=email&utm_campaign=BSO_Daily_Enewsletter&utm_content=thoughtleadership&ca=901590949I*

[3] *Ibid*.

[4] PCI Security Standards Council, *Requirements and Security Assessment Procedures, Version 3.0*, November 2013, *www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf*

[5] Controy, J.; J. Fishman; *From Mag Stripe to Malware: Card Security Risks in 2011*, 13 July 2011, *www.aitegroup.com/report/mag-stripe-malware-card-security-risks-2011*

[6] *Ibid*.

[7] Federal Financial Institutions Examination Council (FFIEC), FIL 114-2004, "Risk Management of Free and Open Source Software," 24 June 2014

[8] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 2014, *www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*

[9] Federal Financial Institutions Examination Council (FFIEC), Advisory Letter, 24 June 2014

[10] Federal Financial Institutions Examination Council (FFIEC), Advisory Letter, 2 April 2014

[11] *Op cit* NIST

[12] *Op cit* FFIEC letter 24 June 2014

[13] *Op cit* FFIEC 2 April 2014

[14] FinCent Resource Center, Intelligence Division, Cybercrime Against Financial Institutions, *www.fincen.gov*

The Underground Threat

Larry G. Wlosinski, CISA, CISM, CRISC, CAP, CBCP, CDP, CISSP, ITIL V3, is a senior associate at the Veris Group LLC, and has more than 15 years of experience in IT security. Wlosinski has been a speaker on a variety of IT security topics at US government and professional conferences and meetings and has written numerous articles for professional magazines and newspapers.

The numbers are astounding. According to the Symantec *Internet Security Threat Report (ISTR) 2014*, the annual cost of cybercrime to consumers in the US is more than US $38 billion; in China it is more than US $37 billion; and in Europe it is more than US $13 billion.[1] On average, there are about 28 billion spam emails per day,[2] and the majority have a malicious intent. According to the *2012 Norton Cybercrime Report*, the highest number of cybercrime victims are in Russia (92 percent), China (84 percent) and South Africa (80 percent).[3] According to the 2014 Trustwave Global Security Report, the top three malware hosting countries are the US (42 percent), Russia (13 percent) and Germany (9 percent).[4] The top three spam hosting countries are the US, Canada and the UK.[5]

How did it get so bad that it is a worldwide problem that affects almost everyone? How did all those computers (i.e., desktops, workstations, laptops, mobile devices) get infected? Who is responsible for infecting all these machines? What are the costs to businesses, financial institutions and society in general? Can this malicious activity be stopped and assets be protected?

HOW DID IT GET SO BAD?

Malware can exist in a variety of forms, including key loggers, computer viruses, worms, Trojan horse, ransomware, spyware, adware and botnets, to name a few. Malware can be embedded in files that are accessed, and it can be activated by simply clicking a malicious file or link in an email. It can be planted, purposely or by accident, on web sites. It can be spread via communications software (e.g., email, Internet relay chats, spam), movable media (e.g., thumb drives, CDs, diskettes), wirelessly by infected mobile devices and by itself within an infected network.

Malware exists because of weaknesses and vulnerabilities in software systems at the operating system (OS), application, software utilities and hardware levels (i.e., computer chips). The complexity of software provides an advantage to those who develop the malware. Sophisticated malware, and those who use it, can hide their activities and cover their tracks by providing false addresses, redirecting traffic, erasing their activities (i.e., deleting files and information in log files), planting false information and working outside of the country in which the malicious activity is being conducted. Polymorphic malware even changes its signatures (i.e., file names and locations) so that antivirus software cannot identify the program components and remove them. Some types of malware make it very difficult to remove them because they can hide by changing file and directory permission settings. In some cases, malware can appear to be removed, but then reinstall itself upon restart.

Malware has grown from simply annoying events to software and systems that can take down government computers, capture access information or steal an individual's money. Those who control malware can obtain personal and financial information, cause havoc within commercial industries and financial institutions, and threaten people's livelihoods and personal wealth.

HOW DID ALL THOSE COMPUTERS GET INFECTED?

As a result of the efforts of cybercriminals, software developers have created malware to control other malware and computers. These systems are called botnets and they have command and control (C&C) centers.

Some of the uses of a bot or botnet include:

- Running a distributed denial-of-service (DDoS) attack that can send large streams of User Datagram Protocol (UDP) packets, Internet Control Message Protocol (ICMP) requests or Transmission Control Protocol (TCP) sync requests
- Infecting other computers on a network by taking complete control of a victim machine
- Utilizing and sharing large amounts of bandwidth among hacker communities
- Installing a backdoor to maintain access after an exploit
- Hosting illegal data on a system by making the data part of a file-sharing network to host illegal files (e.g., software, pirated movies)

To infect or compromise a computer system, a cyberattack goes through three phases:

1. **Precompromise**—This phase consists of:
   - Reconnaissance of the target or intended victim
   - Customizing the malware as a weapon to cause damage, obtain data and spy on the target
   - Establishing a means of access
2. **Compromise**—In this phase, the target system is exploited to the hacker's advantage and, subsequently, the malware is installed on vulnerable systems on the network or computer.
3. **Postcompromise**—Once compromised, the attacker establishes a C&C center to direct future cyberactivities and perform actions to further his/her intent.

Cybercriminals not only use malware to gain access to proprietary, sensitive and personal information, but they piggyback on personal activities to learn about targets and their employer organizations. These activities include:

- Capturing online banking access information
- Emailing source and target Internet Protocol (IP) and email lists
- Manipulating online gaming sites to their advantage
- Monitoring bad patching practices
- Studying a target's browsing routines and habits
- Capturing a target's mobile browsing activities
- Studying social networking and messaging sites

To make the problem even worse, time and bad programming practices have allowed cybercriminals to become organized. They know that not everyone has the best security in place, so they prey on the unaware, untrained and unprepared.

CRIMINAL BUSINESS MODELS

According to Trend Micro, cybercriminals can be viewed as having four models (or classifications)[6] (**figure 1**). The commercial model is about selling their services and software. Organized crime is about exploiting the weak and taking their money. The outsourcing model is about obtaining and using criminals with software development skills for their benefit, and the mentors/apprentices model is about those who want to become better at their criminal activities to advance their financial gains.

To develop malware, one may need to incorporate the following tools, resources and services: tool kits (e.g., Structured Query Language [SQL] injection, exploit), bulletproof hosting sites, compromised web sites, bot resellers, cryptography experts, existing malware (i.e., worm, virus, Trojan horse), programmers, information about the target (e.g., IP addresses/ranges, operating system[s], defenses) and testers.

WHO IS RESPONSIBLE FOR INFECTING ALL THESE MACHINES?

Cybercriminals thrive in forums and chat rooms. They not only share their programs and resources, but also brainstorm and share ideas. It is here that they plan cyberattacks, new malware, new approaches to identity theft, phishing schemes, and other ways to make money or gain information. They include specialists who deploy sophisticated malware, design private botnets, design fake antivirus software, poison and hijack web sites, and develop exploit tool kits. Their methods of promotion include Internet job boards, hacking message forums and the Underground Internet Relay Chat (IRC) channel.

Figure 1—Four Models of Cybercriminals

Model	Description	Sample Activities
Commercial	Sell information, tools and resources	• Sell acquired databases (e.g., credit cards) • Sell malware • Sell services to write malware • Conduct DDoS attacks
Organized crime	Work as groups for specific purposes	• Launder stolen property • Participate in malicious activities (e.g., emptying automated teller machine [ATM] accounts, buying gift certificates)
Outsourcing	Hire programmers to join their group, perform malware development or provide services	• Outsource parts of the malware development process • Request DDoS attacks • Use white hat proof of concept to build malware
Mentors/apprentice	Hire more skilled criminals to learn their craft	• Have skilled programmers teach novices

Source: Larry G. Wlosinski. Reprinted with permission. Content based on: Trend Micro, "Cybercriminal Underground Works in Business Models," 10 May 2014, *www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-underground-works-in-business-models*

Cybercriminals use social networks with escrow services. Like normal businesses, they license malware and receive technical support. Botnets can be rented by the hour. There are even infection services and sources for zero-day exploit information. According to Trend Micro, the main underground cybercriminals groups responsible for most malicious activity are located in Russia, China and Brazil.[7]

UNDERGROUND COMPARISON

Figure 2 provides a summary comparison of the malware products and service offerings of Russia, China and Brazil. It is not all-inclusive, but it does provide a high-level view of the underground criminal business offerings.

The overall underground economy that has resulted from cybercriminals' activities is driven by malware authors, organized crime, money-mule networks, third-party enablers, corporate enablers, insiders, and C&C systems and those who control them.

The consequences of their actions on society include:

- Data loss to governments, commercial businesses, financial institutions and individuals

Figure 2—Comparision of Malware Products and Services From Russia, China and Brazil

Service	Russia	China	Brazil
Denial of service (DoS)	• By email • By land line • By text message	• By SYN traffic • By Hypertext Transfer Protocol (HTTP) Get • Domain Name System (DNS) Server • DDoS tool kit rental	
Botnets		• Windows XP bots • Windows Server 2003/2008 bots • By number of bots	
Banking Trojans		• By level of importance • Account stealers	• Selling builder Trojan • Selling source code
Server hosting	• Virtual private network (VPN) with one exit point • With unlimited exit points and traffic	• By proxy addresses per month • VPN by month(s) or year	
Hacking	By target: • Facebook • Gmail • Hotmail • Others		
Cracking		Encrypted files Software with: • Dongle protection • Registration code • User number limit protection	
Email	Spamming by quantity: • Generic (public database) • Short Message Service (SMS)/texting • ICQ • Skype	Spamming by quantity of email addresses	Phishing of popular banks and financial service providers
Social media			Number of likes for: • Facebook • Instagram • Twitter • YouTube

Figure 2—Comparision of Malware Products and Services From Russia, China and Brazil *(cont.)*			
Service	**Russia**	**China**	**Brazil**
Other product offerings	• Trojan horses—Self-replicating software that contains malicious code • Exploits and exploit bundles • Rootkits—Hide existence of malicious processes or programs • Crypters—File encryption and extraction software • Fake documents, e.g., passports • Stolen credit card and other credentials (e.g., VISA, MasterCard, gaming account)	• System exploit kit to fully utilize administrator capabilities • Fake post/comment/view/follower to inflate counts of postings, comments, video views and followers • Fake site, e.g., malicious online game site • Scanned fake document—Passports for China, the US and Canada • Software serial keys for Microsoft, Adobe and AutoCAD products • Traffic monitoring software—IP addresses per day (priced by tiered quantity) • Trojan horse software—Account stealers and bank Trojan tool kits	• Business application account credentials • Credit card credentials • Credit card number generators and testers • Crypters • Social media followers • Online service account credential checkers • Phishing pages • Phone number lists by town or city • Social media followers/views/likes • SMS (texting) spamming software
Other service offerings	• Dedicated server hosting—Servers rented for malicious activity • Proxy server hosting—Used to ensure anonymity • VPN—Encrypted tunnel that can misdirect traffic analysis (e.g., Tor—an encrypted communications tunnel used by cybercriminals) • Pay-per-install (PPI) of select malware—Free applications bundled with adware • Phishing and spamming—Sending quantities of unsolicited messages/email • Malware checking against security software—To test software effectiveness • Social engineering—Manipulating people to give up sensitive information • Brute-force attacks of email and access accounts • System abuse services • Account hacking services • Blackhat search engine optimization (SEO) services • C&C system server activity-related services • Carding (investigation) services • Crypting services (i.e., encryption and decryption)	• Use a compromised host as a malware or spam distributor • Use a compromised host to run complex computing tasks • Cracking of files (e.g., encrypted, RAR, .ZIP, DOC, XLS, EXE) and software (e.g., software key protection, registration code, user limit protections) • Fake document rework • Hacking of forum, email and other account types • Malware checking against various software (including security software) • Programming, development of Remote Access Toolkit (RAT) Trojan • HTTP SOCKS proxy server hosting (by tiered quantity of IP addresses) • RAT rental to function as a system administrator • Trojan attack—One online game per day • VPN server hosting by month(s) or year	• Malware checking against security software services • SMS spamming services • Training services (crypter programming and fraud) • Provide fraud training by selling how-to videos • Provide support via Skype

Figure 2—Comparision of Malware Products and Services From Russia, China and Brazil *(cont.)*			
Service	**Russia**	**China**	**Brazil**
Other service offerings *(cont.)*	• Electronic-payment-related services • Money-laundering and mule-related services • Obfuscation services • PPI services • Programming services • Messaging fraud-related services		
Source: Larry G. Wlosinski. Reprinted with permission. Based on content from: Goncharoc, M; "Russian Underground Revisited," Trend Micro Cybercriminal Underground Economy Series, 2014, *www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf*. Gu, L.; *The Chinese Underground* in 2013, Trend Micro Cybercriminal Underground Economy Series, 2014, *www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-chinese-underground-in-2013.pdf*. Merces, F.; *The Brazilian Underground Market*, Trend Micro Cybercriminal Underground Economy Series, 2014, *www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf*			

- Identity theft (e.g., stolen credit cards, theft under the names of those affected)
- Online fraud (i.e., theft of account holdings by deception)
- Computer extortion (e.g., ransomware)
- Unauthorized access to networks and personal computing devices
- Copyright infringement that affects commercial businesses and government contractors
- DDoS attacks against businesses, government networks and web sites, rendering systems unavailable
- Data destruction, which can affect data availability and business continuity
- Damage to brand names, which can undermine an entire business and put those who work for it out of a job

To summarize, the results of cybercriminals' malicious actions threaten governments, businesses, individuals and the global economy. The resulting cost to society and the world's economy is high.

WHAT ARE THE COSTS TO BUSINESSES, FINANCIAL INSTITUTIONS AND SOCIETY IN GENERAL?

To calculate the costs, one must first quantify the direct and indirect losses and costs of cybersecurity-related defensive actions. The total cost is the sum of the direct losses, indirect losses and defense costs (**figure 3**).

Figure 3 represents just some of the costs. Even with this small list, it is apparent how powerful the underground has become as a threat and how important it is that work is undertaken to at least minimize the effect.

Figure 3—Losses and Costs of Cybersecurity-related Defensive Actions		
Direct Losses	**Indirect Losses**	**Defensive Action Costs**
• Money withdrawn from victim accounts • Time and effort to reset account credentials (for both banks and consumers) • Distress suffered by victims • Secondary costs of overdrawn accounts, e.g., deferred purchases, inconvenience of not having access to money when needed	• Lost attention and bandwidth caused by spam messages • Missed business opportunity for banks to communicate with their customers by email • Reduced uptake by citizens of electronic services as a result of lessened trust in online transactions • Efforts to clean up all types of computers infected with the malware	• Loss of trust in online banking, leading to reduced revenues from electronic transaction fees and higher costs for maintaining branch staff and check-clearing facilities • Security products such as spam filters, antivirus and browser extensions to protect users • Security services provided to individuals, such as training and awareness measures • Security services provided to industry to protect against web site takedowns • Fraud detection, tracking and recuperation efforts • Law enforcement • Inconvenience of missing an important message falsely classified as spam
Source: Larry G. Wlosinski. Reprinted with permission.		

CAN IT BE STOPPED?

The threat cannot be stopped, but the risk can be assessed, decisions on how to handle the threat made and countermeasures implemented. When determining the risk, it needs to be decided if each risk factor can be accepted, avoided/removed, minimized (plan for remediation), researched for a solution or transferred (e.g., insurance).

> "Stopping all threat sources is a monumental task that requires the cooperation of many countries and organizations."

The problem with the underground threat is not at the organization's enterprise or system level; rather, it is a world threat. While there are three main sources of underground threat, as described previously, there are others who are not as organized but perform similar, if not the same, malicious actions. Stopping all threat sources is a monumental task that requires the cooperation of many countries and organizations.

COUNTERMEASURES

In addition to the IT security defenses and best practices already in place, the following countermeasures could be implemented at the global level:

1. **Reinvent Internet defenses to block malicious activity coming from outside the country.** The reason for this is that some countries will not allow for extradition or do not have the will/capability to stop criminal organizations from conducting cybertraffic. To accomplish this, network monitors and reporting programs need to be implemented at each country's entry point.
2. **Add sensors not only to monitor critical networks and systems but also to track places of origin.** This is needed to better locate the source and minimize the effect of address spoofing. Sensors should be able to verify source addresses before they are permitted to spread or cause DDoS and other malware attacks.
3. **Develop defensive software systems.** That is, applications should be self-monitoring such that if someone attempts changes without permission, the system would send an alert and not allow it. The system would also have the ability to correct itself by reverting back to its baseline.
4. **Develop nonstandard systems.** Developers should be able to create applications with the freedom to design how they see fit. Presently, the programming approach is according to proven best practices. What if programmers could assign code to dynamic memory locations, place files in random locations and create systems that appear random (i.e., at the programmers' choosing) to make it more difficult for cybercriminals? Is this not what cybercriminals are doing? Perhaps learning from virus writers is a means of helping to avoid malicious activities.
5. **Create software viruses that can attach themselves to a malicious virus and remove the malware that was installed.** This would require understanding the malicious virus and setting a trap where the cleaning virus would attach to the bad virus.
6. **Develop an inventory system that would document what it discovers.** It would be a combination of a vulnerability scanner and a patch management system, but it would produce reports that define the system boundary and provide the basis for a system assessment. The system would be designed so that additional information could be added (e.g., location, serial number, purpose) and custom reports created.
7. **Have those who use encryption employ something that cannot be broken.** This concept suggests that each organization develop an internal proprietary encryption formula. Examples of proprietary encryption could be a simple enhancement to normal encryption such as adding to it, multiplying it, applying some polynomial to it or employing some mathematical formula to it that works for the single organization only.
8. **Encrypt sensitive information at the field level.** If the information is a personal identifier (e.g., social security number) or personally identifiable information (PII), at least encrypt these while at rest or in transit. This may require new retrieval and display routines, but the data are important enough to implement more secure measures for customers.

Are there other ways to reduce the threat and the level of risk? Here are some other things to consider:

- **Training**—From where are criminal programmers coming? Are international students trained in how to compromise specific systems? Where are criminally inclined programmers being taught? Is it possible that universities

discard these programmers and developers if they are not good enough? What circumstances are pushing them to find an alternative and, possibly, a more lucrative job in the criminal world?

- **Blackmail**—Are those who become part of the cybercriminal world being forced to work for criminal enterprises for fear of reprisals to them and/or their family and friends? Do they have a way out?
- **Punishment**—Are more prisons needed? Are the laws (in all countries) sufficient to be a deterrent? Can smaller countries work together to share the burden of enforcement?
- **Location**—How are criminals who hide behind distance and anonymity reached? How can other governments be convinced that the malicious cyber-related actions of their people affect the world economy and they need to do the responsible thing?
- **Laws**—How can countries be convinced that their laws need to be adjusted to handle cyberactivities? New laws are needed for the cybercriminal sector and there need to be new rules of interconnectivity.
- **Web security**—How is the problem of a web site with weak security addressed? This refers not only to web sites that have been abandoned, but also to those owned by small businesses that have created company web sites but do not monitor them. These problems can be attributed to weak software patching programs, nonexistent malware scanning and removal, and configuration weaknesses. Should web sites have an automatic retirement/closure capability by default?
- **Reactive measures**—Should the good guys hack and disrupt the bad guys' web sites? Should someone teach them right from wrong? Should there be countermeasures and repercussions against those who work to harm society and the governments of all countries?
- **Businesses**—Should businesses have an incentive to monitor their employees' computers for malware? Business incentives could include tax credits and reduced credit rates (but this would require monitoring and enforcement).
- **Accountability**—Do the countries that harbor cybercriminals need accountability for the malicious cyberactivity they allow? How can transactions be tracked in places that do not capture or report malicious or suspicious activity? Should countries that do not follow honorable practices be removed from the global economic enterprise?

CONCLUSION

Everyone must be encouraged to work together to develop solutions. The threat is so large that entire economies are affected. This, in turn, affects banks (i.e., those who lend money, pay interest on accounts and pay for malicious intrusions), employing organizations and individual prosperity.

Governments, financial institutions, software vendors, system developers and users must work together to take back the economy or things will continue to get worse. Current cyber-related controls and strategies are not acceptable—cybercriminals are getting rich from the hard work of others and the lack of a united cybersecurity front on everyone's part.

ENDNOTES

[1] Symantec, *Internet Security Threat Report (ISTR) 2014*, 2014, *www.symantec.com/security_response/publications/threatreport.jsp?&om_sem_cid=biz_sem_s186232479297029|pcrid|51284528675|pmt|b|plc||pdv|c*

[2] Symantec, *Internet Security Threat Report (ISTR) 2015*, vol. 20, 2015, *www.symantec.com/security_response/publications/threatreport.jsp*

[3] Norton, *2012 Norton Cybercrime Report*, 2012, *http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf*

[4] Trustwave, *Uncovered: Targets, Methods and Motivations of Cybercrime*, 2014 Trustwave Global Security Report, 2014, *www2.trustwave.com/GSR2014.html?utm_source=redirect&utm_medium=web&utm_campaign=GSR2014*

[5] McAfee, *McAfee Labs Threats Report June 2014*, 2014, *www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf*

[6] Trend Micro, "Cybercriminal Underground Works in Business Models," 10 May 2014, *www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cybercriminal-underground-works-in-business-models.* The report includes lists of malware products available in Russia, China and Brazil.

[7] *Ibid*.

Cyberinsurance—The Challenge of Transferring Failure in a Digital, Globalized World

Jeimy J. Cano, Ph.D., COBIT Foundation, CFE, is a research member of the Information Technology, Telecommunications, Electronic Commerce Studies Group (GECTI) of the Law School and a distinguished professor at Universidad de los Andes, Colombia.

Disponible también en español *(www.isaca.org/currentissue)*

As organizations enter the international context and leverage their IT operations, their visibility increases, which, in turn, increases exposure to threats with a global scope. Since information is one of the most valuable assets of an interconnected and dynamic reality, it becomes necessary to understand the requirements and responsibilities that companies acquire when operating in a scenario in which the value-generation model, reputation and relationships with stakeholders are at risk.

In this situation, organizations, as part of their due diligence, progress in the exercise of their risk management and undertake it with the required seriousness. Risk management establishes the general framework for the activities and decisions enterprises make for progressing amid instabilities and troubled times in the business sector. A risk management strategy should take international implications into consideration, as these affect the prospects and projections of their boards of directors (BoDs).

Reports of information security breaches and unauthorized actions on organizations' IT infrastructures have increased. This demonstrates a trend of an increased number of people or groups acting with the goal of drawing attention to particular aspects of the reality of a country or region; these can be financially motivated as well. Unconventional breaches that stress and weaken organizations' technological facilities are used, revealing the need for greater attention to the security and control of operations.

With this understanding, the actions and strategies of companies to make their digital activity more resistant become visible to cyberattackers. Unauthorized third parties seek not only to create fear, uncertainty and doubt in business executives, but also to obtain control of key information, which may be used for commercial purposes, extortion, intelligence or military action. As a result, corporations become strategic targets of national and regional interests.

And, in turn, a new stage of strategic risk management within companies has begun—one in which the composition of a global, digital and political view outlines the reality of cyberrisk.

The term "cyber" requires understanding that organizations not only represent the interests of the company in a business community but are also incorporated in the dynamics of globalization, within which business interests are manifested. In a globalized world, organizations may be affected by countries that contribute to influencing and defining the geopolitical scenario of all nations. Enterprises also obtain a fluidity of movement due to the high interconnectivity and intensive use of information and communication technologies (ICTs) that allow transactions and relationships based on a digital economy that serves emerging communities around the world.

Cyberinsurance is a way to account for cyberrisk and considers the new possible business responsibilities arising from operating in an international context. Presenting cyberinsurance as a coverage option is not designed to compensate for organizations' negligence of fulfilling the duty of protecting their information and technological infrastructure.

BASIC CONCEPTS OF INSURANCE

Insurance generally operates as a compensation strategy for specific situations involving third-party interests. In this sense, a contract or agreement between the parties—the insurer and the insured—is established. Aspects such as insurable risk, the conditional obligation of the insurer and the premium are reviewed to establish the framework of action and the required guarantee, which is based on the principle of good faith that prevails in this relationship.

Do you have something to say about this article?

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

Go directly to the article:

Insurable risk is "a fortuitous event, that due to being sudden and unforeseen, does not have, in its origin and its development, any relationship with conscious human action, whether the consequence is voluntary or not."[1] As can be seen, that which is insured is a condition of exception not subject to deliberate actions by individuals and protects the insured party against the consequences of such events.

It is important to note that there is uninsurable risk associated with fraud (i.e., a voluntary act, intentionally harmful conduct). Certain events (i.e., events that will certainly occur), impossible events (i.e., events that will certainly never occur), past events (i.e., events that occurred and were beyond the initially established scope), events of unique provision of the insured party, and events related to criminal sanctions of an economic nature are uninsurable. These events have no effect on the coverages or payments made, since they are not insured.

The insurable interest shall be understood from the point of view of damage insurance as an economic relationship that links the insured party with an object. While the insurable interest is the subject of insurance contracts, it is necessary to remember that "several insurable interests can converge on the same object on behalf of the same person or different persons...with the condition that the compensation, if the event does indeed occur, may not exceed the total value of the object at the time of the incident."[2]

The conditional obligation of the insurer is applicable when the incident occurs (i.e., when the required condition is fulfilled), at which time the beneficiary may proceed to exercise his/her right that the insurer pay the agreed-upon amount. Conditionality provides two key elements: enforceability and delay. Enforceability indicates when the obligation is no longer pending (the instant when the incident occurs), and this depends on the terms of the agreed compensation. In addition, delay (the preexistence of a formal claim in compliance with the basic evidentiary burdens, the existence of the incident and the amount) indicates that if the claim has not been answered by the insurer within one month, it enters default along with its purposes, interests or compensation for damages.[3]

Finally the premium, as an essential element of an insurance contract, is the onerous element that transfers the risk to the insurer. Technically, it is the result of a rate, expressed in percentage terms, on the insured value. The premium involves four key factors:[4]

- The actual cost of the transfer of risk (risk premium—statistical analysis of the probability of occurrence)
- The cost of administration (includes the cost of reinsurance)
- The cost of intermediation (payment of commission to intermediaries)
- The expected profit

These fundamental concepts of insurance are the basis for reviewing the new conditions of companies' responsibility in the context of cybersecurity.

ARISING RESPONSIBILITIES OF COMPANIES IN THE 21ST CENTURY

As enterprises compete in highly digitized scenarios and with greater involvement of third parties in their operations, the most valuable information of the enterprise depends on correct processing by users who have access to it. This calls for a series of security and control practices that must be validated and guaranteed by each of the parties in the application of the information life cycle.

> "The most valuable information of the enterprise depends on correct processing by users who have access to it."

If the preceding is correct, the risk of loss and/or leakage of information becomes a critical concern for organizations, given that the occurrence of this risk exposes organizations to possible loss of reputation, customers, competitive advantage and markets, in addition to fines, reparatory actions and regulatory sanctions. These entail costs and compensations that, without the proper preparation and prevention, may compromise the viability of the company in the short and long term.[5]

Information has become the new natural resource of the 21st century as it facilitates a world in constant movement, generally shared among different actors. It carries with it risk that must be identified and addressed for the purpose of driving preventive actions that anticipate potential negative impacts due to improper processing. This implies expressing

due diligence and guaranteeing a minimum standard, which should involve the duty of care of individuals, predictability in adverse situations in the processing of information, a standard of due care in information security and a set of reasonable precautions that demonstrate a proactive attitude toward damages that may arise.[6]

Many of the causes of information security breaches are unexpected; however, some of the most common ones identified in the normal operation of companies are:[7]

- Lost or stolen laptops or mobile devices
- Unauthorized transfer of data to universal serial bus (USB) devices
- Inappropriate categorization or classification of sensitive information
- Theft of data by employees or third parties
- Printing and copying of sensitive data by employees
- Insufficient response to intrusions or security breaches
- Unintentional transmission of sensitive data
- Use of weak and/or known passwords
- Conversations in public spaces regarding sensitive data
- Unauthorized monitoring of communications

Due to these causes, a new series of corporate responsibilities is necessary regarding the processing of information associated with computer processes and interactions (whether operated by the company or third parties) to mobilize the value-generation model of the company. This means understanding that in the race for cost efficiency, ICT will play a fundamental role, since by increasing the level of automation, enterprises will become more agile and efficient. However, this dependence will open organizations to previously identified vulnerabilities and security and control failures.

In risk management, there are different approaches to risk: accept, mitigate and transfer. Organizations understand the sensitivity of this subject relative to the protection of their interests and keep it in mind during relevant activities. Consequently, organizations define processing plans that include human, procedural and technological aspects that seek to close the possible identified breaches and reduce the analyzed exposure level. Enterprises also define insurance as a form of risk transfer that requires, from the insured party, systematic and effective practices regarding data protection.

Nevertheless, the impacts of information security incidents—some identified and others emerging—may not be included in the risk analysis. The consequences of these incidents may have onerous and compensatory implications that compromise the best predictions of companies in their strategies for mitigation or transfer of such risk. Therefore, the digital life of enterprises requires reviewing risk transfer proposals to build a more accurate view of this reality and to overcome traditional insurance conditions in this area, such as errors or omissions in the provision of technology services, violation of intellectual property rights, losses due to theft through transactional electronic systems, and computer crime.[8]

UNDERSTANDING CYBERINSURANCE

To date, insurance policies, defined as documents containing the insurance contract,[9] have multiple classifications and names for specifically establishing their scope and limitations. In the case of cyberinsurance, policies for identification of risk classify it as "all-risk" and "named-risk." While the former is directed at covering the insurable interest of any risk other than those excluded by contract or those that are legally insured by express agreement (agreed with the insurer), the latter intends to cover the insurable interest of the defined risk.[10]

This traditional system, from the standpoint of the insured party, takes on the customary difficulties of understanding the contractual identification of risk associated with a basic definition of it and one or more exclusion clauses.[11] Exclusion clauses are defined as circumstances in which the risk, as it is defined, is not covered by option of the insurer. In this context, cyberinsurance is at a crossroads between the insurer, the proposed coverages and the defined exclusions, addressing the needs, demands and requirements of the insured party. This is because the complexity of cyberrisk involves an understanding of human procedural, technological and legal variables in which the interaction provides a scenario of consequences that depends on each particular case.

However, the coverage of cyberinsurance contains aspects similar to all-risk insurance policies such as:[12]

- Overall responsibility for crime through the Internet
- Property (data are not considered property)
- Errors and omissions
- Professional liability
- Liability of directors and officials
- Employment practices liability (actions of employees)
- Business interruption
- Extortion and kidnapping
- Personnel group liability (key personnel)

- Life coverage of key personnel
- Media liability coverage
- Fidelity and crime liability
- Network security coverage
- Intellectual property
- Patent insurance
- Workplace violence coverage

The coverages established by the main cyberinsurance brokers are associated with property and theft, as well as liability.[13] **Figure 1** provides a summary of typical coverage.

Figure 1—Coverages Offered By the Largest Cyberinsurance Brokers

	Coverage
Property and theft	Destruction of information or software
	Recovery from viruses or other malicious codes
	Business interruption
	Denial of service
	Information theft
	Cybernetic extortion
	Losses due to terrorist acts
Liability	Network security
	Harm to electronic media or contents
	Private confidentiality breach

Source: Garcia, K.; "Propuesta de póliza de seguro para el ciber-riesgo en Guatemala," undergraduate thesis, Universidad de San Carlos de Guatemala, 2009, p. 70, *http://biblioteca.usac.edu.gt/tesis/08/08_0420_CS.pdf*

Recent cyberinsurance studies reflect a substantial evolution of the analyzed coverages, which reflects a greater understanding of the complexity exhibited by cyberrisk. A recent study concludes that cyberattacks can be seen as one of the most serious economic and national security challenges faced by governments and organizations globally.[14] With this understanding, the study details the risk factors associated with this challenge:

- Legal liability
- Information security breaches
- Privacy breaches
- Cybertheft
- Cyberespionage
- Cyberextortion
- Cyberterrorism
- Loss of profit
- Recovery of costs
- Reputational damage
- Business continuity/supply chain disruptions
- Cyberthreats to the nation's critical infrastructure

Based on that risk, the study outlines some specific coverage, including aspects such as:

- Data privacy
- Breaches in regulations, fines and penalties
- Interruption of business networks
- Damage to data and cyberextortion
- Crisis management and response to identity theft (includes costs of forensic investigations)

In addition, research specialized in these matters indicates that the insurance market presents an asymmetry of information between the insured party and the insurer, particularly focusing on potential primary losses (e.g., direct loss of information or data, suspension of operations) and less on secondary losses (e.g., indirect loss, decrease of reputation, good name, consumer confidence, strategic strength, loss of customers). When incidents occur, the claims processes will be estimated by the economic valuations represented in the company's operating conditions (primary losses), leaving secondary losses to subjective valuations based on experiences and comparisons with equivalent processes. This creates an imbalance of protection that sometimes favors the insurer and other times the insured party.[15, 16]

> "Cyberinsurance is emerging to prevent the extent and spread of an incident and bear the payment for repair, replacement or reconstruction of the goods affected by the occurrence of the cyberrisk."

It can be concluded that cyberinsurance is emerging to prevent the extent and spread of an incident and bear the payment for repair, replacement or reconstruction of the goods affected by the occurrence of the cyberrisk.

The negotiation implicit to this type of policy is associated with exclusions. Exclusions are circumstances or events that are excluded from the insured coverage and are clearly stated in the insurance policy. These exceptions are usually associated with the previously presented noninsurable risk, including, for example, the obsolescence of the insured asset; inexcusable negligence or defective execution of the

maintenance necessary for the proper operation of the insured interest; and damages to the insured party or third parties as the result of a commercial, industrial or professional activity other than that stated in the policy.[17]

Exclusions respond to the requirement for management to guarantee the insured interest, which in the case of cyberrisk implies a systemic view of the risk in the context of the organization. That is, this view contains an understanding of the relationships of the organization from its business position, its relationships with communities and stakeholders, and the government and management of information technology, in order to understand the interconnectivity that arises in this practice.

Likewise, information security plays a fundamental role in cyberinsurance because the insurer demands an understanding of the information as a strategic asset that serves as the basis for the company's internal and external relationships, as well as the shared responsibility for its management and control with the involved third parties. Third parties also acquire the category of coresponsible parties in this scenario and must also commit to good practices, meaning they will cooperate in preventing cyberrisk by the contracting company.

CONCLUSIONS

The BoDs of organizations must include cyberrisk considerations in their review of the strategic risk of companies. To ignore this interpretation of the current business dynamics (the consequences of which are evident in multiple international cases such as those of Target, JPMorgan Chase, Sony and Office Depot, among others) is to anticipate crisis scenarios that are generally unknown and whose processing requires specialized and coordinated actions to mitigate their harmful effects.

In this practice, board members must not only become familiar with these new realities,[18] generally manifested in large failures and security breaches, but also understand the levels of preparation that the organization has regarding similar situations. It is necessary to establish the required preventive mechanisms and extended protection covering aspects that may be relevant and that current actions only cover partially.

Cyberinsurance appears as an option to consider every time security and control practices are required for companies to limit the effects of massive and coordinated attacks—some for extortionary purposes or cyberespionage—that can compromise the strategic information assets of the company, the identity of their personnel or business strategies, and that can even affect a nation's critical infrastructure operations. Along these lines, cyberinsurance comprises a critical interpretation of the intangible assets of the company in the scenario of an operation that is digitized and deeply integrated in its dynamics and has global visibility.

Cyberinsurance introduces an understanding of relationships in the digital ecosystem in order to comprehend the thresholds of permissible loss of value. This promotes consideration of the object that defines the maximum loss estimated by an organization, given a defined resilience profile that comprises a series of company activities.

The greater the understanding of the organizational culture of information security, the availability of recovery and continuity capabilities, the knowledge of emerging vulnerabilities of the business, and the characterization of the possible attackers, the better the company's preparation and response to cyberrisk will be.

The cyberinsurance world will continue to evolve according to the challenges and demands of the market and the results of introducing disruptive and nontraditional technologies. It is necessary to know the impacts of the inevitability of failure to understand the coverages and exclusions being proposed by insurance contracts, while insurance companies are beginning to accompany organizations, acting as vigilant entities for information technology, communications management and information processing.

ENDNOTES

1 Ordonez, A.; *Elementos esenciales, partes y carácter indemnizatorio del contrato*, Insurance law lesson no. 2, Universidad Externado de Colombia, Bogota, Colombia, 2002, p. 10

2 *Ibid*., p. 32-33

3 *Ibid*., p. 48-51

4 *Ibid*., p. 42

5 Ernst & Young, *Data Loss Prevention. Keep Your Sensitive Data Out of the Public Domain. Insights on Governance, Risk and Compliance*, October 2011, *www.ey.com/Publication/vwLUAssets/EY_Data_Loss_Prevention/$FILE/EY_Data_Loss_Prevention.pdf*

6 Triump, I.; "Confronting the Legal Liabilities of IT Systems," *EDPACS: The EDP Audit, Control, and Security Newsletter*, 46(2), 2012, p. 11-16

[7] *Op cit* Ernst & Young, p. 6

[8] Garcia, K.; "Propuesta de póliza de seguro para el ciber-riesgo en Guatemala," undergraduate thesis, Universidad de San Carlos de Guatemala, 2009, *http://biblioteca.usac.edu.gt/tesis/08/08_0420_CS.pdf*

[9] Ramirez, E.; Specialization in Insurance course, Universidad Externado de Colombia

[10] *Ibid*.

[11] Ordonez, A.; *Cuestiones generales y caracteres del contrato*, Insurance law lesson No. 1, Universidad Externado de Colombia, Bogota, Colombia, 2001

[12] Drouin, D.; "Cyber Risk Insurance: A Discourse and Preparatory Guide," GIAC Security Essentials Certification, 2004, *www.sans.org/reading-room/whitepapers/legal/cyber-risk-insurance-1412*

[13] *Op cit* Garcia

[14] Carpenter, Guy; *Ahead of the Curve: Understanding Emerging Risk*, 2014, *www.guycarp.com/content/dam/guycarp/en/documents/dynamic-content/AheadoftheCurve-UnderstandingEmergingRisks.pdf*

[15] Ordonez, A.; *Las obligaciones y cargas de las partes en el contrato de seguro y la inoperancia del contrato de seguro*, Insurance law lesson No. 3, Universidad Externado de Colombia, Bogota, Colombia, 2004

[16] Bandyopadhyay, T.; V. Mookerjee; R. Rao; "Why IT Managers Don't Go for Cyber-insurance Products," *Communications of ACM*, 52(11), November 2009, p. 68-73

[17] Generali Seguros; "Generali negocio seguro. Condiciones generales y condiciones generales específicas," *http://62.97.131.36/rep_documentos/phogar/GENERALI-CCGG-COMERCIOS.pdf*

[18] Rai, S.; *Cybersecurity: What the Board of Directors Needs to Ask*, ISACA-IIA, 2014, *www.theiia.org/bookstore/downloads/freetoall/5036.dl_GRC%20Cyber%20Security%20Research%20Report.pdf*

Accelerating Access Management to the Speed of Hacks

Chris Sullivan is vice president of advanced solutions at Courion. He is responsible for developing and bringing new products and solutions to market as well as cultivating and innovating new ideas that effectively address the industry's ongoing challenges. Previously, Chris has been vice president of EMEA Operations, Advanced Solutions, Customer Solutions and Professional Services. Chris also serves as chairman of the Access Risk Benchmarking Committee for ISACA and is a frequent speaker at industry conferences including European Identity Conference, Gartner Catalyst Conference, MIT International Science and Technology Initiatives (MISTI), IT GRC Forum and the ISACA ISRM conference.

Also available in Korean
한국어로도 가능

Organizations grant network access nearly every minute of every day. Hackers frequently try to get inside networks using co-opted access credentials. Yet most IT departments still review access privileges only quarterly or semiannually.

Even organizations that review access privileges monthly, which is diligent by today's standards, are not keeping up with hackers who are on the job and working around the clock. It is easy for network security staff, who toil daily to keep intruders out of systems, to lose track of the fact that they are under constant siege. Certifying access on even a monthly basis leaves large open periods of time for intruders or nefarious insiders to sneak in, do their damage and cover their tracks before the next certification comes along.

The attack that penetrated an Anthem database of 80 million customers and employees is a classic example. The breach occurred in May 2014 but was not discovered until early 2015. In many, if not most, data breaches, a delay such as this is the case. According to the Verizon 2015 *Data Breach Investigations Report* (DBIR), 60 percent of compromises took only seconds or minutes.[1] Nearly 50 percent of those tested in the investigation opened emails and click on phishing links within the first hour, according to the report, which surveyed 70 global organizations from 61 countries.

By comparison, 75 percent of detection took weeks, and it was not always because of anything the company did. "We need to close the gap between sharing speed and attack speed," the report concluded.

A similar report showed that attackers were present on victim networks for an average of 229 days before they were discovered.[2] Realities like these are a clear call for a new approach to identity and access management (IAM).

FRAGMENTED SECURITY

The need for open access fuels the big data crush that is overwhelming today's access certification processes. Consumer access models are firmly entrenched in the business world. Employees, contractors and vendors expect access through every online and mobile channel: web sites, direct logins and mobile applications. With every new access point comes another opportunity for intruders to exploit their favorite vehicle into companies' vital assets: legitimate network access credentials.

Data thieves are getting into networks by using the same tactics they have been using for years—phishing, malware attachments, and stolen or compromised credentials—to infiltrate networks. New access options have made those tactics even easier to use and more effective.

Email phishing, for example, is easier now because legitimate email addresses are posted in more locations. Mobile apps may not have gone through the usual security vetting, yet they provide direct network access. Once inside with a legitimate login identity or email address, an intruder can request access to vital systems. Or, they can use malware or fake web sites to steal manager credentials, give themselves access and then cover their tracks once they have taken what they want.

With so many more doors opening to the network, most organizations are under almost constant attack from the inside. Effectively defending against intruders or malicious insiders means eliminating orphan accounts, pinpointing unusual behavior and identifying privileges that do not match an employee's role. That requires a new microcertification model of network management.

Microcertifications continually validate access privileges against business policies when they are triggered by questionable activities and events. If violations are found, notifications immediately go to the relevant managers for remedial action. Managers react only to anomalies, not constantly recertify compliant user accounts.

The problem with microcertifications is that most companies today do not have an enterprisewide IT security framework or the technology tools required to support them. Solutions common in IT environments today automate compliance reviews, but provide only periodic or interval audit checks. That leaves large windows of vulnerability between 90-day and even 30-day review cycles. Reviewing access privileges more frequently is prohibitively expensive, largely due to the manual processes dominant today and almost impossible logistically. Certifying all of their reports every few days would take managers so much time that they would not be able to do much else. The pace of business productivity would be severely reduced.

Intelligence, in the form of embedded data analytics optimized for identity and access management, can reduce the number of certifications that managers must perform by reporting only anomalies that require a sign-off. In an intelligent system, managers do not have to compare and contrast access privileges to determine if there are high-risk combinations or if a privilege is outside an employee's role. The system identifies the risk and calculates how much accepting the exception will increase the employee's risk rating. The manager is left only with the decision of whether the exception is necessary and the risk is warranted.

> "Security is a strategic priority, and COBIT enables organizations to translate it to frontline action."

COHESION THROUGH COBIT

Implementing microcertifications requires two elements: a unified IT security infrastructure and big data analysis tools. The COBIT® 5 governance map, developed by ISACA, addresses the current patchwork nature of most identity and access management systems.

COBIT® integrates security into a cohesive framework that encompasses risk, resource and performance management, in addition to business considerations (e.g., strategic alignment of IT with business goals). With the risk posed by IT breaches so significant, creating this connection between strategic goals and IT is essential. Security is a strategic priority, and COBIT enables organizations to translate it to frontline action.

COBIT provides the common language for defining goals and objectives essential for executing strategic goals. It also defines objectives and metrics for IT security. Metrics serve as the parameters for reconciling access management functions into a cohesive process for identifying the patterns of behavior that can expose an intruder.

COBIT addresses the fragmentation that exists in much of IAM. Access management vendors have developed a broad array of tools to automate tasks. Generating intelligence to detect intruders, however, is still left to manual processes and to management tools without native data intelligence.

"Generating the data to feed effectiveness metrics is not easy," says Gartner analyst Brian Iverson. "Most products in the IAM space do not yet possess a mature understanding of the basic process elements that are needed to demonstrate control over user access. Furthermore, such products also vary in the robustness of their support for analytics, reporting and dashboards. Even if there is a desire to use a product's internal dashboards, there may be a need to process data externally to produce some desired metrics."[4]

AUTOMATION GAP

The lack of intelligent, automated data analysis tools in most corporate IT environments forces companies to make do with manual access management. IT teams present reports to each business manager with lists of permissions granted to each of their direct reports. Managers attest to whether the permissions are appropriate or should be modified. System owners do the same. That means manually parsing large data sets that multiply exponentially with each level of detail.

Usually, IT staff extracts user data from databases and applications into unorganized flat files. Another set of IT staff, usually the security team, has to reconcile those masses of data into formats that can be dissected by spreadsheet applications. The difficulty and expense of this process are primary contributors to the higher risk of credentials being used to improperly access key systems. It is simply too laborious a process to go through more than a few times per year. The problem is even more acute for organizations that want to detect unusual usage patterns that could indicate an intruder.

A manager with 10 direct reports can be taken as an example. Each direct report has access to at least 10 systems. Within those 10 systems, each employee could have dozens of entitlements. The team has to parse that much data for each manager, and the manager must attest to each data point. Some managers might require a specific breakdown.

Shifting that scenario to the company level illustrates how data volumes quickly multiply to outstrip manual analysis. A company with 10,000 employees, each with access to 10 applications, has 100,000 accounts. Take a conservative view and assume the users log in twice per day. That creates 200,000 login activity records per day. One month generates 4 million login activity records.

To detect improper usage, a company must also know what employees are doing within each application. Assuming those same 10,000 workers access 50 data assets per day, there would be 500,000 activity records per day and 10 million per month. With the login records, there are 14 million data elements to analyze per month.

Manually analyzing entire data sets that are that large is impossible. Without automation, IT organizations are left to monitor only select risk areas, leaving many gaps in the security fabric for intruders to exploit.

THE BIG DATA APPROACH

The development of big data management and automated analysis tools makes it possible to close those gaps by constantly analyzing tens of millions of data points to detect suspicious activity. As recently as two years ago, these tools did not exist for IT, even though almost identical tools were common in areas such as sales, marketing and customer service. Big data analysis tools continue to gain a foothold in IT.

Massachusetts (USA)-based health care provider Harvard Pilgrim is among the early adopters to apply identity analytics and intelligence to IAM. With more than 1.2 million subscribers, the company manages tens of millions of records per month. The company implemented a solution to monitor all significant risk areas. Among the key areas the IT staff focused on were detecting unused accounts and closely monitoring privileged accounts that had the ability to change systems and perform maintenance.

Harvard Pilgrim's intelligent IAM solution enables managers to report accounts that have not been accessed in a set amount of time so they can be deactivated before a hacker can exploit them. It also regularly analyzes privileged accounts to determine what access they have as compared to what access they should have. The analysis is automated to run constantly and detect any behavior outside of norms that are determined by managers and expressed in the access management solution. Harvard Pilgrim has used that intelligence to reduce the number of privileged access accounts and eliminate those with unnecessary access.

In another example, Miami (Florida, USA) Children's Hospital implemented the same approach to constantly scan its access environment. Analyzing millions of data points, the automated scan revealed hundreds of orphaned accounts and several user groups with no members. Each represented a data theft risk that would have been difficult, if not impossible, to detect until after damage had been done.

In both cases, adding identity analytics to the IAM equation enabled IT and business managers to instantly identify high-risk individuals and groups by answering questions such as:

- Are there domain administrator accounts whose passwords have been changed?
- Which nonsales systems have sales people accessed?
- Is anyone accessing patient medical information without a genuine need to know?
- Which accounts with at least five entitlements have not been used in more than 30 days?
- Does this account have a suspicious number of privileged entitlements?
- Should part-time employees receive all the access rights they are routinely granted?
- Do contractors continue to access resources after their projects end?
- Are system administrators routinely assigned rights they do not need to perform their jobs?
- Does this business unit have an abnormal number of accounts with unnecessary entitlements?

There are no technical restrictions preventing companies from taking this approach. In the consumer realm, Amazon.com has been doing something very similar for years to track shopping habits. It knows what product a customer views and when they view it so that the company can offer promotions and incentives to purchase. The same practice occurs with credit card companies. They can detect almost instantly when a purchase looks out of character, alert the customer and cancel the card within minutes of detection to prevent losses.

Similarly, there are already IAM solutions on the market that eliminate manual data extraction by working through application programming interfaces (APIs) or scripting. They automatically cleanse the data for analysis and automatically apply analytical intelligence to answer the vital questions for determining who is doing what on the network and when.

TOWARD INTELLIGENT ACCESS MANAGEMENT

The pace of business today demands an increasing degree of open access to IT resources. With that access comes greater risk of data theft or corruption through intruders who use legitimate access points, credentials and user accounts to attack sensitive data sources.

Constantly monitoring access privileges to identify improper use of those resources to remediate risk is nearly impossible with the access management solutions dominant in most corporate IT environments today. Built around the native access management and security tools integrated into key applications and databases, IT security infrastructures are fragmented. This fragmentation contributes to a reliance on manual processes to analyze security data and certify access privileges. Slow and expensive, they cannot scale to accommodate the enormous data volumes generated by today's consumer-inspired open-access environments.

The same consumer models, however, also contain the answer to the problem. Big data analytical tools, comparable to those used in consumer applications, provide the capacity to constantly, quickly and economically analyze access data to support a microcertification access management model. Microcertification systems identify unusual behaviors and ask business managers to react only when there is a potentially risky situation. This allows for constant diligence without bogging managers down with excessive, redundant, unnecessary certifications.

> "IT organizations must adopt automation and intelligence strategies if they hope to stay ahead of hackers."

IT organizations must adopt automation and intelligence strategies if they hope to stay ahead of hackers. Otherwise, as the demand for wider access grows and opens more doors into the network, companies will continue to measure their response times in weeks while data thieves attack in minutes, disappear in seconds and cause years' worth of damage.

ENDNOTES

[1] Verizon, 2015 *Data Breach Investigation Report, www.verizonenterprise.com/DBIR/2015/*

[2] Mandiant, *M-Trends 2014: Beyond the Breach, http://connect.mandiant.com/m-trends_2014*

[3] Frisken, John; "Leveraging COBIT to Implement Information Security," *COBIT Focus*, ISACA®, USA, 4 May 2015, *www.isaca.org/cobitfocus,* figure 2.

[4] Iverson, B.; *Demonstrate Control Over User Access With IAM Effectiveness Metrics*, Gartner, 5 February 2015, *www.gartner.com/doc/2978217/demonstrate-control-user-access-iam*

Preparing for a Cyberattack by Extending BCM Into the C-suite

Gary Lieberman, Ph.D., CISSP, is director of enterprise computing and information security for a global investment bank where he has designed a highly available and secure global infrastructure supporting all critical business functions. He is responsible for and oversees all information security functions within the global infrastructure. He has published numerous research papers and journal articles covering topics such as application-to-application credential management, vulnerability scan and audit finding quantification, and security considerations relating to segregation of duties. Lieberman is also an adjunct professor in cybersecurity, network security, database design and disaster recovery at St. Leo University (Florida, USA) and Caldwell University (New Jersey, USA). He can be reached at *gary@lieberman.us.*

In 2001, a survey of 250 US companies found that three in 10 companies had formal business continuity/disaster recovery (BC/DR) programs in place.[1] That has changed. Since then, nearly all regulatory requirements and risk frameworks have been enhanced and expanded to require formal BC/DR programs that address the ever-growing threat environment.[2] Events such as the 11 September 2001 terrorist attack in the US, the 2011 earthquake and tsunami in Japan, Super Storm Sandy in 2012 in the US, and Ingrid and Manuel in 2013 in Mexico have shown that having a well-developed and thoroughly rehearsed BC/DR plan is key to corporate survival. With 2014 being known as The Year of the Mega Breach,[3] cyberattacks have quickly become a key focus in almost every BC/DR program. The primary goal of a BC/DR program is to reduce the risk and impact of a business interruption.

Megabreaches of companies such as eBay, JPMorgan Chase, Home Depot, Nieman Marcus, Staples and Target have shown that the financial consequences of plummeting sales and crashing stock prices and damage to an organization's reputation from negative press can be catastrophic.[4] Cyberbreach-related lawsuits filed by business partners, customers, investors and the US Federal Trade Commission (FTC) have demonstrated that C-suite executives and the board of directors (BoD) are not immune to being held individually responsible for failure to take reasonable steps to maintain their organization's customers' personal and financial information in a secure manner. Many complaints go on to allege that the individual defendants aggravated the damage to the company by failing to properly handle the cyberbreach once it was discovered. This accountability phenomenon has caused many C-suite and boardroom occupants to find themselves looking for new employment.[5] Home Depot alone is facing at least 44 civil lawsuits as a result of its cyberbreach.[6] Just as the US Sarbanes-Oxley Act of 2002 holds C-suite executives criminally accountable for their firm's accounting and audit practices, it is not unthinkable for those same C-suite executives responsible for the firm's information security to be held criminally negligent for a successful cyberbreach.

In any well-designed BC/DR program, there are three roles that provide leadership: sponsorship, ownership and custodianship. The ownership and custodianship roles generally include the BC/DR plan development, implementation and task execution. Most programs assign middle management to own and oversee the BC/DR plan with the overall responsibility falling squarely on the IT organization. Traditionally, a successful program starts with sponsorship that flows from the C-suite and BoD to the rest of the firm. The impetus to develop and implement a business continuity management (BCM) program may originate from regulatory compliance, risk assessments or business impact analysis. Whatever the reason, socialized support and financial backing from the BoD and the C-suite are key factors in a successful BC/DR program.

Another key factor in a successful program is the maintenance function, which includes constant updating, testing and practice drills. Traditionally, BC/DR preparedness and testing have fallen to middle management and are considered predominantly an IT function. With the exception of some chief information officers (CIO), participation by the C-suite in BC/DR testing is virtually nonexistent. More often than not, the testing and rehearsals are considered a nuisance by C-suite occupants who may be inconvenienced or prevented from working during rehearsals. Perhaps this C-suite distancing is because BC/DR activity is generally viewed as a technical function better left for IT personnel or perhaps it is simply because C-suite executives do not understand the depth and scope of the BC/DR program, even though they are committed to supporting the plan itself.[7] Whatever their reason for staying on the sidelines, the changing BC/DR

risk landscape and the new C-suite cyberbreach accountability is changing the game plan forever.

In 1988, Robert Morris, a student at Cornell University (Ithaca, New York, USA), became the first person convicted under the US 1986 Computer Fraud and Abuse Act for releasing a worm into the wild that caused widespread computer crashes.[8] A little more than 10 years later, three out of 10 US companies had BC/DR plans in place, and even then, only a few considered cyberattacks a valid risk.[9] Today, it would be hard to find a company whose BC/DR plan does not place cyberattacks high on the list of major corporate risk. This is all well and good, but the focus still sits with middle management and on the shoulders of IT and not in the C-suite or the boardroom. The last three Carnegie Mellon CyLabs biennial surveys (2008, 2010 and 2012) reporting on how boards and C-suite executives are governing the security of their organizations have shown only a slight improvement. The overall conclusion of the survey report is that boards and C-suite executives are not actively addressing cyberrisk.[10, 11, 12] One of the most cited reasons for this is that C-suite executives and the BoD consider cybersecurity too technical for them to adequately understand and participate.[13] Perhaps, from a purely technical perspective, the execution of cybersecurity defense programs should remain with middle management, IT and the tactical security operation center (SOC), but with the current atmosphere of executive accountability, one can delegate the authority, but cannot escape the accountability for a cyberbreach.

> "The more prepared the c-suite and BoD are for and the more precision and speed with which they react to cyberbreach will favorably influence the seriousness of the impact on the business."

Despite the ever-increasing attention being paid to cyberattack prevention, the general consensus among cybersecurity experts remains that "there are only two types of companies: those that have been hacked and those that will be."[14] With there being an almost 100 percent certainty of a successful cyberbreach, it is surprising that more attention is not being paid to the handling of the inevitable cyberbreach, especially considering that in 2014 the average cyberbreach had a price tag of almost US $6 million.[15] Most practitioners have seen the benefit of a well-developed and rehearsed game plan. Many sports championships have been won on game plan preparation and practice. That same level of game plan development, preparedness and razor-sharp execution needs to find its way into the C-suite and the boardroom when the inevitable cyberbreach happens. The more prepared the C-suite and BoD are and the more precision and speed with which they react to a cyberbreach, the more they can mitigate the seriousness of the impact on the business. Lisa J. Sotto, Esq., a partner at Hunton & Williams and one of the top cyberbreach attorneys in the US, says, "When facing a cyberthreat, preparation will mitigate harm. It is essential to have identified in advance the trusted advisors who will guide the company in the event of a cyberattack."

So what is the best way to achieve the right level of preparation for handling the inevitable cyberbreach? Considering the foundation for this is most likely already in place, companies today would be well served to extend their BC/DR plan into the C-suite and boardroom. The plan would simply need to be expanded and enhanced to include the postcyberbreach activities of the C-suite executives and the board and, most important, these activities should be updated, tested and rehearsed with the same reverence, attention and level of energy that is given the rest of the BC/DR plan by middle management and IT.

On 10 June 2014, US Securities and Exchange Commissioner (SEC) Luis Aguilar spoke at a Cyber Risk and the Boardroom conference at the US New York Stock Exchange (NYSE). He emphasized that the duty of the BoD is to ensure that the company's cybersecurity stance is on solid ground. He said companies should accomplish this by educating themselves about cybersecurity and making it a part of the board's regular duties. Besides the regular duties of the BoD, it can also arrange for formal training and/or consulting with an outside expert on

cybersecurity to ensure that relevant directors have the required technical understanding to subjunctive evaluate current and future risk.[16] It is key that the BoD understand the full gravity, importance and benefit its participation will play in ensuring that the proper cyberbreach response plan is incorporated into the firm's BC/DR program along with the full participation of the C-suite executives in the program.

The tasks required for handling a cyberbreach by the C-suite will vary from company to company and no two cyberbreaches will ever be identical. Therefore, each cyberbreach must be analyzed and evaluated on its own merits and an action plan formulated that is appropriate for that particular cyberbreach. There are, however, many cyberbreach response tasks that can be enumerated in general and specifically applied in keeping with the individual situation. In the following steps, the general counsel (GC), the CIO, the chief financial officer (CFO) and the chief executive officer (CEO) all play significant roles. The GC plays the most significant behind-the-scenes role, while the CEO and the head of public relations (PR) present the public face of the cyberbreach.[17] The CFO is responsible for the financial, insurance and investor cyberbreach-related considerations:

- **Initial briefing**—Generally, the CIO or IT director will initiate the cyberbreach response and gather the cyberbreach response team together for a full debriefing. This step varies widely between companies. Usually there is a single individual or team that assesses the incident and makes the determination whether or not it warrants the initiation of the formal cyberbreach incident response. Once that decision is made, the cyberbreach team is gathered for a situational debriefing. If the BC/DR cyberbreach program is fully implemented, tested and rehearsed, this will not be the first time the team has met. The debriefing should be a short *who, what, where, when, why* and *how bad* presentation. It is important to gain an initial understanding of the breadth and scope of the cyberbreach. Is it a data-gathering or a destructive cyberattack? This is important as it will dictate the initial technical response by the IT group and the forensic experts. The breadth and scope assessment of the cyberbreach can, and most likely will, be modified and updated numerous times as the investigation continues, new information and insight are gained, and the breach response is underway.
- **Outside counsel and forensic experts**—As part of the development and implementation of the BC/DR cyberbreach program, and prior to any cyberbreach actually happening, the GC should locate an experienced outside cyberbreach expert legal counsel—one who understands the technical, legal and regulatory implications of particular types of cyberbreaches. The outside counsel and forensic experts will advise on and/or perform the following duties:
  - Help further define the breadth and scope of the cyberbreach.
  - Develop a containment strategy.
  - Preserve logs and evidence.
  - Document the cyberbreach.
  - Advise and assist with postbreach remediation activities.

  These steps are important to perform with the advice of outside cyberbreach counsel as the findings gathered may be protected under attorney-client privilege. An additional benefit of bringing in outside expert counsel is that they already have established relationships and connections with law enforcement and other government agencies that can significantly speed up the investigation and smooth out the entire cyberbreach response process. If the cyberbreach was not brought to the attention of the company by law enforcement, these relationships will be even more important when the time comes to report the incident to law enforcement and ask for their assistance.
- **Financial oversight**—The CFO must closely watch all financial channels for inappropriate transactions that may be breach-related. If the company handles credit cards, the CFO will need to alert the appropriate financial institutions. Additionally, the CFO should, with the advice of legal counsel, initiate claims against the firm's insurance policies that cover first-party and third-party loss due to cyberbreaches. Last, if news of the cyberbreach has reached the press, the CFO will need to deal with possible dropping stock prices and a jittery investor community.
- **Employee considerations**—Depending on the nature of the cyberbreach, employee personally identifiable information (PII) may have been compromised. Human resources (HR) will need to advise employees and guide them through the steps necessary to personally protect themselves. If the company has a bring your own device (BYOD) policy, it may be necessary to acquire and inspect personal property

as part of the investigation. In cases where BYOD is in effect, devices may need to be confiscated and held as evidence or for discovery. HR should research these possibilities well in advance of a cyberbreach; understand the firm's rights under federal, state and local law; and be prepared to act as necessary. Even if there are employee-signed personal device usage waivers in place, there may still be privacy issues that need to be addressed related to a cyberbreach. Again, this is where outside counsel's advice can be invaluable.

- **CEO and PR staff**—Once the cyberbreach becomes public knowledge, the CEO and the PR staff will become the public face of the cyberbreach response team. All press releases and public contact should be reviewed by the GC and outside counsel prior to being released. Companies want to avoid public comments that may be inaccurate or cause further damage. It is also important to have a single public face for the cyberbreach and avoid having multiple people talking to the press. How the company's response to the cyberbreach is viewed by the public is a key factor in such things as sales, stock prices and future litigation.

CONCLUSION

There are many steps that can be taken to avoid a cyberbreach, but statistically speaking, the odds are that every company has been or will be breached at some point. It is wise and prudent to make every effort possible to avoid a cyberbreach. However, when a cyberbreach happens, a well-developed, well-tested and well-rehearsed cyberbreach response plan is paramount. The plan must include a detailed playbook; advice and guidance from legal and forensic cyberbreach experts; rehearsals that include in-depth, table-top exercises and constant updating and modification of the plan; and a list of knowledgeable designees who can step in and cover for traveling C-suite executives at a moment's notice. A well-designed BC/DR cyberbreach program that is executed with speed and precision will ultimately make the response process smoother and more efficient and will help to ease any resulting regulatory burden. It will also position the company to better deal with the expected litigation that seems to follow all significant cyberbreaches these days.

ENDNOTES

1 Erbschloe, M.; *Guide to Disaster Recovery*, Thomson/Course Technology, USA, 2003
2 Protiviti, *Guide to Business Continuity Management*, 2013
3 Ponemon Institute, *2014: A Year of Mega Breaches*, 2015, *www.ponemon.org/library/2014-a-year-of-mega-breaches*
4 *Ibid*.
5 Ali, Syed V. P.; J. Dixon; *Why Cyber Security Is a Strategic Issue*, Bain & Company, 2014
6 Calia, M.; "Home Depot Facing at Least 44 Civil Suits in Data Breach," *The Wall Street Journal*, 25 November 2014, *www.wsj.com/articles/home-depot-facing-at-least-44-civil-suits-in-data-breach-1416917359*
7 Deloitte, *"Aware" vs. "Committed" Where Do You Stand?*, Deloitte Touche Tohmatsu Ltd., 2013, *www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/be-aers-ers-bcm-aware-vs-committed_Dec2013.pdf*
8 O'Dell, P. L.; C. Scott; *Cyber 24-7: Risks, Leadership, and Sharing: Sound Advice for the Board, C-Suite, and Non-technical Executives*, CreateSpace Independent Publishing Platform, 2014
9 *Op cit* Erbschloe
10 Westby, J. R.; *Governance of Enterprise Security: CyLab 2008 Report*, Carnegie Mellon, USA, 2008
11 Westby, J. R.; *Governance of Enterprise Security: CyLab 2010 Report*, Carnegie Mellon, USA, 2010
12 Westby, J. R.; *Governance of Enterprise Security: CyLab 2012 Report*, Carnegie Mellon, USA, 2012
13 *Op cit* O'Dell
14 Cowley, S.; "FBI Director: Cybercrime Will Eclipse Terrorism," *CNN Money*, 2012, *http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity*
15 Ponemon Institute, *2014 Cost of Data Breach: Global Analysis*, 2014
16 Tewell, C. M.; *SEC Clarifies Duties of Board of Directors Regarding Cybersecurity and Data Breaches*, Davis, Wright, Tremain, July 2014, *www.dwt.com/SEC-Clarifies-Duties-of-Board-of-Directors-Regarding-Cybersecurity-and-Data-Breaches-07-18-2014/*
17 Smith, R.; W. Cook; "The GC's 30-Minute Breach Drill," Primary Opinion, 10 May 2015, *https://www.primaryopinion.com/articles/gc%E2%80%99s-30-minute-breach-drill*

Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats

Fredric Greene, CISSP, is an experienced IT auditor specializing in technology infrastructure in the financial services industry. His main areas of focus are information and cybersecurity, IBM platforms (mainframe z/OS, AIX Power Systems), databases (DB2, Oracle), and a spectrum of systems and network technology. Another area of focus in recent years is cloud and virtualization technology including VMWare, Citrix and IBM cloud products and services. Greene worked for the legacy organization Bank of Tokyo (prior to its merger to form MUFG Union Bank), Depository Trust & Clearing Corporation (DTCC), and KPMG.

Detective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization's IT environment. These controls include logging of events and the associated monitoring and alerting that facilitate effective IT management. Auditors should identify and assess these critical controls when auditing a cybersecurity program.

According to *Transforming Cybersecurity*, which applies the COBIT® 5 framework and its component publications toward transforming cybersecurity in a systemic way, a key cybersecurity objective is that "attacks and breaches are identified and treated in a timely and appropriate manner."[1]

COBIT 5 also provides the related audit objectives:

1. Confirm monitoring and specific technical attack recognition solutions.
2. Assess interfaces to security incident management and crisis management processes.
3. Evaluate the timeliness and adequacy of attack response.

Another excellent source of guidance for cybersecurity detective controls is the US National Institute for Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).[2] The detect function is a key component of the NIST Cybersecurity Framework, which includes associated categories of anomalies and events and continuous security monitoring.

Cybersecurity detective controls should be designed to identify a range of threats. Lockheed Martin has introduced the Cyber Kill Chain framework, which can be used to detect cyberthreats and includes surveillance (e.g., scanning), weaponization and delivery (e.g., malware), exploitation (e.g., vulnerability), command and control (e.g., compromised administrator accounts), and exfiltration of data (e.g., intellectual property [IP]).

While it is close to impossible to prevent all intrusions, early detection of adverse activity is essential to any cybersecurity regime. Organizations should also emphasize adaptability in their cybersecurity processes and tools to address the dynamic threat landscape.

CYBERSECURITY DETECTIVE CONTROLS

If designed well and operating effectively, specific cybersecurity detective controls should be able to halt the cyberthreats discussed previously. These controls are generally managed or performed by a security operations center (SOC) that is responsible for cybersecurity monitoring.

The security information and event management (SIEM) system is the central software platform that can integrate event logs aggregated from multiple sources with threat data sources (e.g., real-time feeds) and contextual information about assets and users.

There are alternatives to the SIEM approach discussed here, including intrusion detection systems (IDs)and intrusion prevention systems (IPS) that aggregate and analyze security data. There is also an option to outsource the security monitoring function altogether to a third-party vendor. However, this article discusses the SIEM approach, which is highly adaptable and flexible with an organization's requirements.

The SIEM aggregates, normalizes (standardizes format) and correlates event data to identify and prioritize threats, filter out false positives, and provide actionable threat intelligence. An organization's unique context (assets, users, risks) should be integrated into SIEM operations. The SIEM is the essential tool for security analysis, incident response, forensics and regulatory compliance (reporting). *Critical Capabilities for Security Information and Event Management*[4] enumerates many of the key controls in a generic SIEM, including real-time monitoring, threat intelligence, data and user monitoring, application monitoring, analytics, log management, and reporting.

Specific use cases may include detection of suspicious behavior (e.g., compromised privileged user accounts, access to sensitive data), detection of policy violations (e.g., change in server configurations), detection of advanced persistent threats (APTs) (e.g., outbound data flows to international destinations) and detection of fraud (e.g., change in trade volumes or money transfers). Auditors should assess the design and operating effectiveness of the SIEM functionality described.

Event log management is a critical component of the SIEM functionality. Event logs should be aggregated (e.g., pulled) from most or all deployed technology (e.g., source systems) in an organization, including security devices (e.g., firewalls, IDS/IPS, web proxy), network devices (e.g., routers, switches), systems (e.g., mainframe, midrange, distributed servers), applications, databases, storage devices, end-point desktops and mobile devices. Event log data may also be aggregated from various technology functions, such as performance and change management.

Configuring the source systems to send log data to the central SIEM system may require substantial effort. In larger organizations, the volume of event log data can be enormous, and the storage requirements may also be substantial.

A separate module, server or component (e.g., HP Arcsight Log Aggregator, IBM Security QRadar Log Manager) is generally required to manage the logs. Auditors will want to confirm a maximum level of SIEM coverage of logs from around an organization's IT environment.

SOURCES OF THREAT INTELLIGENCE

Gartner defines threat intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."[5]

There is a wide range of threat intelligence vendors that can provide tactical or operational feeds of Internet Protocol (IP) reputation information (e.g., suspected malware sources by IP or uniform resource locator [URL]); malware profiles; indicators of compromise, command and control (C&C) patterns; and exfiltration approaches.

Here is a brief overview of the sources of threat intelligence categorized into current services available for ingestion into a SIEM system:

- SIEM vendors that offer threat intelligence feeds as part of a one-stop solution, e.g., IBM QRadar SIEM combined with IBM X-Force Threat Intelligence service
- Commercial aggregated and packaged threat intelligence from multiple sources—structured and unstructured, e.g., CyberSquared ThreatConnect[6] feed (partnered with Cisco Sourcefire) and AlienVault Open Threat Exchange (OTX), claimed to be the world's largest crowd-sourced repository of threat data
- Free threat intelligence feeds (e.g., Google Safe Browsing API, Zeus Tracker Blocklist) offered through the information security community mostly in the crystallographic information file (CIF) format, including blacklists of IP addresses and URLs suspected in malicious activity[7]
- Original threat intelligence offered as threat feeds, rules, blacklists and parsers (e.g., RSA FirstWatch,[8] which offers intelligence on advanced and emerging threats at the strategic and tactical level)

There are differences in threat information, which may be raw, unfiltered, unvalidated data with varying levels of credibility and intelligence, which are processed, sorted, distilled, accurate and timely, and from reliable sources. Thus, the clear preference is toward threat intelligence.

Threat intelligence becomes more useful when security analysts apply contextual knowledge and analysis to the threat intelligence (e.g., connecting the dots). Contextual knowledge here means the deeper meaning of events—past, present and future. Furthermore, this knowledge includes contextual linkage among tactics, techniques and procedures (TTPs) and the operational environment (e.g., infrastructure).[9]

Intelligence that is specific and enriched with context and actionable data also becomes useful in setting severity and priority ratings.

While this article does not cover the extensive ecosystem of threat data, intelligence and vendors, threat intelligence is, from an audit perspective, a key component of cybersecurity detective controls.

SEVERITY AND PRIORITY RATINGS

An inherent problem with monitoring security-related activity is the potential flood of events and alerts that may be created and transmitted into the SIEM system. FireEye estimates the typical cybersecurity deployment generates five alerts per second.[10] Few, if any, organizations have the resources to investigate such volume of activity.

The key metric of cybersecurity monitoring tools (e.g., SIEM) is not the volume of alerts, but the ability to detect real threats, filter out the meaningful alerts and enrich those alerts with context that facilitates action.[11]

This filtering, validating and correlating of incoming events and alerts is a key process in the overall detective capability. To focus resources (e.g., security analyst time) on the most significant threats, an organization should manage the flow of security events as follows:

- **Reduce the volume of alerts** by reducing the frequency of alerts from devices (e.g., change the frequency of an alert from every second to every minute); aggregate alerts with the same source and destination IP addresses; and remove meaningless indicators and false positives.
- **Prioritize the alerts** that matter most based on business risk. Set priorities by assets, impact on business function (e.g., core processes) and type of activity (e.g., beaconing, policy violation).

CONCLUSION

Detective controls are critical to an organization's cybersecurity posture. A SIEM system is the central component for integrating event logs with threat intelligence and contextual information (organization-specific user, asset and risk data). Event logs should be aggregated from most or all sources in a technology environment. Threat intelligence should be leveraged as tactical or operational feeds of real-time incoming threats. The potential flood of events and alerts should be filtered to enable efficient analysis and response to the most significant and relevant threats.

The net result of implementing these controls in alignment with COBIT 5 is the capability to identify and treat attacks and breaches in a timely and appropriate manner. By reviewing these controls, the auditor can get assurance on the design and operating effectiveness of an organization's cybersecurity detective capability.

ENDNOTES

[1] ISACA, *Transforming Cybersecurity*, USA, 2013, *www.isaca.org*

[2] National Institute for Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 2014, *www.nist.gov/cyberframework*

[3] Lockheed Martin, Cyber Kill Chain, *www.lockheedmartin.com/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html*

[4] Nicolett, Mark; Kelly M. Kavanagh; *Critical Capabilities for Security Information and Event Management*, Gartner, 2012, *www.gartner.com/doc/2022315/critical-capabilities-security-information-event*

[5] Chuvakin, Anton; "Made for Each Other: How to Use Threat Intelligence With SIEM," Gartner, *http://searchsecurity.techtarget.com/tip/Made-for-each-other-How-to-use-threat-intelligence-with-SIEM*

[6] CyberSquared, "ThreatConnect," Cisco Sourcefire, *www.sourcefire.com/partners/technology-partners/sourcefire-technology-partners/threatconnect*

[7] Chuvakin, Anton; "On Comparing Threat Intelligence Feeds," 7 January 2014, *http://blogs.gartner.com/anton-chuvakin/2014/01/07/on-comparing-threat-intelligence-feeds/*

[8] EMC Corp., FirstWatch, *www.emc.com/emc-plus/rsa-thought-leadership/firstwatch/index.htm*

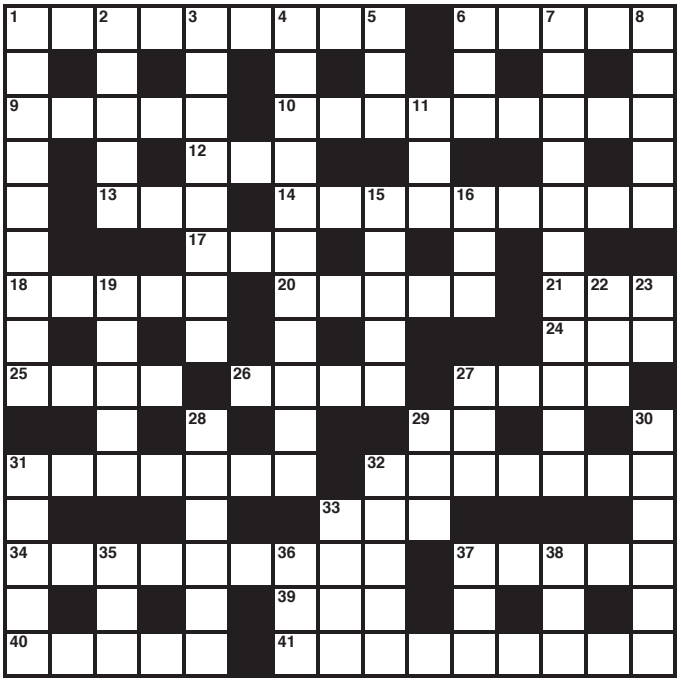
[9] Hartley, Matt; "Cyber Threats: Information vs. Intelligence," 22 October 2014, *www.darkreading.com/analytics/threat-intelligence/cyber-threats-information-vs-intelligence/a/d-id/1316851?page_number=2*

[10] FireEye, "Speed Dating For Security Teams—Finding the Alerts That Lead to Compromise," webinar, August 2014

[11] FireEye, *The SIEM Who Cried Wolf: Focusing Your Cybersecurity Efforts on the Alerts That Matter*, white paper, 2014

Crossword Puzzle

By Myles Mellor
www.themecrosswords.com



ACROSS

1 The I in IDS
6 Concentration
9 Experimental program
10 Uncover diligently, 2 words
12 Sale clause, abbr.
13 Finance abbreviation, up to this point of the year
14 Subjects to rigid order and systematization
17 It's protected by a PIN
18 Incident
20 Review a project for risk and viability
21 Urge (on)
24 Try to win over
25 Examination
26 Go (through), as evidence
27 Matured
29 Latin 1001
31 Mitigate the adverse effects of
32 Diffusion
33 Fault in a program
34 Cadre of professionals who detect and prevent attacks online
37 Up
39 Blemish
40 Incorporate as an essential part
41 They might be worst-case or best-case

DOWN

1 Apply correctly
2 Correspond
3 Reflecting the latest information and practices, 3 words
4 Data
5 "___ any drop to drink": Coleridge
6 Adversary
7 Company's main assets, 2 words
8 Surfing destinations
11 Investor's concern, for short
15 Character who was endlessly awaited in a Beckett play
16 Satisfied a condition
19 Softens
22 Olympian figure
23 Approval for a project, with a
27 Goal
28 Layered
29 Chinese cooking food additive
30 Determine the value, quality, extent and significance of: perhaps a key word for an IT auditor
31 Periodically repeating sequence
32 Seriously unusual or unconventional
33 Bric-a-___
35 Go up and down, as in the water
36 Modem ends?
37 One of the first practical public-key cryptosystems
38 Second sequel's number

(Answers on page 58)

HelpSource Q&A

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

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

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

Do you have something to say about this article?

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

Go directly to the article:

Q How do I ensure that my organization has controls to protect itself from cyberrisk? In other words, what are the key controls that my company must implement to protect itself from cyberrisk?

A There are excellent security frameworks available as public documents that can be used as cybersecurity baseline controls. Here is my list of essential controls:

1. **Patch management**—It is essential to have a structured patch management process. It does not mean that all patches have to be applied, but the enterprise has to make a conscious decision on which to apply and which not to apply. Patch management should be done as a priority for critical applications. While many enterprises apply patches for their IT infrastructure on a priority basis, it is common knowledge that the same rigor is not applied to patch management for software applications.
2. **Administrative privilege control**—It is key to remove administrative privileges from all and grant them only to a select few as determined by job need. Some individuals see it as a status symbol to hold admin privileges. Local admin rights must be removed for a significant majority of users.
3. **Dynamic analysis**—Conducting dynamic analysis, which uses behavior-based detection capabilities instead of the conventional approach of relying on the use of signatures, helps enterprises to detect malware that is yet to be identified. Such dynamic analysis can be undertaken at the enterprise's main gateway, the end point or the cloud, depending on the specific, relevant scenario. Customized sandboxes will help perform structured dynamic analysis.
4. **Host-based intrusion protection/detection system (IPS/IDS)**—Host-based IPS/IDS's detection strength is based on behavior instead of conventional signatures.
5. **Segmenting**—Segmenting the network based on business criticality is yet another essential control. Active Directory and other authentication servers should be able to be administered only from a selected number of intermediary servers called "jump hosts." Jump hosts must be well secured, and jump host access must be limited to a predefined list of users and network devices/equipment. Ideally, jump hosts will have no Internet access.
6. **Multifactor authentication**—Though a number of users view it as painful, it is essential to implement multifactor authentication in the interest of the enterprise.
7. **Internet access**—Direct Internet access from all end points/desktops/laptops must be denied and must instead be processed through a proper proxy.
8. **Passphrase policy**—For service accounts and privileged accounts, it is essential to implement a passphrase policy instead of a password policy; this is yet another area of common resistance.
9. **Web site access**—Access to web sites must be via their domain names and not by IP addresses.
10. **Removable storage media**—Usage of removable storage media must be appropriately controlled—though any restrictions on these are viewed by users as a loss of rights. Any enterprise keen to protect its sensitive information from leakage must restrict access and grant it based on a business need.
11. **User education**—It is not necessarily for all business users, but about educating the developers to write secure code and infrastructure experts to manage it in a secure manner. While users from the business appreciate the risk to the business, it is these experts from the IT world who require more convincing.

12. **External email exchange management**—When emails are exchanged with entities external to the enterprise, it is essential to adopt and implement protocols such as transport layer security (TLS).
13. **Strong asset management**—In terms of having an inventory of authorized devices, equipment and software are essential. Asset management is another area that does not get accorded its due priority.
14. **Web application testing**—Whether the web applications are developed in-house or by a third-party, it is essential to test them for vulnerabilities. They must also be tested via simulated attack scenarios.
15. **The staging environment**—Security testing such as a vulnerability assessment or a penetration test must be done in a replica of the production environment; otherwise, the gap between the environments becomes the weakest link in the chain.
16. **Wireless networks management**—Access must be granted on a need basis with adequate restrictions, and sundries must not be allowed to connect in an unrestricted manner. Ideally, network admission controls mechanisms must be in place.

This is a very indicative list and must not be deemed as exhaustive. Please choose a security framework relevant and apt to your enterprise and use it. These days, cyberrisk insurers also provide guidance documents that they consider prerequisites for any enterprise to buy cyberrisk insurance policies.

In my opinion, it is essential to identify relevant controls and implement them in the most appropriate manner rather than implementing a huge list of controls that are irrelevant and inappropriate. And, of course, the best controls rely on competent professionals to make them work effectively. Sadly, it is a globally accepted fact that there is a huge shortage of cybersecurity professionals. However, ISACA offers on cybersecurity *(www.isaca.org/cyber)*.

CPE Quiz

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

Take the quiz online:

QUIZ #162

Based on Volume 3, 2015—Governance and Management of Enterprise IT (GEIT)
Value—1 Hour of CISA/CISM/CGEIT/CRISC Continuing Professional Education (CPE) Credit

TRUE OR FALSE

DELAK ARTICLE

1. COBIT® 5 integrates widely used human capital methods such as human capital readiness, human capital index and human capital monitor.
2. While COBIT 5 has some limitations when evaluating the level of knowledge and the value of intellectual capital within the organization, an experienced COBIT 5 specialist can very quickly evaluate the level of knowledge management in an organization during due diligence, IS analysis or even IS audit.

PURICELLI ARTICLE

3. Cyberattackers are seeking to gain a foothold a corporate network by leveraging vulnerabilities and, from there, moving laterally to extend the compromised perimeter and take control of other systems within the target company in order to gain access to critical information.
4. According to the investigations performed on the Carabank attack, employees were targeted by social-engineering attacks that resulted in the delivery of malware.
5. By using a controlled web site and tracking the users' behavior, it is possible to measure the inclination of employees to fall victim to such an attack, but it is not possible to estimate the level of exposure of the enterprise to technological follow-up attacks from the simulated phishing campaign.
6. A phishing campaign is not characterized by an impulsive behavior of the employee.
7. Especially in small and medium-sized enterprises, there seems to be a lack of formalized processes that allow enabling countermeasures based on users' reports and, frequently, a poor level of employee knowledge with regard to how to report a security incident.
8. It has been observed that the higher the role in the company, the higher the exposure, but the percentage of deceived managers is marginal, posing some problems that should be considered from a risk management perspective.
9. By using a combination of slapdash exploits, malware code and customized (yet simple) obfuscation techniques, it is possible to bypass the technological countermeasures inside a company and obtain a privileged access to the internal network.
10. Collaboration among departments can support enterprises and help them to define and implement programs that effectively allow for improving the governance of information security.

BRAGA ARTICLE

11. COBIT 5 has embedded the four cross-cutting principles of the UN's sustainable development project to building institutional frameworks that are fit for the challenges of sustainable development.
12. Sustainability requires identifying risk factors that could limit the possibility of future generations to satisfy their needs and put in place countermeasures to prevent negative impacts. It also requires satisfying business requirements.

EVERS ARTICLE

13. The best cloud automation services go to great lengths to always keep customer data safely behind the cloud provider's own firewalls.

VAN NIEKERK AND JACOBS ARTICLE

14. An intrusion block system should be signature-based and not include anomaly and heuristic-based detection.
15. The architecture makes recommendations on providing security in an end-to-end network, and can be applied to various kinds of networks, but not independently of the underlying technology.

ISACA Journal

CPE Quiz

Based on Volume 3, 2015—Governance and Management of Enterprise IT (GEIT)

Quiz #162 Answer Form

(Please print or type)

Name _____

_____

Address _____

_____

_____

CISA, CISM, CGEIT or CRISC # _____

Quiz #162

True or False

DELAK ARTICLE

1._____

2._____

PURICELLI ARTICLE

3._____

4._____

5._____

6._____

7._____

8._____

9._____

10._____

BRAGA ARTICLE

11._____

12._____

EVERS ARTICLE

13._____

VAN NIEKERK AND JACOBS ARTICLE

14._____

15._____

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

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

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

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

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

Answers—Crossword by Myles Mellor

See page 54 for the puzzle.

ISACA MEMBER AND CERTIFICATION HOLDER COMPLIANCE

The specialised nature of information systems (IS) audit and assurance and the skills necessary to perform such engagements require standards that apply specifically to IS audit and assurance. The development and dissemination of the IS audit and assurance standards are a cornerstone of the ISACA® professional contribution to the audit community.

IS audit and assurance standards define mandatory requirements for IS auditing. They report and inform:

- IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession's expectations concerning the work of practitioners
- Holders of the Certified Information Systems Auditor® (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate committee and, ultimately, in disciplinary action.

ITAF™, 3rd Edition (www.isaca.org/itaf) provides a framework for multiple levels of guidance:

- **IS Audit and Assurance Standards**
  The standards are divided into three categories:
  - General standards (1000 series)—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
  - Performance standards (1200 series)—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilisation, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgement and due care.
  - Reporting standards (1400 series)—Address the types of reports, means of communication and the information communicated.
- **IS Audit and Assurance**
  The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorisation as the standards (also divided into three categories):
  - General guidelines (2000 series)
  - Performance guidelines (2200 series)
  - Reporting guidelines (2400 series)
- **IS Audit and Assurance Tools and Techniques**
  - These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programmes, reference books, and the COBIT® 5 family of products. Tools and techniques are listed under *www.isaca.org/itaf.*

An online glossary of terms used in ITAF is provided at *www.isaca.org/glossary*.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The guidance should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the control professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or IS environment.

IS Audit and Assurance Standards

The titles of issued standards documents are listed as follows:

General
1001 Audit Charter
1002 Organisational Independence
1003 Professional Independence
1004 Reasonable Expectation
1005 Due Professional Care
1006 Proficiency
1007 Assertions
1008 Criteria

Performance
1201 Engagement Planning
1202 Risk Assessment in Planning
1203 Performance and Supervision
1204 Materiality
1205 Evidence
1206 Using the Work of Other Experts
1207 Irregularity and Illegal Acts

Reporting
1401 Reporting
1402 Follow-up Activities

IS Audit and Assurance Guidelines

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

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

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

Reporting
2401 Reporting
2402 Follow-up Activities

The ISACA Professional Standards and Career Management Committee (PSCMC) is dedicated to ensuring wide consultation in the preparation of ITAF standards and guidelines. Prior to issuing any document, an exposure draft is issued internationally for general public comment.

Comments may also be submitted to the attention of the Director of Professional Standards Development via email (*standards@isaca.org*); fax (+1.847. 253.1443) or postal mail (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

Links to current and exposed ISACA Standards, Guidelines, and Tools and Techniques are posted at *www.isaca.org/standards.*

Advertisers/Web Sites

Leaders and Supporters

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

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

ISSN 1944-1967

ISACA®
Trust in, and value from, information systems

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

www.isaca.org/bookstore

FEATURED CATEGORY: CYBER SECURITY BOOKS BY ISACA®

INSIGHTS AND RESOURCES FOR THE CYBER SECURITY PROFESSIONAL

Cyber security—where everything that matters in information, technology and business converges. ISACA offers books to meet the cyber security needs of your enterprise; reasonable security at affordable cost. And ISACA's suite of cyber security products can help you prepare for and manage risk and threats.

FEATURED TITLES:

- Cybersecurity Guidance for Small and Medium-Sized Enterprises
- Implementing Cybersecurity Guidance for Small and Medium-Sized Enterprises
- CSX Cybersecurity Fundamentals Study Guide
- Implementing the NIST Cybersecurity Framework
- Advanced Persistent Threats: How to Manage the Risk to Your Business
- Transforming Cybersecurity
- Responding to Targeted Cyberattacks
- Securing Mobile Devices

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

FEATURED CATEGORY:

CYBER SECURITY

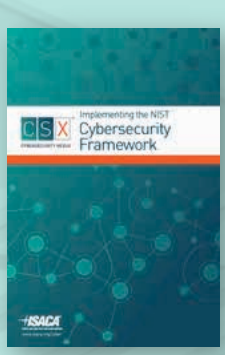
CSX Cybersecurity Fundamentals Study Guide

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

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

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

Implementing the NIST Cybersecurity Framework



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

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

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

Transforming Cybersecurity

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

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

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

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

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

Cybersecurity Guidance for Small and Medium-Sized Enterprises

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

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

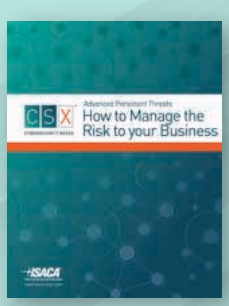
Cyber security is rapidly becoming a critical activity in many enterprises, due to the increasing number of cyber attacks and cyber crime. Cyber attacks often target small and medium-sized enterprises, because cyber criminals expect information in SMEs to be less protected than in large enterprises.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

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

Advanced Persistent Threats: How to Manage the Risk to Your Business

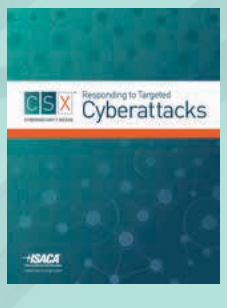


This book explains the nature of the security phenomenon known as the advanced persistent threat (APT). It also provides helpful advice on how to assess the risk of an APT to the organization and recommends practical measures that can be taken to prevent, detect and respond to such an attack. In addition, it highlights key differences between the controls needed to counter the risk of an APT attack and those commonly used to mitigate everyday information security risk.

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

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

Responding to Targeted Cyberattacks



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

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

eBook Product Code: WRTC
Member/Nonmember:
Free/$59.00

Securing Mobile Devices

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

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

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

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

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

Implementing Cybersecurity Guidance for Small and Medium-Sized Enterprises

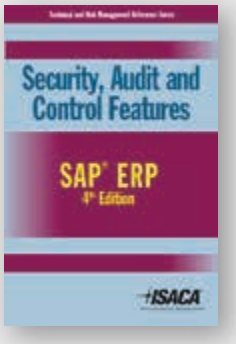
Cybersecurity is a topic of interest for most enterprises, regardless of their size. Cybercrime and cyberwarfare are not restricted to large, multinational enterprises. Increasing numbers of small and medium-sized enterprises (SMEs) are being targeted. In an SME context, information security and cybersecurity are often difficult to implement in a satisfactory and cost-effective manner. SMEs need hands-on guidance for affordable and effective cybersecurity.

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

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

NEW PUBLICATIONS

Announcing New Publications—Now Available in ISACA's Bookstore!



Security, Audit and Control Features SAP ERP, 4th Edition

Product Code: ISAP4
Member/Nonmember: $60.00/$80.00

eBook Product Code: WISAP4
Member/Nonmember: $60.00/$75.00

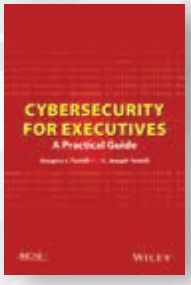
SAP SE is a multinational software corporation that makes enterprise software to manage business operations and customer relations; their primary product is SAP ERP Central Component (known as ECC, but previously named SAP® R/3). This fourth edition of the technical reference guide on the audit of SAP ERP is one of two technical reference guides providing information relating to the world's major ERP systems. The purpose of the fourth edition of this research is to update best practices and identify trends in ERP risk and control.

Controls and Assurance in the Cloud: Using COBIT 5

Product Code: CB5CA
Member/Nonmember: $35.00/$60.00

eBook Product Code: WCB5CA
Member/Nonmember: $Free/$60.00

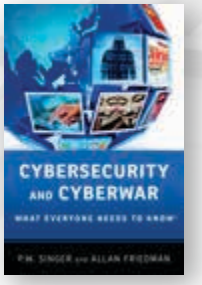
This book provides practical guidance for enterprises using or considering using cloud computing. It identifies related risk and controls, and provides a governance and control framework based on COBIT 5, and an audit program using COBIT 5 for Assurance. This information can assist enterprises in assessing the risk and potential value of cloud investments and determine whether the risk is within the acceptable level.



Cybersecurity for Executives: A Practical Guide by Gregory J. Touhill,C. Joseph Touhill

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

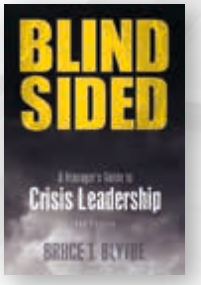
Practical guide that can be used by executives to make well-informed decisions on cyber security issues to better protect their business. Emphasizes, in a direct and uncomplicated way, how executives can identify, understand, assess, and mitigate risks associated with cyber security issues.



CyberSecurity and Cyberwar—What Everyone Needs to Know by P.W. Singer and Allan Friedman

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

Today, our entire modern way of life, from communication to commerce to conflict, fundamentally depends on the Internet. And the cyber security issues that result challenge literally everyone: politicians wrestling with everything from cyber crime to online freedom; generals protecting the nation; business executives defending firms; lawyers and ethicists building new frameworks.



Blindsided: A Manager's Guide to Crisis Leadership by Bruce T. Blythe

Product Code: 9RO
Member/Nonmember: $30.00/$40.00

Hold-on: Blythe lands you in the middle of a fast-breaking crisis and uses case studies and examples to demonstrate what a top-notch leader would say and do at every turn. He then uses his 30 years of global experience to show you how to develop and write a highly practical crisis management plan. His is uniquely two books in one—Crisis Response and Crisis Preparedness interwoven with lessons in Crisis Leadership.

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

EUROCACS/ISRM 2015

9 – 11 November 2015 | Copenhagen, Denmark

GROW YOUR **NETWORK**.

ENHANCE YOUR **KNOWLEDGE**.

Hear from Global Thought Leaders. Apply Fresh Perspective to Taking on Your World.

During his tenure at the DSIS, Former Director General of Danish Security and Intelligence Jakob Scharf successfully led his team to identify and counter an exponential rise in al-Qaeda terrorist threats resulting from the "Cartoon Crisis" stemming from the publication of illustrations depicting the prophet Muhammed in a Danish newspaper. He led efforts to take on the challenge facing his nation after Denmark became a priority target for insider cyber attacks. During his keynote address, ***Fighting for National Security,*** Jakob will share how these experiences shaped Denmark's holistic approach to national security issues and placed the DSIS into a leading role in reducing radicalisation, countering specific terrorist activities and developing measures for effective investigation and prosecution of terrorists. He will also discuss how the government can partner with both public and private organisations in sharing information and intelligence to improve security for all.

Jakob Scharf
Former Director General of the Danish Security and Intelligence Service (DSIS) (2007-2014)

Jakob Scharf was instrumental in successfully identifying, preventing and countering a number of specific threats against Denmark and Danish interests abroad. Jakob now shares his experiences in a more international context.

Take advantage of this and many more opportunities to be inspired, embrace new tools and connect with leaders, experts and fellow professionals in audit, assurance, security, cyber security, risk and governance at Europe's prestigious **EuroCACS/ISRM 2015 conference** at the famous **Tivoli Hotel** in historic **Copenhagen Denmark**.

MORE INSIGHT

Secure your place today! Earn up to 39 CPEs!
Register today at *www.isaca.org/Eurojv5*

ISACA®


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