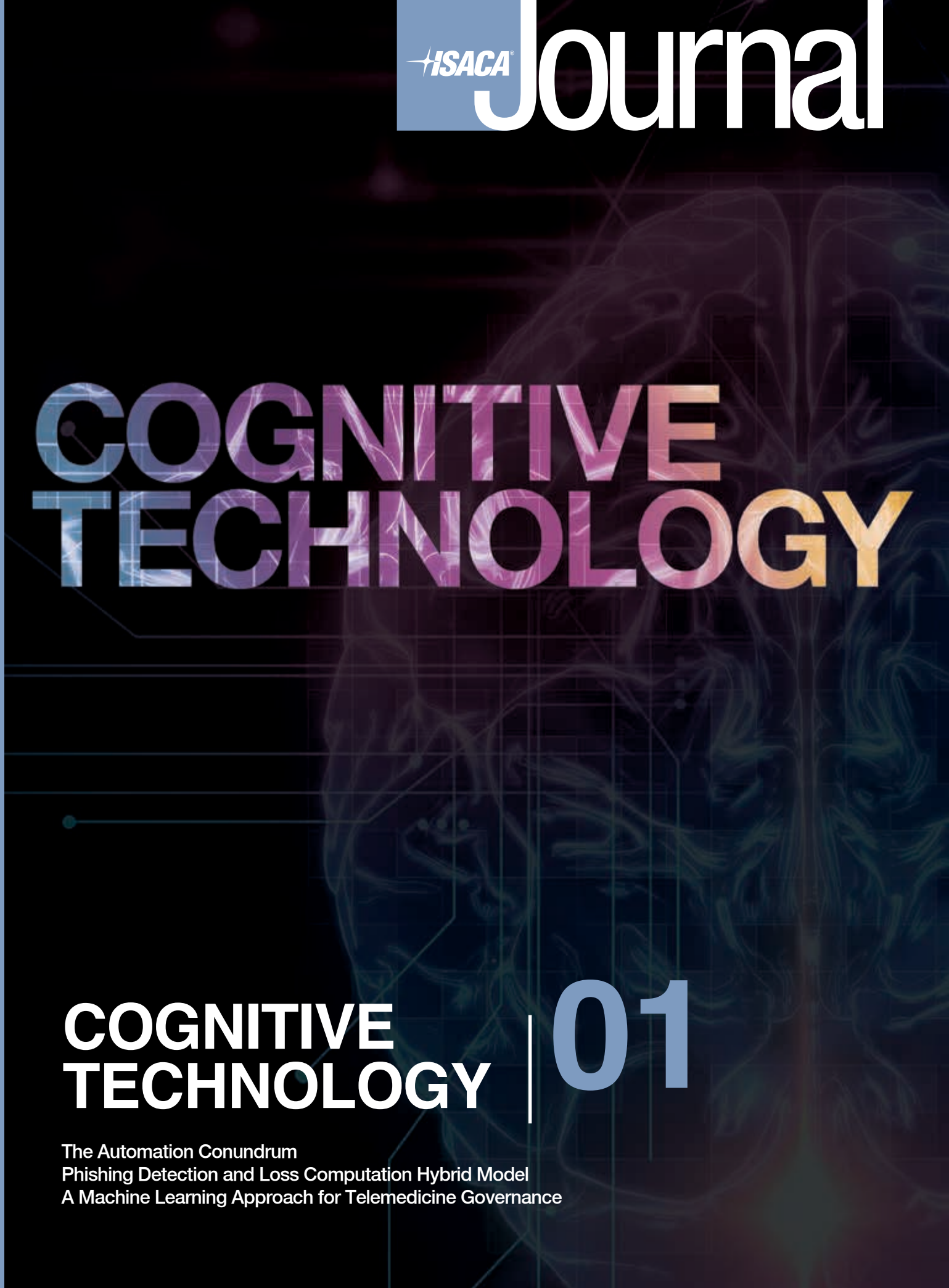
Volume 1, 2017

ISACA Journal

COGNITIVE TECHNOLOGY



COGNITIVE TECHNOLOGY | 01

The Automation Conundrum
Phishing Detection and Loss Computation Hybrid Model
A Machine Learning Approach for Telemedicine Governance

www.isaca.org

Taking an ISACA® certification exam just got a lot more convenient!

Experience the difference starting in 2017.

REGISTER EARLY TO SAVE US $50! Early registration deadline: 28 February 2017

What does this change mean for you?

- > More opportunities to take an exam
- > Larger test center network
- > Faster exam results
- > Test centers designed specifically for testing

Be part of this exciting transition to computer-based testing and be one of the first to take an ISACA® certification exam in 2017! Take the first step towards obtaining a globally respected ISACA certification and becoming recognized as one of the most-qualified professionals in your field of information systems.

Register today at: ***www.isaca.org/2017exams-Jv1***

ISACA®
Trust in, and value from, information systems

DON'T MISS THIS
ONCE-A-YEAR OPPORTUNITY

Society of Corporate Compliance and Ethics

5th Annual

European Compliance & Ethics Institute

2–5 April 2017
Prague, Czech Republic

* Hear the latest on data permissioning and other hot topics
* Learn the latest and best solutions for compliance and ethics challenges from across the legal and regulatory spectrum
* Connect with the global compliance community and expand your network
* Earn the continuing education units you need, and take the Certified Compliance & Ethics Professional-International (CCEP-I)® exam

TO LEARN MORE:

europeancomplianceethicsinstitute.org

Questions? lizza.catalano@corporatecompliance.org

ISACA Journal

FEATURES

PLUS

Online-exclusive Features

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

Online Features
The following is a sample of the upcoming features planned for January and February 2017.

Capability Framework for Privileged Access Management
Richard Hoesl, CISSP, SCF, Martin Metz, CISA, Joachim Dold and Stefan Hartung

Preparing for Auditing New Risk, Part 2
Ed Gelbstein, Ph.D.

Smart Sustainable Cities Need Well-governed Disruptive IT, Not Just IT
Graciela Braga, CGEIT, COBIT Foundation, CPA

Discuss topics in the ISACA® Knowledge Center: *www.isaca.org/knowledgecenter*
Follow ISACA on Twitter: *http://twitter.com/isacanews*; Hashtag: #ISACA
Follow ISACA on LinkedIn: *www.linkedin.com/company/isaca*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

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

Read more from these *Journal* authors...

Journal authors are now blogging at *www.isaca.org/journal/blog*. Visit the *ISACA Journal* blog, Practically Speaking, to gain practical knowledge from colleagues and to participate in the growing ISACA® community.

ISACA®
Trust in, and value from, information systems

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

2017
NORTH AMERICA
CACS™
AN ISACA EVENT
1 – 3 MAY | LAS VEGAS, NEVADA

Hone Your Skills

in Expert-led Workshops at North America CACS 2017

Join us at **North America CACS 2017 in Las Vegas, Nevada, USA—1-3 May 2017**. In addition to growing your professional network, you can hone your skills in cutting-edge workshops on hot-button issues that impact your field of information systems. New this year, each 2-day pre-conference workshop has a 1-day post-conference counterpart that enables you to take lessons learned in the topic area to the next expert level. Choose from exciting interactive sessions in audit, compliance, risk, governance and cyber security and sign up today!

Earn 14 CPEs by attending one of the Pre-Conference Workshops

Saturday, 29 April | 9:00AM – 5:00PM
Sunday, 30 April | 9:00AM – 5:00PM

WS1 COBIT® 5 Foundation
WS2 Cybersecurity Fundamentals
WS3 Applied Data Analysis
WS4 CISA® Prep Course

Earn 7 CPEs by attending one of the Post-Conference Workshops

Wednesday, 3 May | 1:30PM – 5:00PM
Thursday, 4 May | 9:00AM – 12:30PM

WS5 The Intersection of IT & Assurance by Leveraging COBIT 5
WS6 Using Risk Scenarios
WS7 Cybersecurity for Auditors
WS8 IT Audit: Taking the Next Step

EARN UP TO 21 CPE HOURS FOR A CONFERENCE AND WORKSHOP TOTAL OF 39 CPES!
REGISTER TODAY!

Register at ***www.isaca.org/NACACS17jv1***

*See website for pricing and registration details.

ISACA®
Trust in, and value from, information systems

information security matters

State-on-state Cyberconflicts

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

In the second quarter of 2016, a colleague shared with me an article and a database titled "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11," written by Brandon Valeriano of the University of Glasgow and Ryan C. Maness of the University of Illinois.[1] It was published in the *Journal of Peace Research* in April 2014. Now, I suspect that the readership of that fine journal and the one you are reading now do not overlap to a great extent, so I will summarize their work and then give my opinions on the subjects they raise.[2]

Importantly, Valeriano and Maness are writing about a specific subset of all cyberattacks, those initiated by a state on the resources of another state, including their private sector organizations and individuals as well as governmental resources. This study examines only actions taken by a government as the initiator of a cyberincident.[3] It addresses the period from 2001 through 2011, stopping at that point to ensure extensive analysis of all incidents and disputes.[4]

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.

Along with their article, the authors published their information set so that any reader can re-create and, perhaps, extend their analysis.[5] Surprisingly, at least to me, they found only 111 cyberincidents in the period of their research, which they distinguish from cyberdisputes, of which there were 45. They make the differentiation that "Cyber incidents are individual operations launched against a state. Cyber disputes are specific campaigns between two states using cyber tactics during a particular time period and can contain one to several incidents, often including an initial engagement and responses."[6] According to their figures, the most frequent initiator was China; the most frequent target was Pakistan.[7]

Valeriano and Maness are to be congratulated for the thoroughness of their research and the thoughtfulness of their analysis. However, I disagree with their conclusions or, as they put them, their "hypotheses."

But what is the purpose of critiquing an article already three years old in a journal that few ISACA® members have ever heard of, much less read? My rationale begins with the recent statement issued by the G7 Summit in May 2016, which equates state-on-state cyberactivities with acts of war.[8] The people who plan for and respond to government-initiated cyberincidents may very well read the *Journal of Peace Research,* and they are treading into an area where ISACA constituents have significant knowledge and awareness of the current state of both risk and preparedness. So we, too, have a right to be heard on this important topic.

Granted, I have the advantage of knowing about five additional years of cyberincidents, as reported in the media. And perhaps 2011 represented a marked upturn in state-on-state activity. But inasmuch as their hypotheses are stated in future terms, I feel comfortable in extrapolating my own conclusions from the available data.

Hypothesis 1

Due to restraint dynamics, the observed rate and number of cyberoperations between rivals is likely to be minimal. It seems to me that recent events have shown no slowing in the incidence of cyberdisputes. What we lack is definitiveness as to whether the

actions taken were instigated by governments or by individuals acting with state acquiescence, if not outright support. Was it the North Korean government that stole and destroyed information from Sony?[9] Did Russian officials steal emails from the US Democratic National Committee during an election year?[10] Were the distributed denial-of-service (DDoS) incidents suffered by the Philippines after the ruling against China's territorial claims in the South China Sea carried out by the state or by self-styled, but unsanctioned, "patriots"?[11] We will probably never know.

With that proviso, I do not believe that there has been, nor will there be, any diminution in the rate of cyberoperations, whatever those might be. The United States has a Cyber Command in its military, China has a centralized command reporting to the Central Military Commission,[12] the European Union's European Network and Information Security Agency (ENISA) is combatting cyberattacks,[13] and Russia has so-called Information Troops.[14] Anyone who believes that these organizations are for defensive purposes only is, in my opinion, quite naïve.

A more legitimate question is whether any state would carry out a cyber-first strike. I believe that a state would, in the proper circumstances, in which it felt that its vital national interests or even existence are threatened. That is, cyber "weapons" might be used in situations where it was felt that a target state was preparing to use physical, rather than information, force. The Stuxnet attacks on Iranian nuclear facilities, addressed in the Valeriano-Maness study, fit that mold.

Hypothesis 2

When cyberoperations and incidents do occur, they will be of minimal impact and severity due to restraint dynamics. Much of this assertion depends on the definition of "minimal." If the comparison is with the damage caused by World War II, then true enough, cyberincidents thus far have been minimal. But if, for instance, a US presidential election were to be disrupted by cyberattacks, I would consider that a rather severe impact which, in turn, could lead to more serious military consequences.

Valeriano and Maness dismiss this possibility by saying that "offensive states will choose tactics that are easily hidden and free of direct responsibility."[15] The fact that states will seek plausible deniability does not minimize the chance that they will initiate such incidents. Nor does it reduce the possibility that the targeted state will conclude that a state-sponsored incident had occurred and retaliate, setting off an escalation of incidents of greater and greater severity.

"Cyber 'weapons' might be used in situations where it was felt that a target state was preparing to use physical, rather than information, force."

Hypothesis 3

Cyberincidents and disputes that do occur will likely be limited to regional interactions. This hypothesis is the most difficult for me to understand or agree with. In their own analysis covering the period from 2001 through 2011, they report incidents between the United States and Iran, which are certainly not regional. Moreover, governments are generally likely to engage in disputes with neighboring countries, which makes the hypothesis self-fulfilling.

In addition, the Internet has made the entire world one great region, with virtually every action against a given state having repercussions in interactions with other states. These days, no island is an island, entire of itself. Thus, it is likely that the greatest information powers, such as China, the European Union, Russia and the United States, plus lesser

Enjoying this article?

- **Learn more about, discuss and collaborate on cyber security in the Knowledge Center.** *www.isaca.org/cybersecurity-topic*
- **Access career tools, resources and learn more about cyber security certifications on the CSX website.** *https://cybersecurity.isaca.org/*

powers such as Iraq and North Korea (all mentioned in the article), will continue to prepare for and possibly execute war-like activities in cyberspace, which is hardly a regional place.

My issues with the Valeriano-Maness argument do not diminish my respect for their scholarship. I believe that, were he alive today, Carl von Clausewitz, the Prussian general and military theorist, would say that "Cyberwar is the continuation of war by other means."[16]

Endnotes

1 Both Valeriano and Maness have moved on to other universities since the publication of their article.
2 Valeriano, B.; R. C. Maness; "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11," *Journal of Peace Research*, May 2014, vol. 51, no. 3, p. 347-360, *http://jpr.sagepub.com/content/51/3/347.abstract*. The article and its accompanying database are available, but there is a fee of US $36 to download it.
3 *Ibid*., p. 3. Valeriano and Maness eschew the term "cyberattack" as they feel it "to be misguiding and inappropriate in that it conflates the tactic to sound something akin to a conventional military attack." With respect, I will use their terminology here.
4 *Ibid*., p. 5
5 I tried a few analyses of my own and found that I was not getting any new insights, so I stopped. The database is available along with the article.
6 *Op cit*, Valeriano and Maness, p. 3.
7 *Ibid*., p. 10
8 G7 2016 Ise-Shima Summit, "G7 Ise-Shima Leaders' Declaration," 26-27 May 2016, *www.mofa.go.jp/files/000160266.pdf*
9 Park, M.; D. Ford; "North Korea to U.S.: Show Evidence We Hacked Sony," CNN, 14 January 2015, *www.cnn.com/2015/01/13/asia/north-korea-sony-hack/*
10 Sanger, D. E.; E. Schmitt; "Spy Agency Consensus Grows That Russia Hacked D.N.C.," *The New York Times*, 26 July 2016, *www.nytimes.com/2016/07/27/us/politics/spy-agency-consensus-grows-that-russia-hacked-dnc.html*

Brandon Valeriano, Ph.D., Replies

I am pleased to offer a response to Steven Ross's thoughtful review of our article; it is indeed an important topic for anyone concerned with cyberconflict. We cover the issue of the rate of attacks and what we call cyberpeace in our article "The Coming Cyberpeace."[17] While the rate is certainly increasing, there is no clear demonstration of severe attacks we might expect by now. Ukraine Black Energy was fixed fairly quickly by going to the substations. The recent US Democratic National Committee (DNC) and US Republican National Committee (RNC) hacks continue to show an absence of real information leaks[18] and the attacks on US electoral systems represent attempts, but no actual altering of electoral systems.[19] What we witness is cyberespionage, not cyberwar.

Interestingly, we were surprised by the relative lack of significant documented cyberincidents (hacking attempts and intrusions are, of course, fairly common). We assumed we would find more, but this has not been the case and continues to be the trend, in that we are locating only dozens per year. Our point is to counter language such as "could be," "possibly" or "in the future." We have a large amount of data on cyberactions being used in the last 20 years and see cyber as an additive power, not a sole method of attack. That cyber will be the method of first strike is conjecture, but, based on war gaming exercises, it is an unsure tactic that governments are not going to depend on when they attack. Plus, there is the issue of cyberactions being one-shot weapons. Once a vulnerability is exploited, the opposition will close that hole in the future. We are not in cyberwar and unlikely to ever see it. Thomas Rid, professor in Security Studies, King's College London (UK) writes frequently on this issue from the Clauzwitzian perspective. What we are concerned about and fear in the future is government-led attacks on individuals such as activists, protestors and journalists.

Cyber used for violence and war is purely an additive technology, a method of espionage or disruption. Making this point clear is imperative as it shapes the policy we construct, our assumptions about future conflict, and can often exacerbate fears, making a technology with so many positive attributes closed to society.

11 Piiparinen, A.; "China's Secret Weapon in the South China Sea: Cyber Attacks," *The Diplomat*, 22 July 2016, *http://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/*

12 *Bloomberg News*, "China Military Seeks to Bring Cyber Warfare Units Under One Roof," 22 October 2015

13 Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, 2013

14 Giles, K.; "'Information Troops'—A Russian Cyber Command?," 3rd International Conference on Cyber Conflict, 2011, *https://www.researchgate.net/publication/224247775_Information_Troops_-_A_Russian_Cyber_Command*

15 *Op cit*, Valeriano and Maness, p. 5

16 What he actually said is that "War is the continuation of politics by other means."

17 Valeriano, B.; R. C. Maness; "The Coming Cyberpeace: The Normative Argument Against Cyberwar," *Foreign Affairs*, 13 May 2015, *https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace*

18 Eichenwald, K.; "Dear Donald Trump and Vladimir Putin, I Am Not Sidney Blumenthal," *Newsweek*, 10 October 2016, *www.newsweek.com/vladimir-putin-sidney-blumenthal-hillary-clinton-donald-trump-benghazi-sputnik-508635*

19 Department of Homeland Security, Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security, press release, 7 October 2016, USA, *https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national*

20 Limnell, J.; T. Rid; "Is Cyberwar Real?," *Foreign Affairs*, March/April 2014, https:*//www.foreignaffairs.com/articles/global-commons/2014-02-12/cyberwar-real*

IS audit basics

Preparing for Auditing New Risk, Part 1

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

This is the first of two articles attempting something unwise: predicting future risk arising from information systems and technology. These pages are an invitation to readers to discuss them and suggest missing items, incorrect assumptions and how the role of auditors may change as a result.

Two quotations are especially apt: "Look to the future, because that's where you'll spend the rest of your life,"[1] and "The trouble with the future is that it usually arrives before we're ready for it."[2] Both apply to organizations taken by surprise before they can even consider issuing a policy and to everyone else (including auditors).

Innovative technologies have unintended consequences that become apparent after they have been adopted. Old-style audits were like driving a car by looking in the rearview mirror: They concentrated on past actions, looked for faults and recommended improvements. Now there are risk-based audits, which rely on acceptance that risk is in the future and collaboration with those identifying and assessing risk is the most effective approach.

Doing this strengthens the consultancy role of internal audit by opening a dialog with the risk function, data custodians and information systems/information technology (IS/IT) operations, and raising awareness with senior management. Accountability for following up and mitigating emerging risk remains with the auditees.

Ed Gelbstein, Ph.D., 1940-2015
Worked in IS/IT in the private and public sectors in various countries for more than 50 years. Gelbstein did analog and digital development in the 1960s, incorporated digital computers in the control systems for continuous process in the late '60s and early '70s, and managed projects of increasing size and complexity until the early 1990s. In the '90s, he became an executive at the preprivatized British Railways and then the United Nations global computing and data communications provider. Following his (semi)retirement from the UN, he joined the audit teams of the UN Board of Auditors and the French National Audit Office. Thanks to his generous spirit and prolific writing, his column will continue to be published in the *ISACA® Journal* posthumously.

It is also necessary to accept that attackers are smart, hard-working and possibly more motivated than the defenders. Attackers have fewer challenges to contend with such as administrative trivia, justification of expenditures, organizational politics and lack of senior management interest.

Attack tools continue to become more sophisticated and data assets more valuable and critical. All of these factors make thinking about future risk more important than ever.

Evolving Domains of IS/IT and Their Potential Risk: The "Known Knowns"

Auditors are not accountable for risk management or assessment, but it is appropriate for them to take an interest in developments likely to change their organization's exposure to risk. An initial list—readers are invited to suggest additional items—includes the items outlined in **figure 1**.

Figure 1—Overview of Emerging IS/IT Risk Domains

Known Knowns	Known Unknowns
Governance	Internet of Things
Mobile	Big Data
Cloud	Militarization
Software	Over the Horizon

Source: E. Gelbstein. Reprinted with permission.

Governance Audit Challenges

Board members and senior managers (the C-suite) have a broad range of responsibilities, huge demands for their time and attention and, inevitably,

a limited knowledge of many corporate disciplines. IS/IT are probably the ones they know the least about.

> **"IS/IT is ubiquitous in any organization and may create an illusion of intuitiveness and simplicity, neither of which is true."**

Chief information officers (CIOs) are seldom part of the C-suite and, when things work, IS/IT becomes invisible. That is, until budget time, at which time the "Why are we spending so much on this?" issue is raised. Because information is intangible, quantifying the return on investment (ROI) of IS/IT remains a challenge.

This is unfortunate because both strategy (and the res that support it) and policies need the informed participation and commitment from the executive level. This can lead to two potential negative outcomes:

1. Policies[4] are not issued before the lack of them creates an irreversible situation (as happened in many organizations with social media and bring your own device [BYOD]).
2. When policies are issued, they are not understood or complied with in day-to-day activities.

IS/IT is ubiquitous in any organization and may create an illusion of intuitiveness and simplicity, neither of which is true. The chief audit executive (CAE), the IS/IT auditors and the audit committee are well placed to convey these messages to the leadership of the organization and address them at the strategic level.

The Audit Challenge of the Mobile World

Developments in mobile technologies have occurred faster than many expected; even some vendors were taken by surprise (and went out of business). The reality now is that smartphones, phablets and tablets are rapidly displacing the easier-to-control environment of networked personal computers, thus introducing new risk to the organization.

Individually owned devices used to access corporate data should be of concern to auditors because, at a minimum, the following may occur:

- Nobody is accountable for the security of the devices—not the chip designers and manufacturers, the operating system designers, the designers of applications (apps), network operators, Internet service providers, or others.
- Owners of mobile devices can easily learn how to remove restrictions placed by their vendors,

Enjoying this article?

- **Read IT Risk Management Audit/Assurance Program.** *www.isaca.org/auditprograms*
- **Learn more about, discuss and collaborate on audit tools and techniques in the Knowledge Center.** *www.isaca.org/it-audit-tools-and-techniques*

"jailbreaking" in iOS devices and "rooting" in Android devices. This is a form of privilege escalation, i.e., a method to gain access to resources that are normally protected from an application or a user. This leaves the device open to cyberattacks and the leakage of sensitive information.

- Countermeasures against the loss or theft of a device accessing sensitive corporate data or malware fall into two categories: building greater awareness of good practice to protect their devices and the data they contain (good hygiene)[5] among owners/users and using products such as antimalware detection and protection. It is questionable to what extent these are implemented.
- Because of the reliance on such devices, auditors should discuss with the executive level whether mobile devices should be included in disaster recovery and business continuity plans. However, at present, this is rarely the case.
- Legislation on individual rights concerning privacy may not allow an organization to monitor or audit such devices and this leaves the organization exposed to unknown risk.

Among the high-impact developments to be expected in the mobile world is an enterprise app store providing certified software, data visualization, predictive analytics and augmented reality; in fact, these offerings are already on the horizon. Is it possible to predict what will come after them?

Outsourcing and Cloud Services

While outsourcing has been around for many years and is well understood, the growth of cloud usage has been faster than many expected and data have migrated[6] to this environment before data owners could give due consideration to the implications of doing so. Given that operational accountability has been transferred to a third party, this can create the "out of sight, out of mind" reaction.

Corporate businesses store sensitive personal and proprietary information in the cloud. However, their contractual arrangements may not have adequate provision for auditing how the service provider protects this information against unauthorized access by third parties and by their own personnel.

The case for assessing this individual risk and how to do so (if it is at all possible) should be discussed with the service provider, and the discussion needs to reflect the criticality and sensitivity of the data concerned. This risk could change rapidly if and when there is a consolidation of the market for cloud service providers involving mergers, acquisitions and disposals.

These issues add to the already long list of things auditors need to consider including in their audit strategy and audit plans related to the cloud.

> **"Risk could change rapidly if and when there is a consolidation of the market for cloud service providers involving mergers, acquisitions and disposals."**

Software

This topic is so large it could fill a book. The following provide only a high-level view:

- **End-user computing (EUC)**—This includes spreadsheets, personal databases and small applications. No one knows exactly what is "out there," undocumented, untested and possibly of questionable quality. This does not stop these files being used to support critical business decisions.
- **Apps for mobile devices**—Apps are easy to buy, download and install, but they can also introduce embedded malware. In addition, suppliers of the devices add apps that the buyer cannot remove. Users who jailbreak their devices create additional risk. These are all hard to audit and present unknown risk.

- **Conventional off the shelf (COTS)**—Shrink-wrapped and/or customizable software such as enterprise resource planning (ERP) and customer relationship management (CRM) will not be discussed in this article because they have been around for a long time and, therefore, have been extensively audited.

Custom software[7] has specific audit needs including built-in controls (e.g., access controls, privileges, segregation of duties) and toxic code back doors, logical bombs or other features programmers can exploit at will. Auditors are well aware of these issues.

Programming techniques such as service-oriented architectures and the emerging software-defined architecture cannot be audited without substantial knowledge of what they involve—another challenge for the auditors.

Interim Conclusions

This column discusses the "easy" aspect of new risk. By now, we should have recognized these aspects and started to audit those areas for which there are guidelines (admittedly, not many). Part 2 of this series will focus on more speculative items.

Endnotes

1 George Burns, 1896-1996, US comedian, actor and producer
2 Arnold H. Glasow, 1905-1998, US businessman
3 Lyra, M. R.; J. C. F. Simoes; "Checking the Maturity of Security Policies for Information and Communication," *ISACA® Journal*, vol. 2, 2015, *www.isaca.org/Journal/archives*
4 IBM MaaS360, "Bring Your Own Device—Ten Commandments," *www2.maas360.com/services/maas360-ten_commandments_of_byod_bring-your-own-device.php*
5 Gelbstein, E.; "Imperfect Technologies and Digital Hygiene: Staying Secure in Cyberspace," *ISACA Journal*, vol. 5, 2014, *www.isaca.org/Journal/archives*
6 Gelbstein, E.; V. Polic; "Data Owners' Responsibilities When Migrating to the Cloud," *ISACA Journal*, vol. 6, 2014, *www.isaca.org/Journal/archives*
7 A three-part IS Audit Basics Column, "Large Software Projects," will cover this topic and are to be published in upcoming issues of the *ISACA Journal*

Gail Coury, CISA, CISM, CISSP
Has more than 20 years of experience in information security infrastructure systems and network management, security technical consulting, information systems auditing, and programming. She has worked in industries including software and hardware technology, airline reservation systems, insurance, banking and retail. She leads the risk management function for Oracle's Managed Cloud Services. This includes security strategy, security solutions, operational compliance, customer security services, audit compliance and delivery assurance. She is the former chief information security officer for PeopleSoft and former chief information security officer for J.D. Edwards.

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

A: Security leaders today are frequently advising senior management on information risk. Gone are the days when security people were only technicians who set the dials on who could access files or set firewall configuration to allow or deny traffic into the network. Then, security was seen as an IT issue. But today, businesses are more reliant than ever on technology to deliver products and services. Now, security is defending the enterprise from external cyberattack and enabling the business to continue functioning. With the frequency and magnitude of security breaches and the resulting business impact, the subject of information risk has moved to the board room.

This increased importance of information security led many enterprises to establish the role of the chief information security officer (CISO). Initially CISOs were very tactical and placed security goals above business goals. They became despised as they often objected to business goals as being insecure. They were called the ones who put the "no" in knowledge.

Today's CISOs need to broaden their technical skills to include business understanding. They need to communicate risk in business terms and help guide the balance of security risk and business strategy, knowing that there may be times when the company may accept more security risk in order to move the business forward.

Q: What leadership skills do you feel are critical for a woman to be successful in the field of information security?

A: First and foremost, you must be knowledgeable about information security, compliance and privacy. Your credibility as a leader depends on this.

You must also understand your business and your business strategy, and be organizationally aware—who are the leaders and what are their overall goals? With this information, you can use security as an enabler to help the business succeed and achieve its goals within an acceptable level of risk.

Also, successful security leaders are very good influencers—they are able to articulate risk in the language of the individual business and technology leaders. This skill helps get buy-in for the CISO's objectives.

Q: What do you think are the most effective ways to address the lack of women in the information security workspace?

A: We need to get in front of high school-age young women and communicate the opportunities that are available in this field as they contemplate their higher education options. Also, having a presence at large conferences through speaking opportunities or panels of women leaders can inspire women engineers or technical auditors to explore information security as an option.

Q: You took an unconventional road to the career field you have now. How did you arrive at a career in information security?

the network
She Leads IT

A: I graduated from college with a degree in computer science. I love problem solving and am a logical thinker, so it was the perfect fit for me. But being a developer sometimes required long or odd working hours. When I started a family, this became difficult. So I accepted a job as an IT auditor for a large local bank. I enjoyed using my problem-solving skills to look for weaknesses in systems.

After a number of years as an IT auditor, I was working for a large airline reservations systems company when the Internet began to be used to deliver services. The company was transforming from mainframes and hard-wired connections to distributed computing and, eventually, to Internet connections. The information security manager decided to retire and I was asked not only to step into that role, but also to remediate all the security issues I identified when I was their auditor.

A couple of years later, I was hired by J.D. Edwards to help form a security program. I was named the CISO in 2000. In 2003, J.D. Edwards was acquired by PeopleSoft and I was asked to stay on as the CISO for PeopleSoft, which was then acquired by Oracle in 2005.

Q: There is much discussion about the global cybersecurity skills gap. What do you think is the best way to encourage women to enter and remain in the field of cybersecurity?

A: This is such a fun and challenging profession—there are never two days that are the same. In some companies, it also provides opportunities to have flexible work schedules or work-from-home days that can help provide that work/life balance. However, keep in mind, it is a very high-stress career, and the time demands still exist, even with flexible work arrangements. It could still be challenging to start a family, but it may be easier now than it was when I started.

Cybersecurity is a profession that will continue to grow and expertise in this area will be highly sought after, which will drive up compensation.

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

A: It was a challenge to come into a new company as part of an acquisition and take on a leadership role. There was some skepticism among the ranks. I knew that I would need to establish my own credibility.

I asked a lot of questions and I listened to the answers. I shared what I was thinking and why with my team—then asked for their input. I made some hard and sometimes not-too-popular decisions, but I was able to explain my thinking with my management and my peers. And I made sure through influencing that my direct team was on board. I also made sure that stakeholders knew and understood the team's plans.

There were naysayers who said things had been tried before, but we did achieve success and the business benefited. And because of this success, the next undertaking was not quite as challenging—at least there were fewer naysayers.

www.sheleadsit.org

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

Cybercrime. The year-over-year growth is astronomical.

2 What is on your desk right now?

- A globe pinned with the places in the world I have traveled
- A basketball player's bobble head that has a picture of my son's face on the head
- An "art project" made of discarded/trash objects that my granddaughter made when she was in day care.
- A small plaque from United Airlines commemorating the million air miles that I have flown with them

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

Know your stuff, stay current with changing technologies, and understand your business and where it is headed.

4 What is your favorite benefit of your ISACA membership?

Being part of the Connecting Women Leaders in Technology program. I also appreciate the *ISACA® Journal* for keeping up to date on security concerns.

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

I am a huge Denver Broncos fan, so during football season, I follow the team and all their games. Otherwise, I spend my time with my family: my husband who also happens to be a CISO (you can imagine our dinner conversations), my six children and their spouses, and my eight, soon to be nine grandchildren.

Connecting Women Leaders in Technology

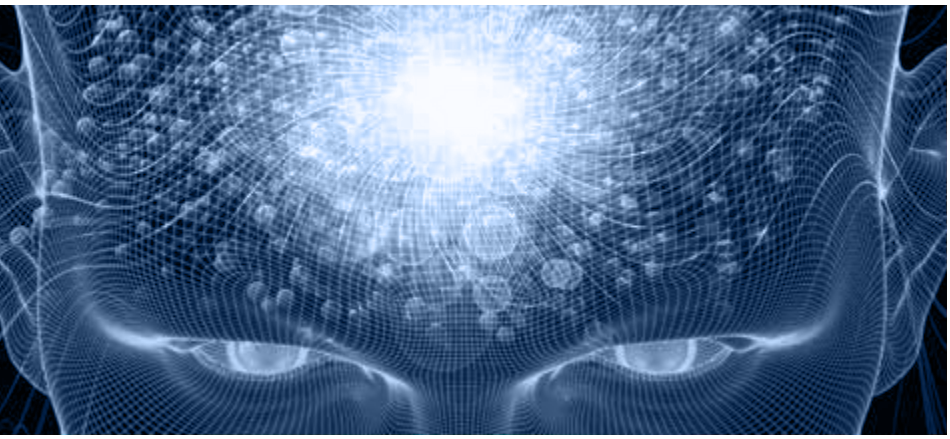
The Automation Conundrum

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

日本語版も入手可能
www.isaca.org/currentissue

"The computer is a moron. And the stupider the tool, the brighter the master must be," claimed Peter Drucker, in an often-quoted 1967 article.[1] Although this statement lends itself to a bit of hyperbole, the argument was clear and perhaps relevant at the time, because computers were only replacing clerical chores.

Fifty years later, artificial intelligence (AI) systems, riding on the exponential increases in computing power and the availability of big data, are outperforming humans in numerous domains. These intelligent systems continue to penetrate every industry sector and are delivering enormous benefits in the form of new business opportunities, deeper customer insights, improved efficiency, enhanced agility and so forth.



Phillimon Zongo
Phil Zongo is a cybersecurity consultant based in Sydney, Australia. He has more than 10 years of technology risk consulting and governance experience working with leading management consulting firms and large financial institutions. He has practical experience advising senior business and technology stakeholders on how to manage critical risk in complex technology transformation programs. He also authored "Managing Cloud Risk Top Considerations for Business Leaders," published in volume 4, 2016, of the *ISACA® Journal*.

US-based Memorial Sloan Kettering Cancer Center is using IBM Watson to compare patient medical information against a vast array of treatment guidelines, published research, journal articles, physicians' notes and other insights to provide individualized, confidence-scored recommendations to physicians.[2] In Canada, Bank of Montreal deployed robo-advisors to provide automated, algorithm-based portfolio management advice to its customers.[3] Massachusetts Institute of Technology (MIT) (USA) developed an AI system that can detect 85 percent of cyberattacks by reviewing data from more than 3.6 billion lines of log files each day and informing about anything suspicious.[4]

Adoption of AI systems is expected to accelerate over the next few years. A December 2015 report by Bank of America Merrill Lynch Research predicted that the robotics and AI solutions market will grow to US $153 billion by 2020—comprising US $83 billion for robotics and US $70 billion for AI-based analytics. The same report estimates that this exponential growth can boost productivity by up to 30 percent and cut manufacturing labor costs by 18 to 33 percent.[5]

While some organizations are still experimenting with AI using insignificant business tasks, others are taking ambitious strides by delegating mission-critical roles to AI algorithms. One such example is Deep Knowledge Ventures, a Hong Kong–based venture capital firm, which, in May 2014, took a leap of faith and appointed an AI algorithm to its board of directors.[6] The algorithm, named Vital, automates due diligence by scanning financing, clinical trials, intellectual property and previous funding rounds of prospective enterprises then votes on whether to invest in the enterprise or not; a role with significant responsibility and consequence.

The proliferation of AI raises intriguing opportunities; however, associated risk exists—and should it prevail, its impacts can result in significant consequences. A number of strategic concerns have been documented regarding the rise of AI; however, this article highlights three crucial risk

concerns that leaders face when adopting AI within their businesses and provides practical insights to minimize business exposure while maximizing AI potential. These risk concerns are:

- Critical business decisions based on flawed or misused AI algorithms
- Cultural resistance from employees whose roles are vulnerable to automation
- Expanded cyberthreat surfaces as AI systems replace more vital business functions

Flawed or Misused AI Algorithms

A well-designed AI system can significantly improve productivity and quality, but when deployed without due care, the financial and reputational impacts can be of epic magnitude. In banking and finance, flawed algorithms may encourage excessive risk taking and drive an organization toward bankruptcy. In the health care sector, flawed algorithms may prescribe the wrong medications, leading to adverse medical reactions for patients. In the legal sector, flawed algorithms may provide incorrect legal advice, resulting in severe regulatory penalties. In 2012, Knight Capital Group, a US-based market-making firm, provided an unsettling insight into the likely impacts of such risk when it lost more than US $440 million in just 30 minutes as a result of an untested change to its high-frequency trading algorithms. Dubbed “the mother of all software glitches,” the incident cost the firm four times its 2011 net income.[7]

In contrast to traditional rule-based systems where errors can be rolled back with minimum business impact, minor errors in critical AI algorithms can result in severe consequences. Further complicating this risk is the probability that AI systems can behave unpredictably when interacting with humans or the external environment. As intelligent systems increasingly take on vital business roles, the risk that crucial business decisions might be based on flawed algorithms invariably rises. Therefore, the need for the AI system concepts to match those of its human designers increases as the AI system becomes more powerful and autonomous.[8]

The three key critical steps that can help businesses to maximize AI value while managing risk are:

- Align AI adoption with business strategy and risk appetite
- Experiment with low-risk functions
- Test rigorously

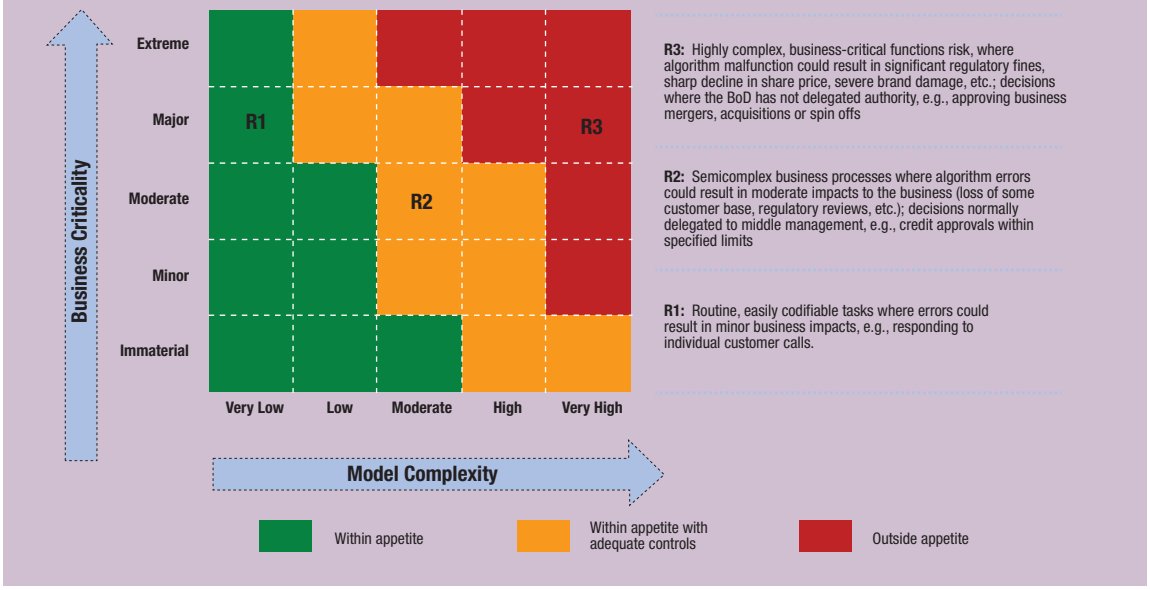
Align AI Adoption With Business Strategy and Risk Appetite

Business leaders should be mindful of key risk that is inherent in AI adoption, conduct appropriate oversight, and develop principles that articulate the business roles that can be partially or fully automated. Equally important, the board should approve the automation of high-risk business functions, ensuring that the business is not exposed to risk beyond its capacity or risk that does not contribute to the business strategy.

“In contrast to traditional rule-based systems where errors can be rolled back with minimum business impact, minor errors in critical AI algorithms can result in severe consequences.”

A simple way to conduct this assessment is illustrated in **figure 1**, which models risk exposure along two factors: criticality of the business function being automated and complexity of the associated model. In the example in **figure 1**, a financial institution may decide to automate some call center functions (R1) and avoid automation of business acquisition or spin-off approvals (R4), based on different risk exposures. Routine or clerical business roles are naturally easier to automate and pose less business risk compared to complex functions such as those requiring intellectual reasoning, creativity, interpersonal skills or emotional intelligence.

Figure 1—Risk Assessment for Business Process Automation



Source: P. Zongo. Reprinted with permission.

A clear understanding of regulations that govern specific business functions is also vital because full automation of some business functions might be prohibited in certain jurisdictions. For example, in April 2016, the Massachusetts (US) Securities Division published a policy statement in which the division questioned the ability of robo-advisors to act as state-registered investment advisers. The securities regulator stated, "It is the position of the Division that fully automated robo-advisers, as currently structured, may be inherently unable to carry out the fiduciary obligations of a state-registered investment adviser."[9] The division's argument was that a fully automated robo-adviser may not act in the best interest of its client, does not conduct sufficient due diligence, provides advice that is minimally personalized and may fail to meet the high standard of care.[10] This policy position underscores the importance of carefully considering the legal implications that are associated with automating a business function, including anticipated reforms, before committing any project capital.

An effective risk assessment requires business leaders to answer the following crucial questions:

- How can intelligent systems advance the enterprise business strategy and what does success look like?
- What are the plausible financial, reputational or regulatory risk if the AI system malfunctions, and does the business have enough capacity to absorb associated impacts if the risk materializes?
- What are competitors doing in this space, and how far have they advanced in pursuit of these goals?
- Is the business willing to take a leadership role or wait until the benefits of AI are fully proven?
- Does the organization have demonstrable expertise in managing the risk? If this is being outsourced, has the identified vendor successfully delivered AI transformation programs of similar or larger scale?

Although AI adoption introduces significant challenges, it can also be a catalyst for risk reduction. The first industrial robot, Unimate, created in 1961 by American inventor George Devol, was designed for that purpose. The 4,000-pound robotic arm transported die castings from an assembly line and welded these parts onto automobile bodies. This was a high-risk task for workers who could be poisoned by exhaust gas or lose a limb if they were not vigilant.[11] A similar, but more current, example is the IBM Watson system, which is being used by companies operating in heavily regulated industries to keep up with ever-changing legislation and compliance standards.[12]

Experiment With Low-risk Functions

Delegating a crucial task before attaining a solid theoretical understanding of the associated outcomes has high risk.[13] Therefore, organizations should experiment, learn and adapt using low-risk, low-cost and easily codifiable tasks. After the underlying assumptions are validated, competences are proven and major uncertainties are resolved, organizations can gradually automate more complicated functions.

Test Rigorously

Due to their high degree of uncertainty, intelligent systems require more extensive testing than traditional applications. When constructing intelligent systems that learn and interact with all complexities of reality, it is not sufficient to verify that the algorithm behaves well in test settings. Additional work is necessary to verify that the system will continue working as intended in live environments.[14] This testing should be performed by employees with appropriate qualifications and motivations. Likewise, detailed testing should be performed after the AI system has been modified, or after it has acquired new intelligence, and the conditions under which these tests are conducted should reflect a real-life environment.

Cultural Resistance

Any significant transformation program can be deeply unsettling for employees. AI programs amplify this risk, because employees whose jobs are vulnerable to automation—especially those performing less-skilled and repetitive tasks—may be worried about the fate of their jobs. Consequently, these employees may dig in to protect their turf and actively resist change, derailing AI program success. Revolts against innovation are not new. One of the most famous examples is the Luddite movement of the early 19th century, during which a group of English textile artisans protested the automation of textile production by seeking to destroy some of the machines.[15] Furthermore, lack of clear and consistent communication from leaders leaves employees open to confusion and distrust of important AI transformation programs.

> **“To successfully lead an AI transformation, business leaders must create an environment of trust and ensure high levels of employee engagement, buy-in and support.”**

A 2011 report emphasized that the “reshaping of employee attitudes and behaviours is just as critical to the success of a transformation as the implementation of process changes.”[16] To successfully lead an AI transformation, business leaders must create an environment of trust and ensure high levels of employee engagement, buy-in and support. To do this, business leaders should:

- Communicate a compelling change story that motivates employees and promotes a shared automation vision for the future
- Identify segments susceptible to automation; assess impact on employees and identify alternative job opportunities

- Establish a dedicated change management team consisting of senior business leaders, human resources, and change professionals to communicate the transformation agenda, anticipate challenges, and minimize attrition rates. Change management communications should also be targeted and allow for employee feedback.
- Identify opportunities for employees to work alongside AI systems and formulate strategies to maximize those synergies. Knowledge jobs generally consist of a range of tasks, so automating one activity may not make an entire position unnecessary.[17] For example, algorithms can perform routine tasks, freeing time for humans to manage customer relationships or derive deeper business insights. Also, highly regulated tasks might not be completely replaced by machines.
- Engage legal teams for due diligence to understand applicable job protection laws and appropriate responses if the program intends to completely automate some jobs
- Establish incentives to promote behavioral changes and keep people engaged

> **"The ability of AI systems to fully transform business hinges on the effectiveness of their security and privacy controls."**

Businesses will continue to automate tasks that were performed by humans to drive down costs, improve efficiency and reduce operational errors. Given the disturbing impact that automation can have on an organization's most valuable assets—its employees—it is essential for business leaders to anticipate potential risk early to minimize possible negative impacts. Employees also have a part to play: up-skilling themselves to remain relevant in the face of disruptive innovation. Researchers have predicted, "As technology races ahead, low-skill workers will reallocate to tasks that are non-susceptible to computerisation—i.e., tasks requiring creative and social intelligence. For workers to win the race, however, they will have to acquire creative and social skills."[18]

Expanded Cyberattack Surface

The ability of AI systems to fully transform business hinges on the effectiveness of their security and privacy controls. Failure to provide these assurances can inhibit their acceptance. The Bank of America Merrill Lynch Research report states that cyber security and privacy concerns, and other critical factors such as regulation, insurance and cost, remain primary hurdles to self-driving-car adoption. The report cites that 54 percent of buyers fear that connected cars will be hackable, and 30 percent do not want to use a connected car because of privacy concerns.[19] In 2015, a group of Virginia (USA)-based researchers successfully hacked into a driverless car system and took control of a vehicle, highlighting the significant threat posed by unsecured AI systems.

Cyberrisk continues to increase in frequency and business impact, and has gained significant attention from boards of directors, regulators and policy makers. Public and private-sector enterprises are already struggling to keep up with relentless, sophisticated and well-resourced cybercriminals. AI further complicates this struggle with the issues that are described in the following sections.

Vulnerabilities

To date, no industry standards exist to guide the secure development and maintenance of AI systems. Further exacerbating this lack of standards is the fact that start-up firms still dominate the AI market. A recent MIT report revealed that, other than a few large players such as IBM and Palantir Technologies, AI remains a market of 2,600 start-ups. The majority of these start-ups are primarily focused on rapid time to market, product functionality and high return on investments. Embedding cyberresilience into their products is not a priority.

Inadvertently, vendors ship solutions with basic security controls and easily exploitable vulnerabilities such as default passwords or weak authentication techniques. These weaknesses not only provide easy targets for cybercriminals to exploit, but also potentially refute layers of existing network security controls. The Verizon *2016 Data Breach Investigations Report* highlighted that 63 percent of confirmed breaches involved weak, default or stolen passwords.[20]

The self-learning capabilities of AI systems also present unique challenges. Cybercriminals might successfully predict the data that are used to train an algorithm and deliberately manipulate its behavior, contrary to its design objectives. The results of a recent Microsoft live experiment with an AI chat-bot, named Tay, offers a cautionary tale about the dangers of exposing vulnerable AI systems to the Internet. In March 2016, Microsoft admitted that it had made a critical oversight when a coordinated attack exploited vulnerability within its experimental AI algorithm. Tay was designed to mimic a teenage girl, interact with people on social media and learn from them. Unfortunately, Microsoft's oversight left Tay open to a specific vulnerability that was exposed by the attack and resulted in Tay sending wildly inappropriate, offensive and hurtful tweets and images, including racial slurs misrepresentative of Microsoft's values and Tay's design.

A Zero-sum Game

Intelligent systems are already playing a crucial role in combating cybercrime, for example, through automated fraud detection and spam detection. However, this role may prove to be a zero-sum game, because the same technology can be used to perpetrate highly sophisticated and evasive cyberattacks against critical systems. This sentiment was echoed by more than 75 percent of respondents who were polled in a 2014 survey that was jointly conducted by McKinsey and the World Economic Forum (WEF), including chief information officers (CIOs), chief risk officers (CROs), chief technology officers (CTOs), regulators and business unit executives, who conceded that the sophistication or pace of cyberattacks would grow faster than their own defensive capabilities.[21]

Therefore, an important question is: Will these malefactors continue to outsmart security vendors and develop superior and elusive AI programs that will unleash advanced persistent threats against critical systems, manipulate stock markets, perpetrate high-value fraud and consistently steal intellectual property, and, in doing so, destroy associated forensic evidence?

If current cybercrime trends continue unabated, residual business cyberrisk exposure may continue to rise.

Building Cyberresilient Intelligent Systems

To support business innovation and maximize its value, comprehensive cyberresilience for intelligent systems is vital. Unified efforts by policy makers, business leaders, regulators and vendors are a prerequisite for long-term success. However, before these concerted standards come to realization, business leaders should:

- Use existing, industry-accepted industry standards where possible. Although these are not specifically designed for intelligent systems, they can help businesses to identify common security risk and establish a solid baseline for securing new technologies. Notable frameworks include:
  - **Open Web Application Security Project (OWASP) Top 10**[22]—A list of the 10 most current critical web application security flaws, along with recommendations to ensure that web applications are secured by design.
  - **US National Institute of Standards and Technology (NIST) Cyber Security Framework**[23]—Consists of standards, guidelines and practices to promote the protection of critical cyberinfrastructure.
  - ***COBIT® 5 for Information Security***[24]—Provides detailed and practical guidelines for security professionals to manage and govern important information security, and make more informed decisions while maintaining awareness about emerging technologies and the accompanying threats.

- Engage experienced security consultants to review critical controls for AI products (including detailed penetration testing) and fix any exploitable security vulnerabilities before going live
- Conduct due diligence to determine vendor security capabilities, product security road map and frequency of security updates—with a long-term commitment to product security being a critical success factor

> **"In today's dynamic business environment, organizations need to experiment with new digital capabilities and accept risk in pursuit of new product offerings and to remain relevant to their customers."**

- Deploy robust encryption to protect sessions between AI systems and critical records from compromise (commonly referred as man-in-the-middle attacks)
- Grant minimum system privileges and deploy strong controls to protect service accounts that are used by AI systems to execute critical tasks from abuse—especially those with administrator—equivalent privileges
- Adopt defense in depth to ensure that a failure in one control layer will not result in a system breach

Conclusion

Looking ahead, numerous challenges remain for the full adoption of intelligent systems, like any emerging technology. These challenges may pale in comparison to the consequences of missing opportunities presented by AI.

In today's dynamic business environment, organizations need to experiment with new digital capabilities and accept risk in pursuit of new product offerings and to remain relevant to their customers. To do so, organizations need to align their innovation strategies with their risk appetite, anticipate major pitfalls and embed the right governance structures into transformation programs. For this to succeed, executive buy-in and oversight is paramount to AI success.

Author's Note

The author thanks Gina Francis, Innocent Ndoda, Shingi Muvenge, Kathleen Lo and Andrew Strong for their valuable feedback, which helped to improve this article.

Endnotes

1 Drucker. F. P.; "The Manager and the Moron," *McKinsey Quarterly*, 1967, *www.mckinsey.com/business-functions/organization/our-insights/the-manager-and-the-moron*
2 IBM Corporation, "Memorial Sloan-Kettering Cancer Center: IBM Watson Helps Fight Cancer With Evidence-Based Diagnosis and Treatment Suggestions," January 2013, *www-935.ibm.com/services/multimedia/MSK_Case_Study_IMC14794.pdf*
3 Alexander, D.; "Bank of Montreal Jumps Into Robo-Advising Ahead of Other Lenders," Bloomberg Technology, 18 January 2016, *www.bloomberg.com/news/articles/2016-01-18/bank-of-montreal-jumps-into-robo-advising-ahead-of-other-lenders*
4 Conner-Simons, A.; "System Predicts 85 Percent of Cyber Attacks Using Input From Human Experts," Massachusetts Institute of Technology,

USA, 18 April 2016, *www.csail.mit.edu/System_predicts_85_percent_of_cyber_attacks_using_input_from_human_experts%20*

5 Bank of America Merrill Lynch, "Thematic Investing: Robot Revolution—Global Robot and AI Primer," press release, November 2015, *www.bofaml.com/content/dam/boamlimages/documents/PDFs/robotics_and_ai_condensed_primer.pdf*

6 Wile, R; "Venture Capital Firm Just Named an Algorithm to Its Board of Directors—Here's What It Actually Does," *Business Insider*, 14 May 2014, *www.businessinsider.com.au/vital-named-to-board-2014-5*

7 Philips, M.; "Knight Shows How to Lose $440 Million in 30 Minutes," Bloomberg, 2 August 2012, *http://www.bloomberg.com/news/articles/2012-08-02/knight-shows-how-to-lose-440-million-in-30-minutes*

8 Sotala, K.; "Concept Learning for Safe Autonomous AI," Machine Intelligence Research Institute, 2015, *www.aaai.org/ocs/index.php/WS/AAAIW15/paper/download/10131/10137*

9 Massachusetts Securities Division, "Robo-Advisers and State Investment Advisor Registration," Policy Statement, 1 April 2016, *www.sec.state.ma.us/sct/sctpdf/Policy-Statement--Robo-Advisers-and-State-Investment-Adviser-Registration.pdf*

10 *Ibid*.

11 Mickle, P.; "1961: A Peep Into the Automated Future", *www.capitalcentury.com/1961.html*

12 Kelly, E.; "Computing, Cognition and the Future of Knowing How Humans and Machines are Forging a New Age of Understanding," IBM, 2015, *www.research.ibm.com/software/IBMResearch/multimedia/Computing_Cognition_WhitePaper.pdf*

13 Soares, N.; B. Fallenstein; "Aligning Superintelligence With Human Interests: A Technical Research Agenda," Machine Intelligence Research Institute, 2015, *https://intelligence.org/files/TechnicalAgenda.pdf*

14 *Ibid*.

15 Autor, H. A.; "Why Are There Still So Many Jobs? The History and Future of Workplace Automation," *Journal of Economic Perspectives*, 2015, *http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.3.3*

16 Aiken, C.; D. Galper; S. Keller; "Winning Hearts and Minds: The Secrets of Sustaining Change," McKinsey & Company, 2011, *www.ru.is/media/opni/frettir/Winning-hearts-and-minds-McKinsey.pdf*

17 Manyika, J.; M. Chui; J. Bughin; R. Dobbs; P. Bisson; A. Marrs; "Disruptive Technologies: Advances That Will Transform Life, Business, and the Global Economy," McKinsey Global Institute, 2013

18 Frey, C. B.; M. A. Osborne; *The Future of Employment: How Susceptible Are Jobs to Computerisation?,* 17 September 2013, *http://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf*

19 *Op cit*, Bank of America Merrill Lynch

20 Verizon, *2016 Data Breach Investigations Report*, 2016, *www.verizonenterprise.com/verizon-insights-lab/dbir/2016/?utm_source=pr&utm_medium=pr&utm_campaign=dbir2016*

21 Bailey, T.; J. Kaplan; A. Marcus; D. O'Halloran; C. Rezek; *Beyond Cybersecurity: Protecting Your Digital Business*, Wiley, USA, 2015, *www.wiley.com/WileyCDA/WileyTitle/productCd-1119026849.html*

22 The Open Web Application Security Project, "Category: OWASP Top Ten Project," 2016, *https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project*

23 National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," USA, 2014, *https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf*

24 ISACA®, *COBIT® 5 for Information Security*, USA, 2012, *www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx*

Phishing Detection and Loss Computation Hybrid Model

A Machine-learning Approach

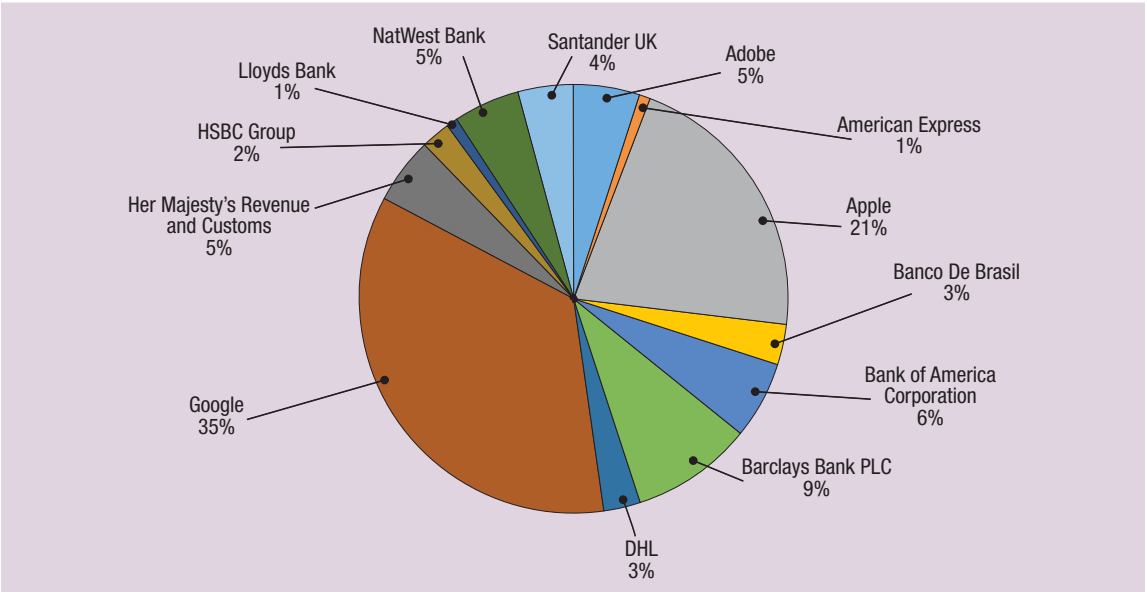
Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Phishing involves social engineering of data over the Internet to acquire personal or business information from unsuspecting users. The 2015 Internet Crime Report from the US Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) states that chief executive officer (CEO) email scams, also known as business email compromise (BEC), cost US firms US $246 million in 2015. Affected firms have reported more than 7,833 BEC complaints to the FBI IC3.[1] In contrast, identity and credential theft costs were lower, at USD $57 million, with 22,000 reported cases in 2015.

Phishing attacks are aimed at naive users to trick them so they unintentionally divulge critical information, such as usernames; social network passwords; and banking, financial and credit card details. Phishing attackers use spam emails, corrupt web URLs and multimedia messages to target users and lure them to fake web pages. For example, Dridex phishers sent targeted emails that had malware attached in the form of Microsoft Office macros to users in English-speaking nations in efforts to steal their banking credentials.[2] **Figure 1** shows the top targeted firms in 2016 from various industries.[3]

In light of these events, a hybrid model can be considered to compute the probability of a URL being malicious and the expected loss for the first

Figure 1—Percentage Share of Top Targeted Firms Based on PhishTank Archive in 2016



Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

Baidyanath Biswas
Is a Ph.D. student in information technology and systems at the Indian Institute of Management (Lucknow, India). His research interests are privacy and risk issues in information systems, the economics of cyber security, and health care IT. He has worked as a senior software engineer for nine years with Infosys, IBM and Cognizant. He can be reached at fpm15005@iiml.ac.in.

Arunabha Mukhopadhyay, Ph.D.
Is an associate professor in information technology and systems at the Indian Institute of Management (Lucknow, India). He is the recipient of the Best Teacher in Information Technology Management Award in 2013 and 2011, and the 19th Dewang Mehta Business School Award. He can be reached at arunabha@iiml.ac.in.

24 hours after the phishing attack. The model also offers a set of strategies to help the C-suite make policy-level decisions and frame organizational security policies to minimize losses due to such phishing attacks.

Proposed Hybrid Model for Phishing Detection and Loss Computation

Figure 2 describes the hybrid model for phishing detection and loss computation for firms that regularly face phishing attacks. The hybrid model consists of three modules:

- Risk analysis to calculate the probability of a prospective URL that can lead to a phishing attack
- Loss computation to estimate the expected loss to stakeholders after the phishing attack
- Risk mitigation to offer techno-social recommendations to minimize losses arising from such an attack

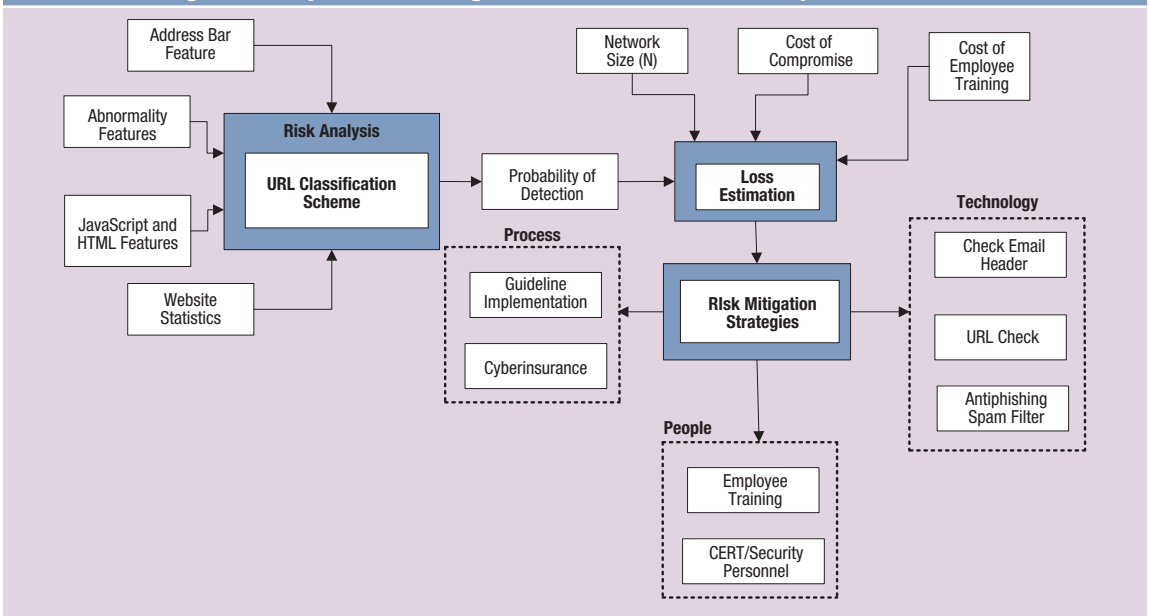
What Are Machine Learning Techniques?

Machine learning techniques consist of pattern recognition from data and learning algorithms that apply to practical applications such as intrusion detection systems (IDS) and antispam and antiphishing filters. **Figure 3** provides a schematic view of the classification and regression tree (CART)-based model that generates rules that apply to the data set of legitimate and corrupt websites. The CART uses the Tree Bagger method to ascertain the importance of the variables. Unknown URLs are predicted as legitimate or suspicious using the classifier and its rule set.

Bagger Algorithm for Decision Tree

Bootstrapping aggregation, also known as bagger, is an ensemble technique used in the CART algorithm. It generates multiple prediction trees and combines each model to improve accuracy and

Figure 2—Hybrid Phishing Detection and Loss Computation Model



Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

reduce overfitting the original classifier. The input data are generated by randomly choosing records with replacement from the original training set. The error of the model is used as an estimator for the importance of a predictor variable. An ensemble model will have higher model error if the majority of the predictor variables are influential and *vice versa*.

Data

Google and Alexa Top 500 website rankings offer a list of legitimate sites.[4] Phishing sites that report through MillerSmiles and PhishTank archives deliver the malicious URLs.[5] The predictor variables in the data set are encoded:

+1 = legitimate URL

0 = suspicious URL

-1 = phishing URL

The target variable is encoded -1 for phishing and +1 for legitimate websites. Training and testing are performed in 80:20 ratios, with 8,844 records for testing and the remaining 2,211 for training.

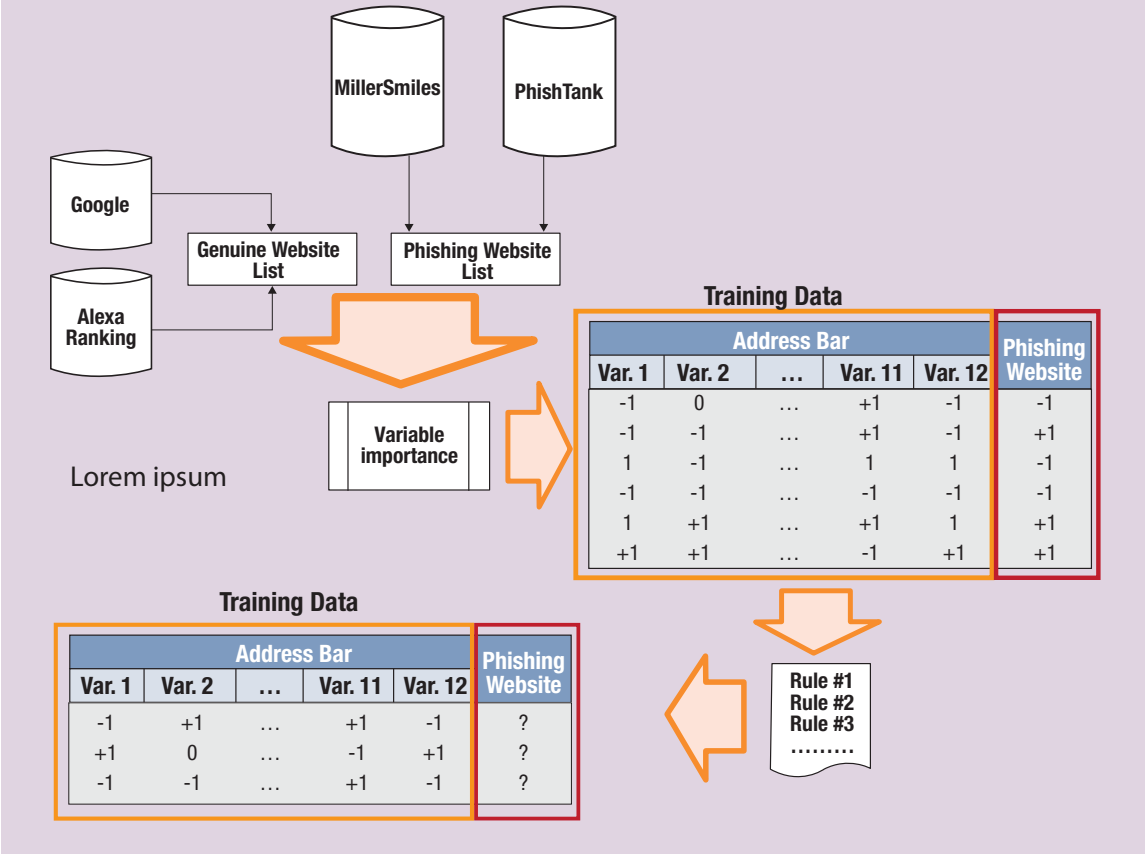
Methodology for the CART-based Hybrid Classifier

Figure 4 illustrates the steps of the CART-based hybrid classifier that focuses on the training data to create a rule set and run test data, as in **figure 3**. The classifier uses a bagger algorithm to create a list of the most significant variables from the total training set of the 30 encoded predictors.

Identifying the Most Significant Variables

In the experimental data set,[6] there are 30 input variables, broadly categorized as address-bar

Figure 3—CART-based Phishing URL Classifier and Ruleset Generation



Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

Figure 4—Steps to Implement CART-based Hybrid Classifier	
Step 1	Load the list of legitimate URLs based on website ranking (data set D1).
Step 2	Load the list of phishing and suspicious websites (data set D2).
Step 3	Load the input file after combining the two data sets (D1, D2).
Step 4	Identify the most significant predictor variables using the CART-based hybrid classifier algorithm.
Step 5	Train the Tree Bagger using the significant predictor variables only.
Step 6	Test with out-of-sample data and measure the accuracy of the CART-based hybrid classifier.

Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

properties, abnormality features, HTML and JavaScript features, and website statistics.[7] **Figure 5** shows the plot of importance based on out-of-bag features for all 30 variables. The plot also indicates the top five significant variables in order of their importance, which are #8 (HTTPS in URL), #14 (URL of anchor), #26 (website traffic statistics), #15 (links in <Meta>, <Script> and <Link> tags) and #7 (URL subdomain). The classification technique generates rule sets based on all/some of these significant predictors only.

Figure 6 illustrates the general website URL-based predictor variables for probable phishing links and their attributes of identification.

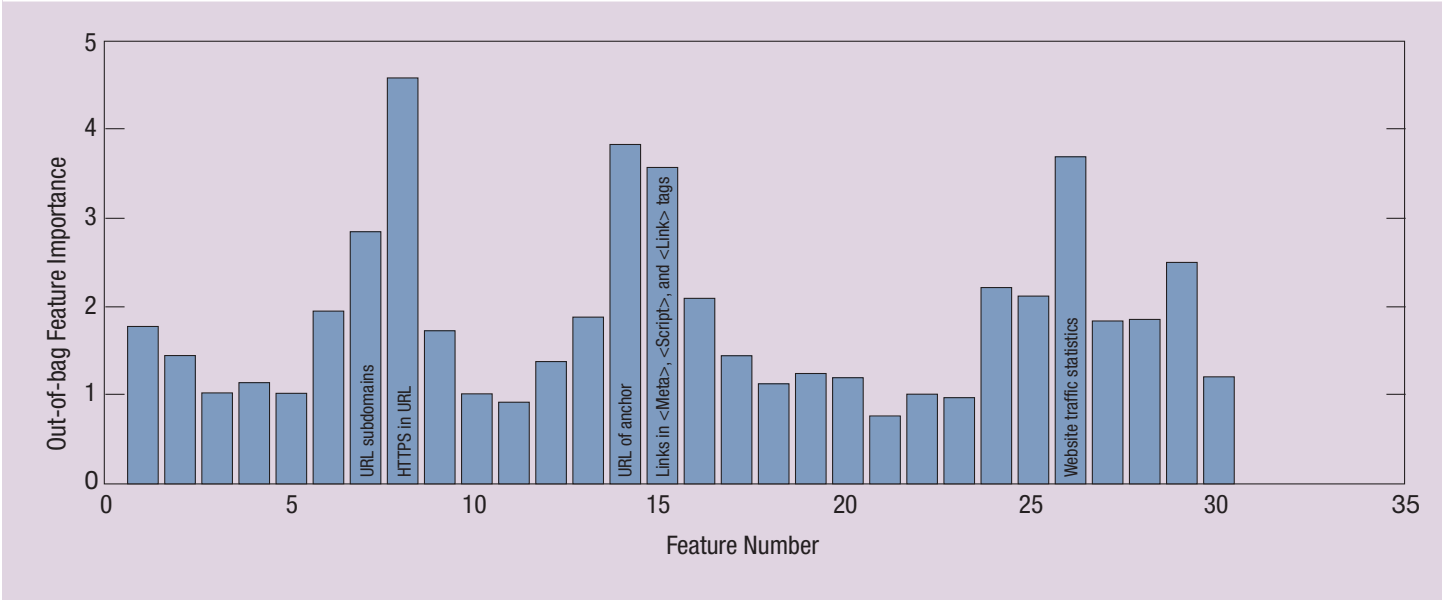
Loss Computation for Firms After a Phishing Attack

Consider a corporate network of N = 10,000 users, and assume that the network traffic saturates as more users join in following a logistic diffusion curve.[8] **Figure 7** illustrates the multiple stages of a phishing attack and the probability of user decisions and actions.

The stages are:

- Attackers spam the network with infected emails.
- Attackers wait for a naive user to open the infected email.
- Users read the email(s).

Figure 5—Variable Importance for All Phishing Predictors



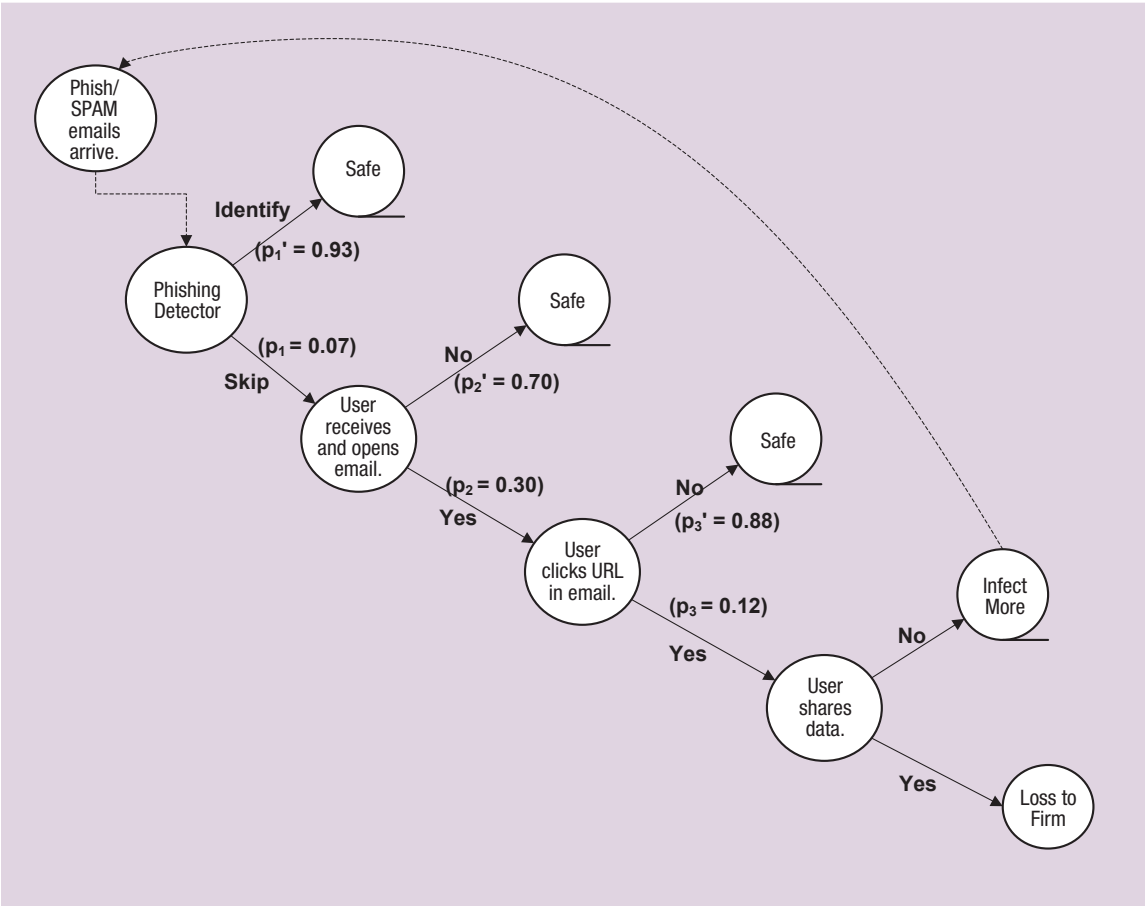
Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

Figure 6—Common URL-based Features in Phishing URLs

Feature	Example Link (Source: PhishTank Archive)
Redirect Using //	*http://www.tasteofthewest.co.uk/images//wsecure/ap5c/*
Extremely Long URL	*https://docs.google.com/a/valpo.edu/forms/d/17zrMsBmbTzz4tvu3VqcXM3huxNwnxfeyuU0Bc9iTKZc/viewform?usp=send_form*
@ Symbol in the URL	*http://imessage-audits.org/profile/?email=abuse@example.com*
HTTPS (Hypertext Transfer Protocol with Secure Sockets Layer)	*https://accounts.google.com/ServiceLogin?continue=https://drive.google.com/st/auth/host/0Bz9pzRUAjfXaT3RXengxQXV3dlU/*
- Separator	*http://irstax.wap-ka.com/index.xhtml*
Sub/Multisub Domains	*http://www.grandimperial.com.my/v2/en/*
Nonstandard Port	*http://www.belcotech.com:32000/mail/wait.html*
IP Address in the URL	*http://194.78.154.195/CFIDE/services/labanquepostale.html*
HTTPS within URL	*http://www.roma.md/templates/system/https:/www2.itau.com.br/atendimento/*

Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

Figure 7—Process Flow Diagram for User Action(s) After Phishing Attack



Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

- Users click on the malicious URL.
- Users share their credentials through the fraudulent URL.[9]

The following equation gives the loss per hour after the phishing attack:

> Loss per hour = N (size of the network) * (Number of skipped URLs) * Prob (open_email) * prob (click_URL) * prob (share_ info) * (monetary impact of phishing)

Results

Figure 8 shows that out of 980 test records of phishing URLs, the classifier can pick up 876 records with a phishing URL, with a true positive (TP) rate of 89.29 percent [876/(876+105)]. The model-identified good websites are at a true negative (TN) rate of 94.24 percent [1,179/(1,179+72)]. The classifier works with an overall accuracy of 92.94 percent [(876+1,179)/2,211] in predicting phishing and legitimate websites. Out of 100 test URLs assigned to the rule-based model, 93 URLs were marked as legitimate, suspicious or phishing. Therefore, the probability of correctly identifying a phishing website is 0.9294 for the hybrid model described in **figure 2**.

The following example demonstrates loss computation. In 2016, a payment card firm was targeted by 29 percent of 1,000 URLs, which equals 290 phishing URLs. Out of this 29 percent, the probability of successful prediction by the classifier is 92.94 percent, and the dilemma of decision making for the firm's management may arrive from the remaining 7.06 percent of 290 URLs, which is approximately 21 URLs. In the next step, the estimated loss is calculated from the equation described previously.

Calculation for Expected Loss

1. The accuracy of the classifier: 92.94 percent (calculated)
2. Phishing URLs that may skip the filter: 1-92.94 percent = 7.06 percent
3. Out of 1,000 URLs sent in total, a firm targeted in approximately 29 percent of the cases received 29 percent of 1,000, which equals 290 URLs.
4. Combining (2) and (3), total phishing URLs that skip the filter are 7.06 percent of 290 = 21.
5. Given the probability of opening email equals 30 percent, probability of clicking URL equals 12 percent and probability of sharing info equals 12 percent. Average monetary impact of phishing in financial industry equals US $264.[10] Substituting values into the equation, the cumulative loss per hour = (N) * 21 * 30% * 12% * 12% * $264, where N increases exponentially with network diffusion rate equals 0.2, and total strength of the network equals 10,000.
6. The hourly calculation is shown in **figure 9** (also indicated by the blue graph in **figure 10**).

Based on the exponential rule of diffusion, after the users start clicking on the phishing URLs, the network starts blocking these sites. Gradually, the system is saturated and the phishing attackers cannot extract much of a financial impact and, thus, the loss begins to reduce. The nonlinear and diminishing nature of the loss curves (**figure 10**) attributes to this phenomenon. With a high probability state of {open, click, share} = {0.50, 0.20, 0.20}, the loss is greater than that of the medium state, which is {0.40, 015, 0.15}, and that of the low state, which is {0.20, 0.10, 0.10}.

Figure 8—Confusion Matrix for Classification Based on URL Predictors

	Predicted: Phishing		Predicted: Genuine	
Actual: Phishing	876	**TP**	105	**FN**
Actual: Genuine	72	**FP**	1179	**TN**

TP = true positive FP = false positive TN = true negative FN = false negative

Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

Figure 9—Calculation for Expected Loss

Time (in Hours)	Hourly Network Strength	Cumulative Loss (US Dollars)	Loss Per Hour (US Dollars)
1	5,498	128,387	11,407
2	5,987	139,794	10,967
3	6,457	150,761	10,348
.....	.....	.....	.....
.....	.....	.....	.....
24	9,918	231,595	417
25	9,933	231,939	343
26	9,945	232,220	281

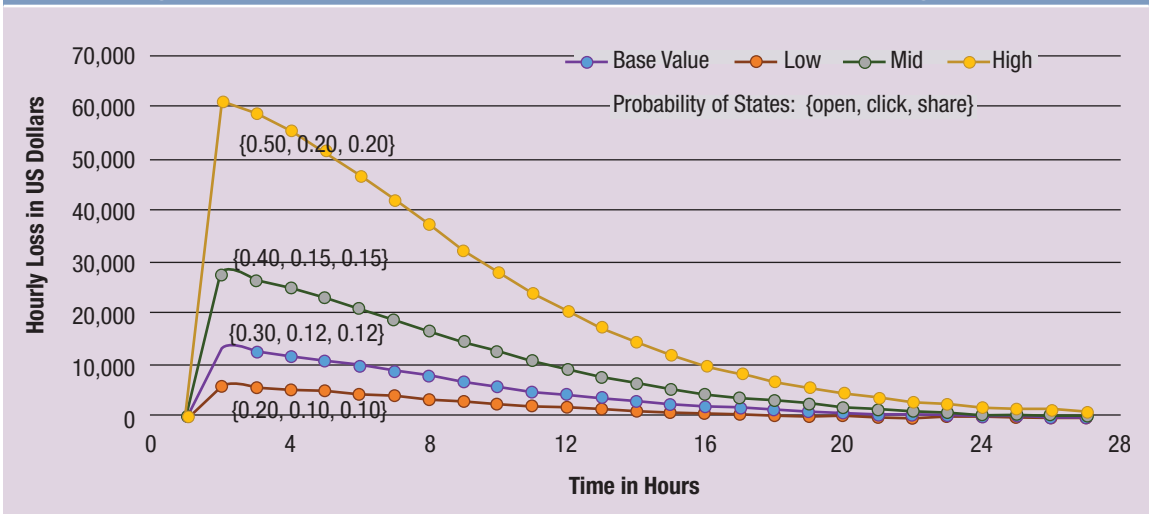
Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

Risk Mitigation Strategies

Figure 11 shows that when mitigation strategies (people, process and technology) are low, the measured financial impact of phishing attacks is highest. When the mitigation plan is high for all the factors (people, process and technology), the loss due to phishing minimizes.

Risk reduction should begin with technology tools, for example, software checks for suspicious emails and web pages, and installing antispam and antiphishing filters across the network. Top management executives such as chief information security officers (CISOs) and chief technology officers (CTOs) should readily implement stringent security guidelines and system processes in the organization to be able to identify such scenarios. Appropriate training organized by human resources executives should follow so that employees remain cognizant of the behavior of phishing attacks and their categories. Organizations should maintain computer emergency response teams (CERT) and system administrators for their corporate networks to accurately scan assets and encourage employees to abide by the guidelines.

Figure 10—Expected Loss for the First 24 Hours After a Phishing Attack



Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

Figure 11—Multilevel Mitigation Strategies and Loss Levels

Level of Phishing / Mitigation Strategy	Base Values (Verizon DBIR 2016)	Low-impact Phishing	Medium-impact Phishing	High-impact Phishing
People		High	Middle	Low
Process				
Technology				
Prob. (Open)	30%	20%	40%	50%
Prob. (Click)	12%	10%	15%	20%
Prob. (Share)	12%	10%	15%	20%

Source: B. Biswas, A. Mukhopadhyay. Reprinted with permission.

Conclusion

The three-level model proposed in this article can be used to compute the probability of phishing through corrupt URLs and the expected loss during the first 24 hours after an attack. This article presents multitier recommendations against phishing attacks for broad categories of businesses and their employees. The classification scheme (**figure 3**) considers significant variables to predict the target class—phishing or legitimate websites. The associated probability of the classifier is then applied to compute the estimated loss (**figure 8**) through a period of 24 hours, immediately after the firm has suffered a phishing attack. Recommendation strategies for people, process and technology should be applied in sync with each other so that the estimated loss arising due to phishing attacks is lessened.

Endnotes

1 Department of Justice, Federal Bureau of Investigation, "2015 Internet Crime Report," Internet Crime Complaint Center, USA, *https://pdf.ic3.gov/2015_IC3Report.pdf*

2 O'Brien, D.; *Dridex: Tidal Waves of Spam Pushing Dangerous Financial Trojan*, Symantec, 2016, *www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf*

3 APWG, *2016 APWG Phishing Attack Trends Reports*, 2016, *www.antiphishing.org/resources/apwg-reports/*

4 Alexa, "The Top 500 Sites on the Web," *www.alexa.com/topsites*

5 PhishTank Archives, *https://www.phishtank.com/developer_info.php*

6 Lichman, M.; "UCI Machine Learning Repository," 2013, *http://archive.ics.uci.edu/ml/*

7 Mohammad, R. M.; F. Thabtah; L. McCluskey; "Predicting Phishing Websites Based on Self-structuring Neural Network," *Neural Computing and Applications*, vol. 25, iss. 2, 2014, p. 443-458, *http://eprints.hud.ac.uk/19220/3/RamiPredicting_Phishing_Websites_based_on_Self-Structuring_Neural_Network.pdf*

8 Ransbotham, S.; S. Mitra; "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," *Information Systems Research*, vol. 20, iss. 1, 2009, p. 121-139

9 Verizon Enterprise, *2016 Data Breach Investigations Report*, 2016, *www.verizonenterprise.com/verizon-insights-lab/dbir/*

10 Ponemon Institute, *2016 Cost of Data Breach Study: United States,* 2016, *www-03.ibm.com/security/data-breach/*

University of San Diego®

POWER YOUR CAREER

MASTER'S IN CYBER SECURITY OPERATIONS AND LEADERSHIP

Cyber crime is on the rise and today's employers are looking for tech-savvy people to combat online criminals. Prepare yourself for these growing opportunities by earning your Master's in Cyber Security in 20 months and join the fast and exciting world of Cyber Security.

- Top 100 nationally ranked university
- Curriculum dedicated exclusively to critical aspects of cyber security
- Immersive and unique career-building education
- 100% online: flexibility for busy professionals
- Complete the degree in 20 months

BECOME A CYBER SECURITY LEADER

USD offers an on-campus Master of Science in Cyber Security Engineering

» (619) 260-4580 | (888) 832-0239
» CyberOps.SanDiego.edu

sponsored feature

Ravid Circus
Is vice president of products at Skybox Security

SKYBOX™ SECURITY

Indicators of Exposure and Attack Surface Visualization

It is undeniable that IT systems have become enormously complex, and they continue to be influenced by rapid changes that are redefining networks, such as deperimeterization, mobile devices, virtual environments, Software as a Service (SaaS) and the Internet of Things (IoT). This growing complexity is occurring in an environment where resources are limited and regulatory requirements are forcing senior management to demand more information, leaving security practitioners scrambling to communicate the state of their security across departmental silos and to business executives and the board.

Enterprises need to think of their entire network infrastructure—physical, virtual and cloud—in the same way that attackers do: a very large, diverse and geographically dispersed attack surface (all the ways in which IT systems and networks are vulnerable to attack). All too often though, security practitioners have no means of viewing the attack surface that they are protecting in its entirety; therefore, they rely on a dangerously narrow perspective to identify, prioritize and remediate that which they believe are critical vulnerabilities. Typically, these tasks are done in crisis mode and with little context of precisely how those vulnerabilities may or may not pose an actual threat.

This narrow perspective is changing with the emergence of visualization tools that give security practitioners unprecedented views of their attack surface and subsequently greater insight into how to best address threat exposures that put enterprises at risk. Such tools combine attack path modeling with advanced threat reporting (the ability to correlate threat intelligence with vulnerabilities found in the enterprise) and analytic engines that automatically prioritize vulnerabilities and generate alerts. This article describes the foundation of such tools and the concept of indicators of exposure (IOEs) as the critical underpinning of attack surface visualization.

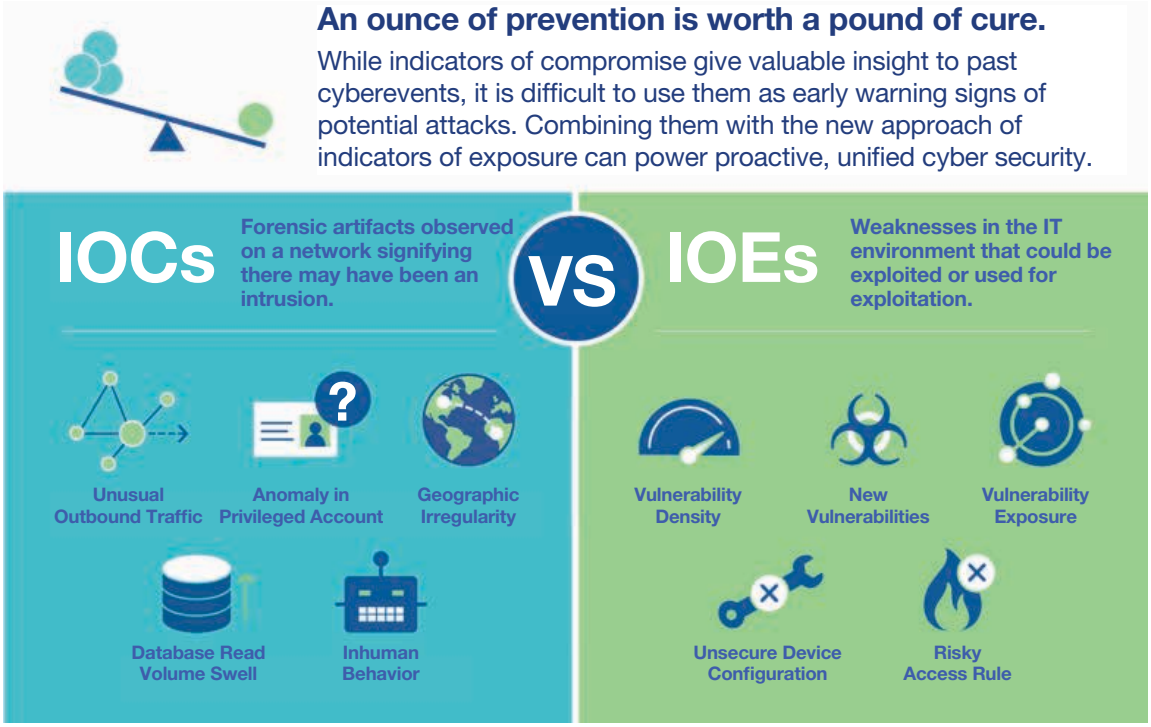
Understanding Indicators of Exposure—The Ounce of Prevention

Since the emergence of the Google Aurora attack in 2010,[1] advanced persistent threats (APTs) have dominated cyber security headlines, making security practitioners ever more aware that attacks against their networks are no longer a matter of if, but when. Security teams have quickly expanded their use of attack detection tools that are armed with advanced capabilities to identify indicators of compromise (IOCs) and used to mount a rapid response to limit damage.

As Benjamin Franklin said, “An ounce of prevention is worth a pound of cure.”[2] IOCs can be used to identify the hallmarks of attacks in progress, such as unusual outbound traffic, anomalies in privileged accounts and geographic irregularities. Certainly, tools to detect and respond to IOCs have their rightful place in any security tool kit, but a singular focus on detection and response can take security attention (and budget) away from the proactive measures that reduce the chance of an attack occurring in the first place. If security leaders maintain such a narrow focus on IOCs and do not have a strategic plan in place for minimizing the factors that can lead to them, then the enterprise will forever be in firefighting mode.

IOEs are the factors that can lead to an attack and should be identified alongside IOCs. IOCs represent an artifact of an attack; IOEs highlight the preconditions that make an exploit more likely (**figure 1**). By combining IOEs into a single, dynamic

Figure 1—Indicators of Compromise vs. Indicators of Exposure



Source: R. Circus. Reprinted with permission

view, security practitioners gain the advantage of access to a comprehensive representation of their enterprise attack surface. This level of attack surface visibility and analysis of the IOEs that contribute to it constitute a game changer for security managers and chief information security officers (CISOs).

Identifying Indicators of Exposure

IOEs describe security weaknesses that are particular to an enterprise network and can be exploited by an attacker. It is not enough to only catalog a list of vulnerabilities. Consideration must be given to those vulnerabilities that are not only exposed to a potential attack, but also put key assets at risk. IOEs are determined by analyzing multiple factors, i.e., events as opposed to observing a single one. An unexpected firewall rule change is an event, but an unexpected firewall rule change that opens up an access path to a critical asset is an IOE. By linking together IOEs with an understanding of network topology and assets, enterprises can discern which attack vectors are most likely to be exploited in a multistep attack.

Working with identified IOEs rather than raw vulnerabilities and other risk data also allows security teams to use the power of contextual analysis to determine actions that will significantly reduce the size of their attack surface with less effort than a “fix everything” approach.

A Working Set of IOEs

Research shows that most attacks exploit known vulnerabilities where a patch has been available for months or even years.[3] In addition, a variation of the 80-20 rule is in effect for vulnerabilities. The top 10 vulnerabilities accounted for 85 percent of successful exploit traffic, while 900 different vulnerabilities accounted for the remaining 15 percent.[4]

Attack risk tends to cluster around common exposure factors, which can be grouped into five of the most prevalent IOEs:

- Vulnerability exposure encompasses all vulnerabilities that are exposed and can be used in an attack vector. Contributing factors include vulnerability assessment, network context and security controls. Vulnerability exposures are ranked by risk and exposure level. Direct exposures are ranked ahead of second-step exposures. Vulnerability exposure contains an advantage over a standard Common Vulnerability Scoring System (CVSS)-based ranking, which does not account for unique network context or potential for multistep attacks.
- New vulnerabilities are all vulnerabilities that were identified in the past 30 days and ranked by risk. Contributing factors include vulnerability assessment, threat intelligence and time. It is worth noting that 59 percent of enterprises scan every 30 days (or less frequently), so recent vulnerabilities are more likely to be unpatched and available to exploit.[5]
- Vulnerability density is a high concentration of vulnerabilities in a particular network area and indicates an increased likelihood that an adversary will attempt repeated attacks on several of those vulnerabilities to achieve a successful breach. Contributing factors include vulnerabilities, vulnerability severity and network asset groups. Vulnerability densities can also indicate that security managers need to scrutinize the vulnerability remediation process in a particular area.
- Unsecure networking or security device configurations include networking or security device configurations that violate policy or create security gaps. Contributing factors include violations, severity and network asset groups. This IOE is ranked by the severity of the configuration policy violations, using the highest-severity configuration policy violation in each network asset group.
- Risky access rules in firewalls and networking devices encompass a variety of rules in firewalls or networking devices that could allow attackers to reach critical assets. Contributing factors include access violations, network device rule violations and access path analysis. This IOE is ranked by highest severity and number of violating rules.

The list of possible IOEs can be expanded to include commonly employed attack techniques and their combination of factors that are likely to lead to exploit.

Role of IOEs in Attack Surface Visualization

Understanding the nature and location of possible exposures is key to understanding the attack surface. Unfortunately, at any point in time, an enterprise can have hundreds of thousands of IOEs to manage, and that amount of data quickly becomes overwhelming. Therefore, prioritization and coordination of limited resources are critical.

Enterprises need a means of consolidating and analyzing data from dozens of security controls and other sources to create a visual, interactive model that links network topology, network connections, business units and organizational hierarchy, i.e., an attack surface visualization tool with IOEs. With such visualization, senior management and technical security teams can more easily understand the security posture of the enterprise and make more informed decisions.

At the highest level, IOEs should be viewed in a simple, representational picture of the attack surface that is mapped to geography, business units, asset types or other logical structures. Different types of users are able to view the data in the manner most appropriate to their needs. For example, a security team that is responsible for manufacturing operations views a map consisting of the enterprise factories, while a team that is responsible for regional data centers views geographic locations or network architecture. Trending information should also be available for each view, giving security leads important information about the progress that has been made in alleviating risk exposures for a specific aspect of the network.

Attack surface visualization can also help tremendously in security management of cloud

or hybrid IT environments where it is even harder to evaluate the interaction of the virtualized components with the physical world. For a complete picture of the attack surface, security information must be integrated from physical and virtual environments, and from cloud services. Security visualization shows the applied policy within virtual networks, analyzing access into and out of the network (north-south traffic), and access within the virtualized data center (east-west traffic). This visualization can also ensure that policies within the virtualized environment align with policies covering the rest of the network. As an example, contextual analysis of the east-west movement of data must be readily available to control access to, for example, financial data, which may need to be managed differently from manufacturing data.

Role of IOEs in Prioritizing and Remediating Risk

With any large data set, prioritization is critical when evaluating early signs of security weaknesses. Customized filters are beneficial for focusing the efforts of security teams on severity levels above a specific threshold or on specific types of IOEs. This focus avoids the risk of too many false positives, which cause individuals to waste their efforts chasing unprioritized alerts instead of addressing the truly serious issues. In addition, vulnerabilities should be assessed beyond the one-dimensional critical or medium severity ranking. A critical vulnerability might be effectively neutralized in a relatively easy manner through modifications in configurations and existing security controls, while a medium vulnerability on a business-critical asset and behind a misconfigured firewall can create a dangerous exposure to attack. The context of vulnerabilities in relation to the business is key. Security practitioners should always use contextual analysis to determine the existence of a vulnerability and its importance, considering the possible exposure of key enterprise assets or information, under a variety of compliance regulations such as the US Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Payment Card Industry Data Security Standard (PCI DSS) and the European Union General Data Protection Regulation (GDPR).

Finally, to turn high-level analysis into remediation action, an attack surface visualization tool should enable a user to easily and intuitively drill down from the attack surface view to greater levels of granularity where the user can fully evaluate potential actions. For example, a security manager identifies hot areas of the network when viewing vulnerability density at the highest level and then drills down to understand the set of vulnerabilities that are the greatest contributors to those hot spots. The user then zooms in further to identify the individual hosts or devices and actions that will have the greatest impact on vulnerability density.

Figure 2 shows how IOCs and IOEs are used in the attack life cycle.

Zero-day Attack Scenario

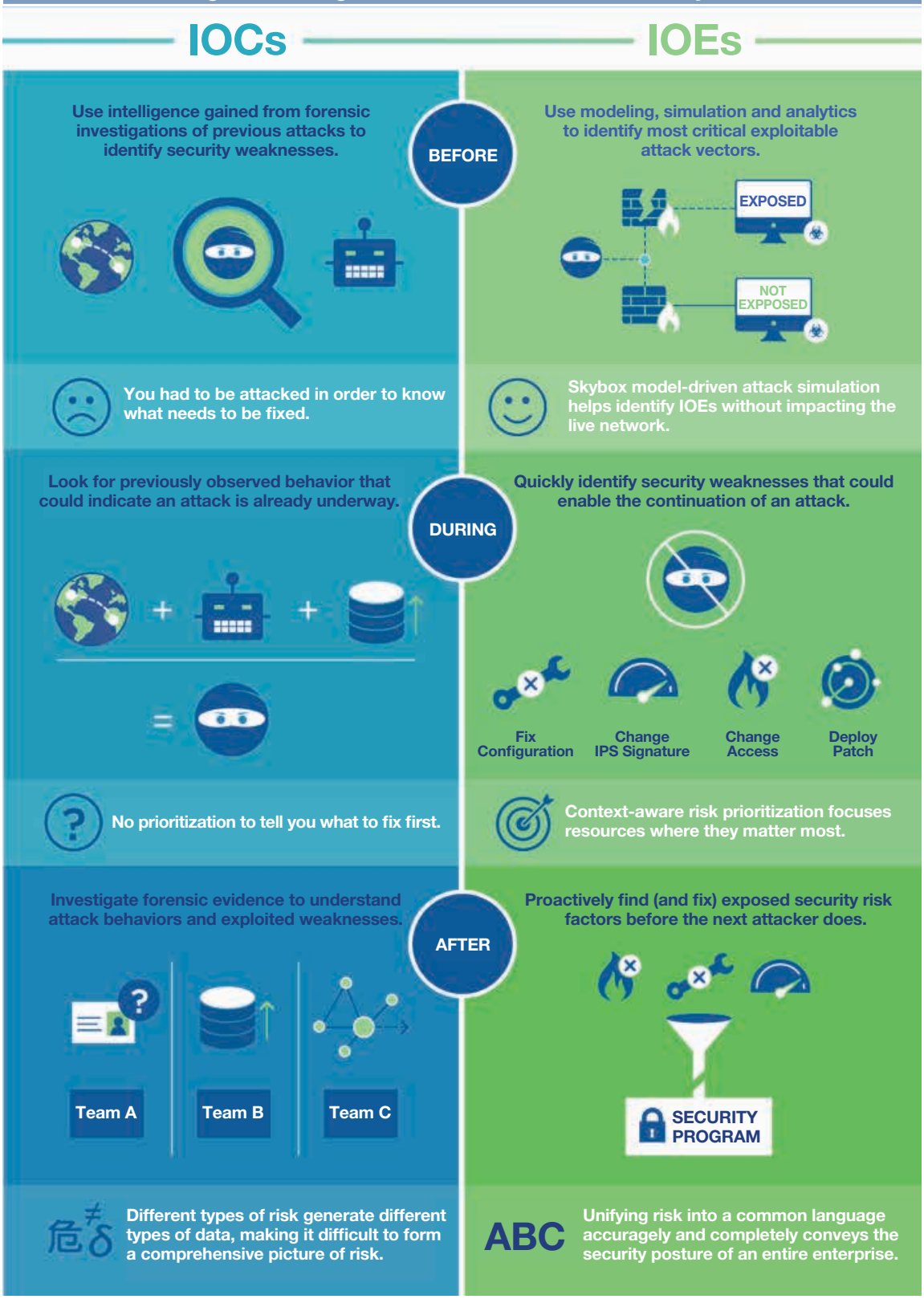
When discussing IOEs, it helps to place them in the context of a real-world scenario. To illustrate, take zero-day attacks, in which time is of the essence. Security teams must identify vulnerable hosts within minutes and neutralize attack vectors immediately. The 2016 news reports describing the simultaneous exposure of network vulnerabilities that were discovered by the US National Security Agency (NSA) and the malware code that was needed to exploit those vulnerabilities highlight the need for quick action.

The following timeline is an example of such a zero-day situation for an enterprise using an attack surface visualization tool with IOEs:

1. Zero-day vulnerability is announced. Immediate knowledge of susceptibility is required, so a real-time attack surface model is pulled up.
2. IOEs are updated in minutes through a reanalysis rather than a rescan of the network, which can take days to complete.
3. Filters are applied to identify only those IOEs containing the newly discovered vulnerability.
4. The ability to drill down to the host or device level provides security teams with the precise information that they need to perform the necessary remediation.

The assets that are most exposed to the attack can be attended to as highest priority. The attack that could threaten the livelihood of an enterprise can be quickly and effectively thwarted.

Figure 2—Using IOCs and IOEs in the Attack Life Cycle



Source: R. Circus. Reprinted with permission

The Network Security Pendulum

For years, the pendulum of network security has swung between the extremes of prevention and reaction. A happy medium that incorporates both is needed. Such an approach combines close attention to IOCs with close attention to IOEs—because simply knowing that security has been compromised is no longer enough. Security practitioners must be able to redress attack vectors before they can be exploited. A complete understanding of the attack surface is fundamental to both, requiring a solution that combines an intuitive, visual representation at every level with the ability to drill down into specific assets and the vulnerabilities within those assets. Attack surface visualization tools with IOCs and IOEs provide this solution.

Endnotes

1 Ayers, P.; "Cybersecurity: Issues and ISACA's Response," lecture, Jacksonville ISACA Chapter, Jacksonville, Florida, USA, June 2014
2 Goodreads Inc, "Benjamin Franklin," *www.goodreads.com/quotes/247269-an-ounce-of-prevention-is-worth-a-pound-of-cure*
3 Verizon, *2016 Data Breach Investigations Report*, 2016, *www.verizonenterprise.com/verizon-insights-lab/dbir/2016/*
4 *Ibid*.
5 Skybox Security Inc., "2015 Enterprise Vulnerability Management Trends Report," 29 April 2015, *www.skyboxsecurity.com/resources/report-2015-enterprise-vulnerability-management-trends*

A Machine Learning Approach for Telemedicine Governance

Telemedicine is a component of ehealth that uses information and communication technology (ICT) to deliver health care services to overcome distance and connect the provider and the patient. "Telehealth isn't just about the patient and treatment, but knowledge about the equipment is vital as well."[1]

Telemedicine helps during teleconsultation and tele-education for local doctors by facilitating efficient delivery of medical care to "remote areas, vulnerable groups and aging populations."[2] Telemedicine also helps to provide postoperative care through remote follow-up and monitoring.[3, 4] An efficient telemedicine initiative requires an active ecosystem that is comprised of patients, care providers, information technology and participating hospitals within the network. Proactive telemedicine governance helps to ensure an efficient health care delivery system and improves the quality of experience.[5]

This article presents a two-stage decision support system (DSS) framework for telemedicine governance, known as the DSO-R model. The first stage is the department-session-organization (DSO) model, which uses a machine learning approach to predict the probability that a remote organization will participate in a particular telemedicine session; the second stage is the risk estimating (R) model.

Budget constraints and poor demand for telemedicine in lower- to middle-income countries make optimal usage of available resources necessary. A case study of the TELEMED medical center in India is used to validate the model.

Barriers to Telemedicine

The telemedicine market is growing globally at a compounded annual growth rate (CAGR) of 14.3 percent and, from 2014 to 2020, is expected to reach US $36.3 billion. Teleconsultations are among the most common type of telemedicine sessions.[6] Despite the rising demand for telemedicine, research attributes the low penetration of telemedicine to (**figure 1**):

- Initial setup cost
- Competition for care delivery systems
- Lack of technical knowledge
- Concern for health care standards[7, 8]

Telemedicine has some initial setup and running costs that need to be covered by the revenue obtained from telemedicine sessions. Thus, an optimal number of sessions ensures the sustainability of the project.[9]

Applying the DSO-R Model

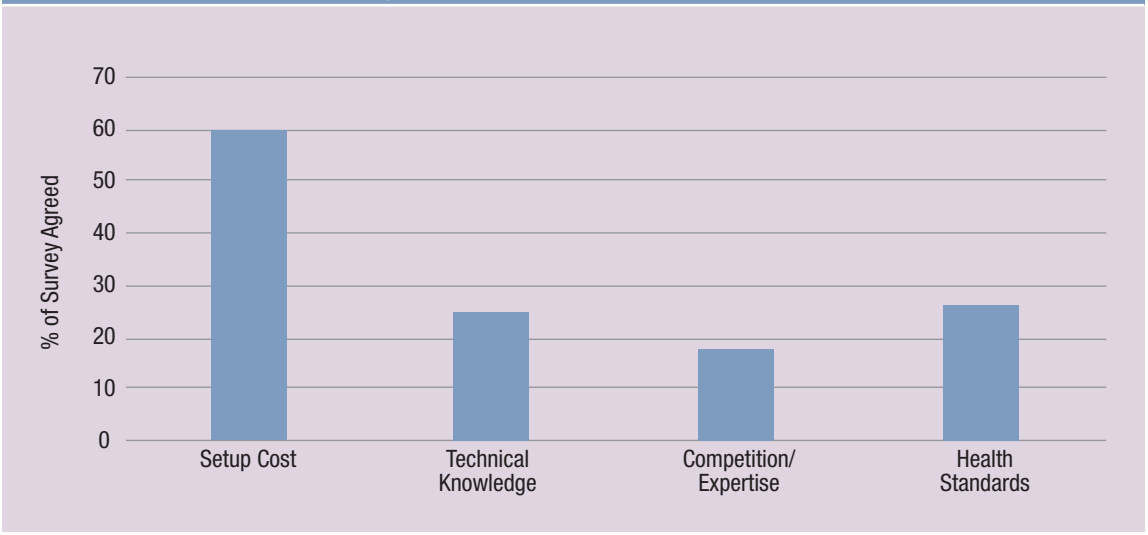
Telemedicine sessions that are related to diabetes, intensive care units or hemodialysis use machine learning techniques in a clinical decision support system (CDSS).[10, 11, 12] The purpose of the DSO-R model is to understand the objectives of health care organizations for setting up a telemedicine project and their traditional health care delivery processes and to determine the health care organizations that are best suited to set up telemedicine session initiatives. One can manually compute the expected loss of the organization conducting the telemedicine

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Shounak Pal
Is a Ph.D. student in the information technology and systems department at the Indian Institute of Management, (Lucknow, India) where he is a member of the ISACA® student group. He has worked as a software engineer in a leading multinational software consulting firm. He can be reached at fpm15015@iiml.ac.in.

Arunabha Mukhopadhyay, Ph.D.
Is an associate professor in the information technology and systems department at the Indian Institute of Management, Lucknow, India. He was the recipient of the Best Teacher in Information Technology Management Award from Star-DNA group B-School in 2011 and 2013, and the 19th Dewang Mehta Business School Award in 2013. He can be reached at arunabha@iiml.ac.in.

Figure 1—Barriers to Telemedicine



Source: S. Pal, A. Mukhopadhyay. Reprinted with permission.

session, in case the model incorrectly selects a remote hospital through its classification mechanism based on the following input parameters:

- Department type (i.e., endocrine surgery, transfusion medicine)
- Session type (i.e., general sessions, follow-up, tele-common grant round [tele-CGR])
- Receiver organization type (academic or nonacademic)

After learning from prior knowledge, the telemedicine DSO model predicts the partner health care organizations (e.g., National Medical College Network [NMCN], South-East Asia Telemedicine Forum and Sub-Sahara e-Network Project) that are best suited for setting up a telemedicine session initiative. Such a model can help to optimize TELEMED's reach across India and abroad.

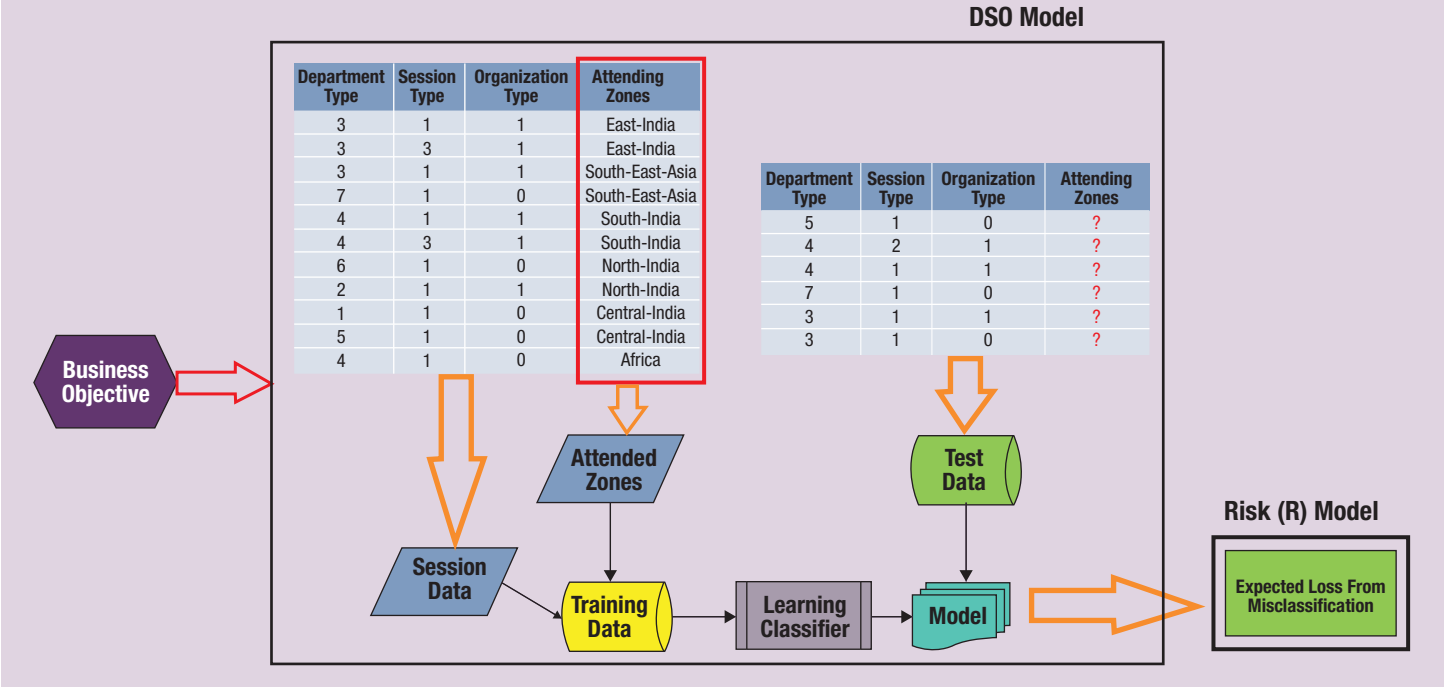
The risk-estimating model computes the expected loss arising from misclassification in the DSO model prediction of suitable partner health care organizations. The risk computation depends on the accuracy rate of the decision tree, interest of patients in telemedicine, in-house treatment available and monetary impact of an admitted patient. **Figure 2** illustrates the proposed DSO-R model.

Telemedicine In India

Associated Chambers of Commerce and Industry of India (Assocham) reported a 20 percent annual growth rate of the telemedicine market in India and estimated that its market value will double by 2020, to US $32 million.[13] Telemedicine service delivery is ideal for India, because it has vast expanses of remote hilly regions, tribal areas and islands,[14] in which "Seventy-five percent of the doctors practice in urban, 23 percent in semi-urban areas and only 2 percent in the rural areas where the vast majority of the population lives."[15]

Telemedicine projects at the Christian Medical College (CMC) Vellore and All India Institute of Medical Science (AIIMS) New Delhi are set up in collaboration with the Japanese International Cooperation Agency (JICA). JICA provided the initial investment for the IT equipment for telemedicine initiatives. The 11th five-year plan of the Government of India, for 2007-2012, lists 11 states (including Andaman-Nicobar and Lakshadweep) and eight super-specialty hospital networks that have established telemedicine projects.[16] The type of communication used is video satellite (VSAT or Sky IP), integrated services digital network (ISDN) or both. The funding and implementing agencies of the different telemedicine projects are carried out by

Figure 2—Telemedicine DSO-R Model



Source: S. Pal, A. Mukhopadhyay. Reprinted with permission.

Indian Space Research Organisation (ISRO), Centre for Development of Advanced Computing (CDAC), IIT Kharagpur and others. The Department of IT, Ministry of Information and Technology of India is also acting as the facilitator for several telemedicine projects.[17]

Case Study

A case study of the TELEMED medical center is used to measure and validate the DSO-R model. The vision for TELEMED in Lucknow, India, was adopted from the US National Institutes of Health (NIH) Clinical Center:

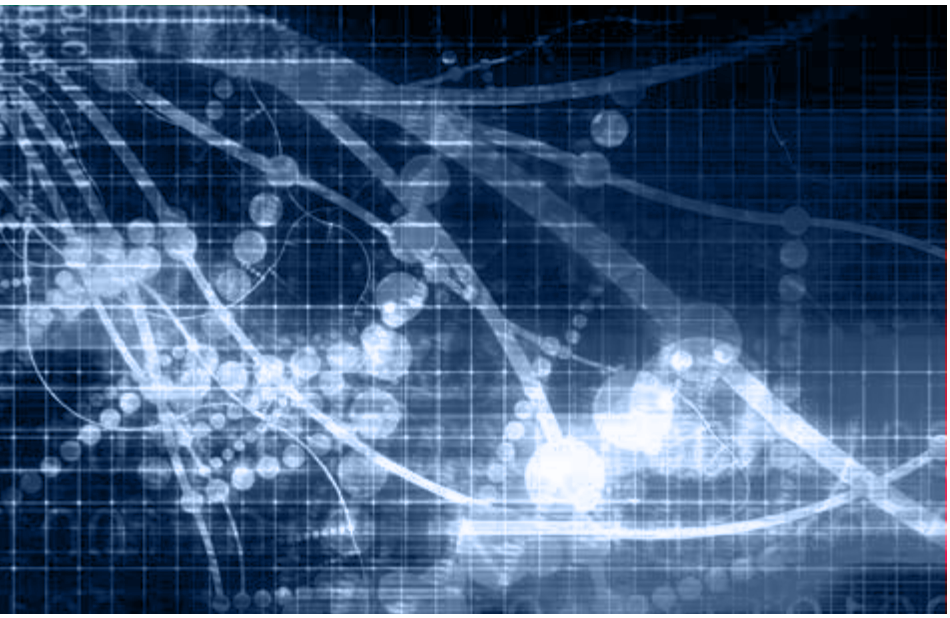
> *TELEMED intends to be a top-class medical institute in Asia, with the intention to minimize long distances traveled for treatment of their diseases. TELEMED also intends to emerge as a super-specialty medical care unit, in terms of availability of skilled doctors, nurses and technicians and being able to meet up to international best practices.*[18]

TELEMED is a tertiary-level referral academic medical center that is mainly involved in training and teaching in the 18 specialist departments in its 30-department center. The aim of the medical center includes delivering state-of-art tertiary-level medical care, and super-specialty research and capacity building through teaching and training.

TELEMED has moved toward maintaining a well-developed infrastructure for education, research, training and application for telemedicine. TELEMED receives both intramural and extramural project grants that have aided in the sustenance of the telemedicine program and research works. The funding institutions include several national and international funding agencies. TELEMED also conducted approximately 450 intramural projects that helped it to sustain its research incentives.[19]

TELEMED wanted to analyze its past data about departments that were involved in telemedicine sessions (general sessions, follow-up and tele-CGR) with remote organizations (academic or nonacademic). It was also necessary to determine

the risk that is associated with an incorrect decision made by the DSO-R model. Realization of the cost associated with the risk can help to optimize telemedicine session utility and minimize the loss.



Methodology Used

This section describes the methodology that was used in the TELEMED case study.

DSO Model

TELEMED's past data consist of various levels of categorical variables. This type of data set is ideal for developing classification rules that can contribute to the identification of the target from a given pattern of attributes.[20] The classification tree is implemented through the MATLAB R2012a program. The program predicts the location of the remote organization based on predictors entered by the user. The classification rule consists of the probability of occurrence of different zones for a particular set of data. The accuracy of the classification tree was tested by training the classification tree with 80 percent of the past data set and using the remaining 20 percent as a test set. This DSO model will help to reduce the low-utility risk that is associated with a telemedicine session.

Risk (R) Model

The R model further determines the accuracy of the decision tree. A hospital incurs a considerable inpatient care cost (about 43 percent in the United States).[21] If a patient is not treated properly through a scheduled telemedicine session, then the cost to the patient and the hospital increases. An exponential function of number of days and diffusion rate of ICT was used to calculate the number of patients who used telemedicine (**figure 3**).

Figure 3—Number of Patients Who Arrived for Telemedicine Treatment

Number of patients who arrived at the telemedicine center for treatment =

$$\frac{\text{Population of the rural setup where the telemedicine center is located}}{1+e^{-bx}}$$

where b = diffusion rate of ICT and

x = number of days post introduction of telemedicine center at remote location.

Source: S. Pal, A. Mukhopadhyay. Reprinted with permission.

The result of the **figure 3** equation was used in the equation in **figure 4** to determine the expected loss for each day.

Figure 4—Expected Loss per Day

Expected loss per day = Population * (1-Accuracy of location classifier) * Number of patients who arrived at the telemedicine center for treatment * {1-Probability (Treatment available)} * Probability (Patient travels for further treatment) * Monetary impact due to patient admission

where the "monetary impact due to patient admission" is denoted as a negative value

Source: S. Pal, A. Mukhopadhyay. Reprinted with permission.

Data

The data on session details for each telemedicine session that the TELEMED telemedicine project group conducted from 2007 to 2015 consisted of 2,612 data points, which are categorized in **figure 5**. They consist of more than 30 departments and three session types, i.e., general sessions, follow-up sessions and tele-CGR sessions. Several partner health care organizations associated with TELEMED for teaching and patient care. The partner hospitals

were separated into teaching and nonteaching organization types. For simplicity of explanation, **figure 5** shows only the top seven departments (in maximum number of sessions) and categorizes the partners into six zones.

The purpose of the case study is to establish a pattern between location determination (zone) and session type to ensure error-free decision making. The results can also be used to recommend zones for conducting new sessions and can be included as a part of TELEMED's risk mitigation strategy.

Results

DSO Model

In the first stage of the DSO-R model, the resultant zones were determined based on their probability of occurrence for a predictor set. The resultant decision tree that is illustrated in **figure 6** can suggest only a single zone based on a particular set of predictors.

Figure 7 compares the predicted data with test data for the test data set. Not all the predicted data match the test target data. The prediction tree predicted 415 out of 523 (80 percent) of the test data set accurately. However, the receiver operating characteristic (ROC) curve performed better for S-E-A, South-India and East-India due to the higher number of sessions of these zones in telemedicine activities (**figure 8**). Central-India and North-India showed lower accuracy due to lack of consistency between training and test data. The prediction accuracy was highly affected by the prior knowledge of the training data set and, therefore, can be a weak recommendation system.

Risk (R) Model

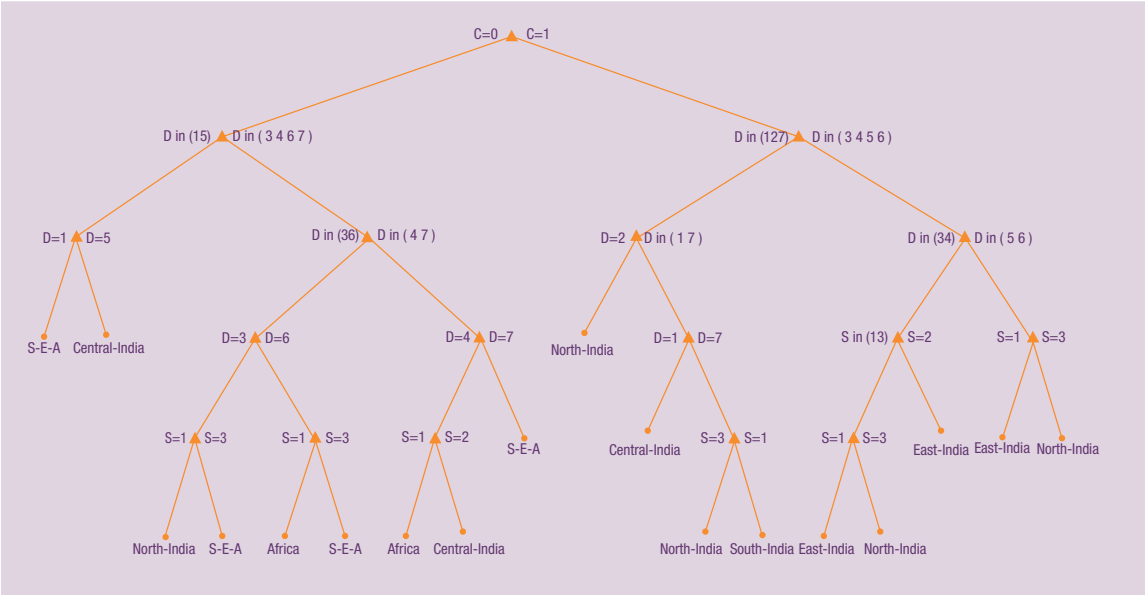
In the second stage of the DSO-R model, the equation in **figure 4** was used to calculate the expected loss due to misclassification of the decision tree in the first stage. In a rural setup in India with a population of 3,000, the pace of diffusion of ICT is slow (0.05). Therefore, the number of patients who arrived at the telemedicine center for treatment is a minuscule fraction of the rural population tree. For a public super-specialty hospital, it is always important to lower the cost. The accuracy rate of the decision is rounded off to 70

Figure 5—Categorized Data Set for TELEMED

Department types (D)	1. Administrative activities 2. Case-based teaching 3. Clinical immunology 4. Endocrine surgery 5. Nursing skill 6. Pathology 7. Transfusion medicine
Session types (S)	1. General 2. Follow-up 3. Tele-CGR
Organization types (C)	1. Nonteaching hospital 2. Teaching hospital
TARGET: Zones	1. Africa 2. Southeast Asia (S-E-A) 3. East India 4. Central India 5. South-India 6. North-India

Source: S. Pal, A. Mukhopadhyay. Reprinted with permission.

Figure 6—Classification Tree Using TELEMED Training Data Set



Source: S. Pal, A. Mukhopadhyay. Reprinted with permission.

Figure 7—Effectiveness of the Classifier on the Test Data Set

Department Type	Session Type	Organization Type	Predicted	Actual
5	1	0	Central-India	Central-India
4	2	1	East-India	East-India
4	1	1	East-India	North-India
7	1	0	South-East-Asia	South-East-Asia
3	1	1	East-India	South-India
3	1	0	Africa	Africa

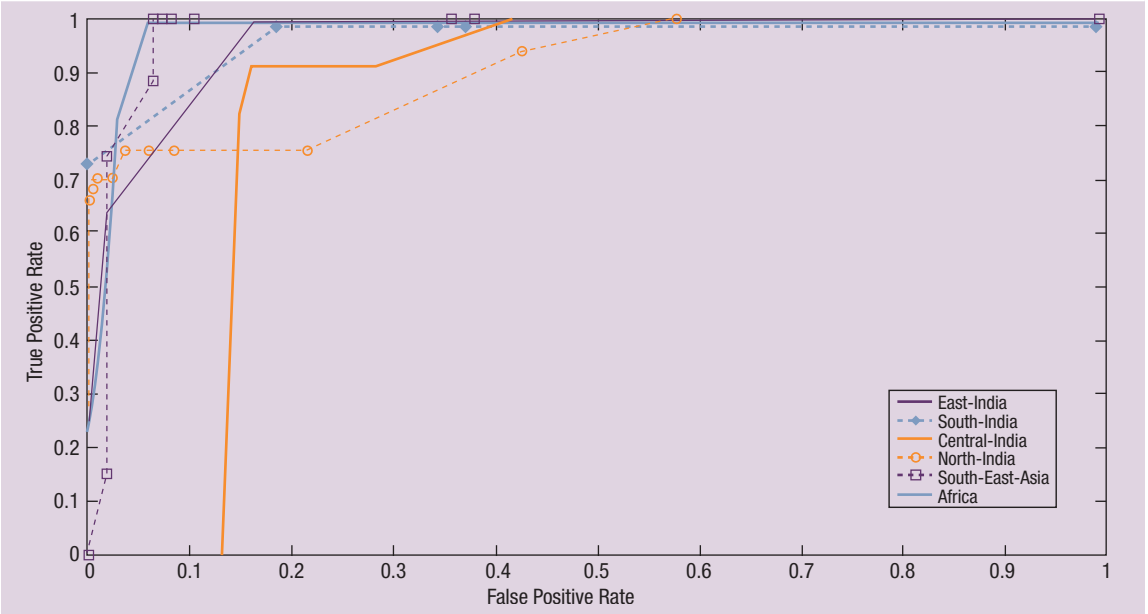
Source: S. Pal, A. Mukhopadhyay. Reprinted with permission.

percent. For the purpose of simulation, the equation in **figure 4** is used, where the probability (treatment available) equals 12 percent, probability (patient traveling for further treatment) equals 60 percent, and monetary impact equals US $135. **Figure 9** demonstrates the result of the calculation and also computes the average expected loss for each day.

Conclusion

The data and session details were analyzed carefully and then the data set was further simplified by selecting appropriate departments based on TELEMED's frequency of telemedicine broadcasting sessions. The DSO-R model ensures better utilization

Figure 8—ROC Curve to Check Prediction Accuracy for the Testing Data Set



Source: S. Pal, A. Mukhopadhyay. Reprinted with permission.

Figure 9—ROC Curve to Check Prediction Accuracy During the Testing Phase

Days	Patients Arriving for Telemedicine	Treatment Available	Patient Travels for Further Treatment	Expected Total Loss in US Dollars ($)
1	81	10	5	690
2	86	10	5	737
3	92	11	6	783
4	97	12	6	828
			Average expected loss per day =	759.5

Source: S. Pal, A. Mukhopadhyay. Reprinted with permission.

of a telemedicine session, because the probability of the remote organization participating in a particular session has already been obtained. The model facilitates faster decision making in broadcasting telemedicine sessions to selected zone(s) and helps with risk identification by precalculating the expected loss from misclassification by the classification tree.

However, a data set consisting of appropriate hospital names rather than zones will improve the prediction accuracy and, therefore, the expected loss when using the DSO-R model. Future development of the DSO-R model will apply more robust and intelligent machine learning techniques to improve the prediction accuracy. The effect of a miscalculation with field

data will also be tested, which will help with studying relevant factors that can increase or decrease the expected loss of a telemedicine session.

Endnotes

1 Hall, S.; "Global Telemedicine Market Forecast: 18.5% Growth Rate Through 2018," FierceHealthcare, 16 December 2013, *www.fiercehealthcare.com/it/global-telemedicine-market-forecast-18-5-growth-rate-through-2018*

2 World Health Organization, "Third Global Survey on eHealth," 2015, *www.who.int/goe/survey/goe_2015_survey_en.pdf?ua=1*

3 European Commission, "Telemedicine for the Benefit of Patients, Healthcare Systems and Society," Commission Staff Working Paper, EC (2009) 943 final, 2009

4 Telemedicine Healing Touch Through Space, "Enabling Specialty Health Care to the Rural and Remote Population of India," Indian Space Research Organisation, Publications and Public Relations Unit, ISRO Headquarters, Bangalore-560094, p. 3-5

5 May, C. R.; M. M. Mort; F. S. Mair; T. Finch; "Telemedicine and the 'Future Patient'?: Risk, Governance and Innovation," Economic and Social Research Council, 2005, *www.york.ac.uk/res/iht/researchfindings/MayFindings.pdf*

6 MedGadget, "Telemedicine Market—Rising Demand for Personal Healthcare Solutions to Boost Deployment of Telemedicine Services, Says TMR," August 2014, *www.medgadget.com/2016/08/telemedicine-market-rising-demand-for-personal-healthcare-solutions-to-boost-deployment-of-telemedicine-services-says-tmr.html*

7 Gulube, S. M.; S. Wynchank; "Telemedicine in South Africa: Success or Failure?," *Journal of Telemedicine and Telecare*, 7 (Supplement 2), 2001, p. 47-49, *https://www.researchgate.net/publication/11608739_Telemedicine_in_South_Africa_Success_or_Failure*

8 World Health Organization, "Global Observatory for eHealth: Survey 2009 Figures," 2009, *www.who.int/goe/survey/2009/figures/en/index1.html*

9 Whitten, P. S.; F. S. Mair; A. Haycox; C. R. May; T. L. Williams; S. Hellmich; "Systematic Review of Cost Effectiveness Studies of Telemedicine Interventions," BMJ, 15 June 2002, *www.bmj.com/content/324/7351/1434*

10 Bellazzi, R.; C. Larizza; S. Montani; A. Riva; M. Stefanelli; G. d'Annunzio; J. Cermeno; "A Telemedicine Support for Diabetes Management: The T-IDDM Project," *Computer Methods and Programs in Biomedicine*, vol. 69, iss. 2, September 2002, *https://www.researchgate.net/publication/11275070_A_telemedicine_support_for_diabetes_management_The_T-IDDM_project*

11 Thursky, K. A.; M. Mahemoff; "User-centered Design Techniques for a Computerised Antibiotic Decision Support System in an Intensive Care Unit," *International Journal of Medical Informatics*, 2006, *www.ijmijournal.com/article/S1386-5056(06)00201-2/pdf*

12 Rose, C.; C. Smaili; F. Charpillet; "A Dynamic Bayesian Network for Handling Uncertainty in a Decision Support System Adapted to the Monitoring of Patients Treated by Memodialysis," ICTAI '05 Proceedings of the 17th IEEE International Conference on Tools With Artificial Intelligence, 2005, *http://dl.acm.org/citation.cfm?id=1106120*

13 B2B Bureau, "Indian Telemedicine Market to Become More Than Double by 2020," *Business Standard*, June 2016, *www.business-standard.com/content/b2b-pharma/indian-telemedicine-market-to-become-more-than-double-by-2020-116060600568_1.html*

14 *Ibid*.

15 Mishra *et al.*; *25 Years Anniversary SGPGI Souvenir*, 2013, *sgpgi.edu.in/pdf/25%20Aniversary%20SGPGI%20souvenir.pdf*

16 *Op cit,* Thursky

17 Government of India Planning Commission, "Report of the Working Group on Health Informatics Including Tele-medicine," 2016, *www.planningcommission.gov.in/plans/planrel/11thf.htm*

18 *Op cit,* Mishra *et al.*

19 *Ibid*.

20 Quinlan, J. R.; "Induction of Decision Trees," *Machine Learning*, vol. 1, 1986, p. 81-106, *www.hunch.net/~coms-4771/quinlan.pdf*

21 Klaassen, B.; B. J. van Beijnum; H. J. Hermens; "Usability in Telemedicine Systems—A Literature Survey," *International Journal of Medical Informatics*, 2016, *https://www.ncbi.nlm.nih.gov/pubmed/27435948*

Smashing the Information Security Policy for Fun and Profit

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

日本語版も入手可能
www.isaca.org/currentissue

One of the chief components of an organization's information security strategy is the security policy. This is a compulsory, high-level administrative document that sets out the strategic objectives and principles of information security that must be adhered to in any activity that may affect the organization's environment and defines the responsibilities and roles of all the actors involved. By way of a rhetorical comparison, it could be said that an information security policy is to an organization what a constitution (or the Magna Carta) would be to a country.

However, and just like an organization's physical or logical assets, the documentary and administrative components of an organization have vulnerabilities and can be exploited to impact its security and operation. Sadly, these kinds of vulnerabilities are not taken into account in a "traditional" risk analysis, leaving the organization exposed to potential attacks, such as a "work-to-rule."

David Eduardo Acosta R., CISA, CRISC, CISM, BS 25999 LA, CCNA Security, CEH, CHFI Trainer, CISSP Instructor, PCI QSA, OPST
Is an information security consultant and lieutenant in the Professional Reserve Officers of the National Army of Colombia. He currently works with Internet security auditors in Barcelona, Spain, and is chief editor of *PCI Hispano (www.pcihispano.com)*, a web portal specializing in Payment Card Industry Security Standards Council standards in Spanish. He is an active member of the IEEE. He can be contacted at dacosta@ieee.org.

The "Work-to-Rule" in the Unionized Context

A "work-to-rule," or "rule-book slowdown," is a type of industrial action where workers take advantage of errors in the contextualization and details of a procedure, applying these in the strictest, most meticulous and literal way possible in normal operating conditions, leading to delays and alterations in the organization's productivity. Unlike traditional strikes, which involve explicit temporary cessation of labor, in a work-to-rule, the tasks assigned to the worker are neither interrupted nor lacking compliance with established rules. This tends to make them more effective and more difficult to contain and correct. Often, this type of industrial action is developed in a covert and highly organized fashion, leaving management without any means of handling its impact.

One of the sectors most prone to undertaking this kind of action is the health care sector.[1] In this sphere, procedures for hygiene and handling of patients, samples and medications must be extremely detailed to guarantee their appropriateness and safety, for both the patients and medical staff. However, if these protocols are written in a specific way and then adjusted to the medical environment where they are to be applied without considering possible exceptions, their strict implementation may lead to unjustified delays in care and abusive bureaucracy, even to the point where human lives could be at risk. By taking advantage of this pressure, striking workers can exact compliance with their demands. Additionally, if the administration seeks out the potential causes of the industrial action, it may turn out that the origin lies in its own shortcomings in its phrasing of the regulations. This might render it counterproductive to ask the workers not to comply with the procedures initially established and thus be forced to accept responsibility

for their entire impact on the operation, without the tools to apply corrective measures with respect to the personnel who have taken part in the industrial action.

Undermining an Information Security Policy With a Work-to-Rule

Following from the concept previously described, undermining a poorly written information security policy can be fairly easy. Taking into account that the vast majority of these documents are based on generic templates, are rarely reviewed, are not adapted to the actualities of the organization's business or the current state of its information environment, and generally do not include procedures for managing exceptions, the reality of adhering strictly to these types of regulations can lead to delays in operation and/or consequences for the integrity, confidentiality or availability of information. With the addition of the obligation-to-comply factor on the part of those involved, such failures can be amplified by means of a work-to-rule, causing productivity losses to the business, with knock-on effects that are both financial and operational (i.e., affecting service level agreements [SLAs]).

Additionally, an information security policy is supported and complemented by auxiliary documents that focus more on specific areas/topics whose importance is classified according to the degree of obligation they entail. This is the situation for regulations, standards, procedures, technical instructions, guides, recommendations, etc. The implementation of a work-to-rule would be possible via any of these components of an organization's regulatory framework.

Several illustrative examples of work-to-rule on an information security policy or a vulnerable auxiliary document include:

- A company's information security policy makes it obligatory for "all operating systems susceptible to malware to have an updated, working antivirus solution installed." However, this organization has within its computer pool a series of stations with limited hardware used as point-of-sale (POS) terminals. A work-to-rule can be implemented through the obligatory installation of antivirus software on these stations, with the ensuing impact on their performance and availability adversely affecting customer response times and normal operation, as well as their response to daily transactions and sales.
- The information security policy makes it obligatory to install security updates during the month following their release by the manufacturers. The work-to-rule could be applied to the unplanned-for updates to critical components by merely complying with the time frames indicated, which can affect the availability of the company's services.
- With regard to password management, the policy states that "changes to passwords that have been forgotten must be applied with physical validation of the user's identity." If the user is not in the city or the country, the administrator in charge of the change may apply the work-to-rule to the implementation of this check, thereby affecting the user's access.

> **"Undermining a poorly written information security policy can be fairly easy."**

Additional examples can be found in the implementation of policies on change management and user management, where often the stages for request, approval and implementation tend to be very strict and the implicit red tape can be exploited in a process of work-to-rule, impacting the company's normal operation.

Unfortunately, the organization affected by this problem cannot contradict itself by making its workers disobey the security policy's controls, since this would invalidate the regulations; thus, the situation leaves the company at the mercy of the resulting procedural chaos.

Enjoying this article?

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

Protecting a Security Policy From a Work-to-Rule Attack

It is easily concluded from the aforementioned descriptions that the vulnerabilities exploited by a work-to-rule are usually related to errors in phrasing, problems with the management of exceptions, lack of updating, and the design of a security policy or its auxiliary documents that does not reflect the reality of the company and is inappropriate in operational terms. These kinds of mistakes generally have their origin in the belief that security documentation serves only as filler for the purposes of bureaucratic procedures and no one ever reads them—common faults in developers, operators, systems administrators and some misguided heads of security.

> **"The security policy should be designed to adapt to the environment it protects rather than the reverse."**

To prevent this risk, the following series of premises should be borne in mind when drawing up and implementing a security policy:

1. **Carry out periodic testing with hypothetical scenarios to identify failures in the policy that could be exploited by malicious users.** To identify weaknesses in the regulatory framework before they can be exploited by malicious employees, management can make use of exercises involving the application of the information security policy in simulated situations where the participants—personnel from key areas within the company (i.e., legal, human resources, public relations, physical security, business continuity)—can interact in a hypothetical scenario. These types of exercises are very common in plans for incident response and business continuity, whose testing methodology can also be extrapolated to information security policies.

   To detect problems that may be exploited by a work-to-rule, it is necessary to analyze a situation involving the application of a security policy (simulation principle) and go step-by-step through the instructions described in the regulatory framework. If the process detects any tasks or guidelines that could adversely affect normal operation or if cases of possible exceptions are identified, they are reviewed in detail and the following criteria are applied.

2. **Analyze the organization's information security context and try to find a balance between security and operational controls.** The security policy should be designed to adapt to the environment it protects rather than the reverse. This is why it is necessary to have prior, detailed understanding of the need to protect information and the cultural environment in which the organization works so procedures can be written that are:

   - **Logical**—Procedures should be as natural as possible and aligned with the organization's present operation. Likewise, they must comply with cost/benefit criteria based on the potential existing threats. Implementing controls that are out of line with the reality of the company can lead to controls whose focus is either too narrow or too broad and that can needlessly prove wearing to the organization. At this point, the experiences of other organizations are often useful for review purposes (benchmarking).
   - **Precise**—The policy should be written in such a way that it expresses exactly the organization's security needs and focuses on this point in particular. Any deviation can open the door to a potential vulnerability. Modularization can be an important element at this point.
   - **Concise**—The policy should be phrased using only those words strictly essential to express the idea. It should avoid the use of any words that

may be unusual, superfluous or unnecessarily technical, or any filler phrases that might blur the concept and permit ambiguity and misunderstandings. Brevity is essential.

- **Timely**—The policy should be up-to-date at all times and describe the present situation and needs of the environment in which it is being applied. The imbalance between changes and controls can result in a deterioration of security levels, allowing vulnerabilities in the implementation of countermeasures and safeguards.
- **Clear**—The policy should be written with the target audience in mind (i.e., the users). Anyone who reads the document should be able to understand it without needing to resort to external references. This means restricting the use of technical terms to those strictly necessary and utilizing simple language.
- **Complete**—The security policy should adhere to the maxim of the five Ws (and an H):[2]
  - Who?
  - What?
  - Where?
  - When?
  - Why?
  - How?

  The absence of any of these elements in a guideline can indicate that it is an unnecessary control that can be ignored as it has no practical justification.
- **Objective**—The policy should be written in the third person, eliminating any subjective factor that might indicate that a guideline was chosen due to favoritism or preference for a particular individual, technology or area.

On finishing the task of writing the policy (or during review/reevaluation), its guidelines should be analyzed in terms of these listed filters for the purpose of identifying any unnecessary or vulnerable elements.

3. **Establish compensatory controls and measures for exceptions.** The flexibility to adapt to inevitable changes in technology and new threats should be a key factor in the security policy to ensure its validity and currency. In addition to guidelines (among which the policy itself is to be found) aimed at deterrence, prevention, detection, correction and recovery that make up the basic protective arsenal, there should be compensatory controls. A compensatory control is defined as an alternative control that can be implemented when there is a justified administrative or technical limitation (exception) that does not allow the use of an initially established guideline.[3] These types of controls allow a level of security equal or superior to the original.

> **"The use of incentives can be implemented as a tool for persuading personnel to become involved in these types of initiatives."**

In addition, it is essential to establish extraordinary measures in case of emergencies. These measures are known as exceptional measures and they enable the policy to be adapted to unforeseen situations, acting as a countermeasure in the event of a control failure or a response to unforeseen activities.

4. **Define communications mechanisms to obtain feedback from the policy's users.** The creation of bidirectional communications channels allows management to garner first-hand information from policy users that can be used to adapt the policy on the basis of experiences of day-to-day operation. Contact forms, suggestion

boxes, online chats or other social network tools can be valid channels for gathering feedback that will enable early detection of errors and their proactive correction.

The use of incentives can be implemented as a tool for persuading personnel to become involved in these types of initiatives.

> **"The use of incentives can be implemented as a tool for persuading personnel to become involved in these types of initiatives."**

5. **Establish schedules for periodic review of the security policy and updates when significant changes to the environment arise.** Responsibility for reviewing documents, deadlines and scenarios that trigger these reviews should be established in the policy itself, including changes in technology, entry or retirement of third parties, delegation of tasks to external companies (i.e., outsourcing), and acquisitions/mergers, which may be catalogued as significant changes in the environment.

   Additionally, it is essential that the head of security keep the controls in the security policy aligned to the threats in the environment. This guarantees that application of this document is valid and aligned to the reality of the company, avoiding obsolete or unnecessary guidelines.

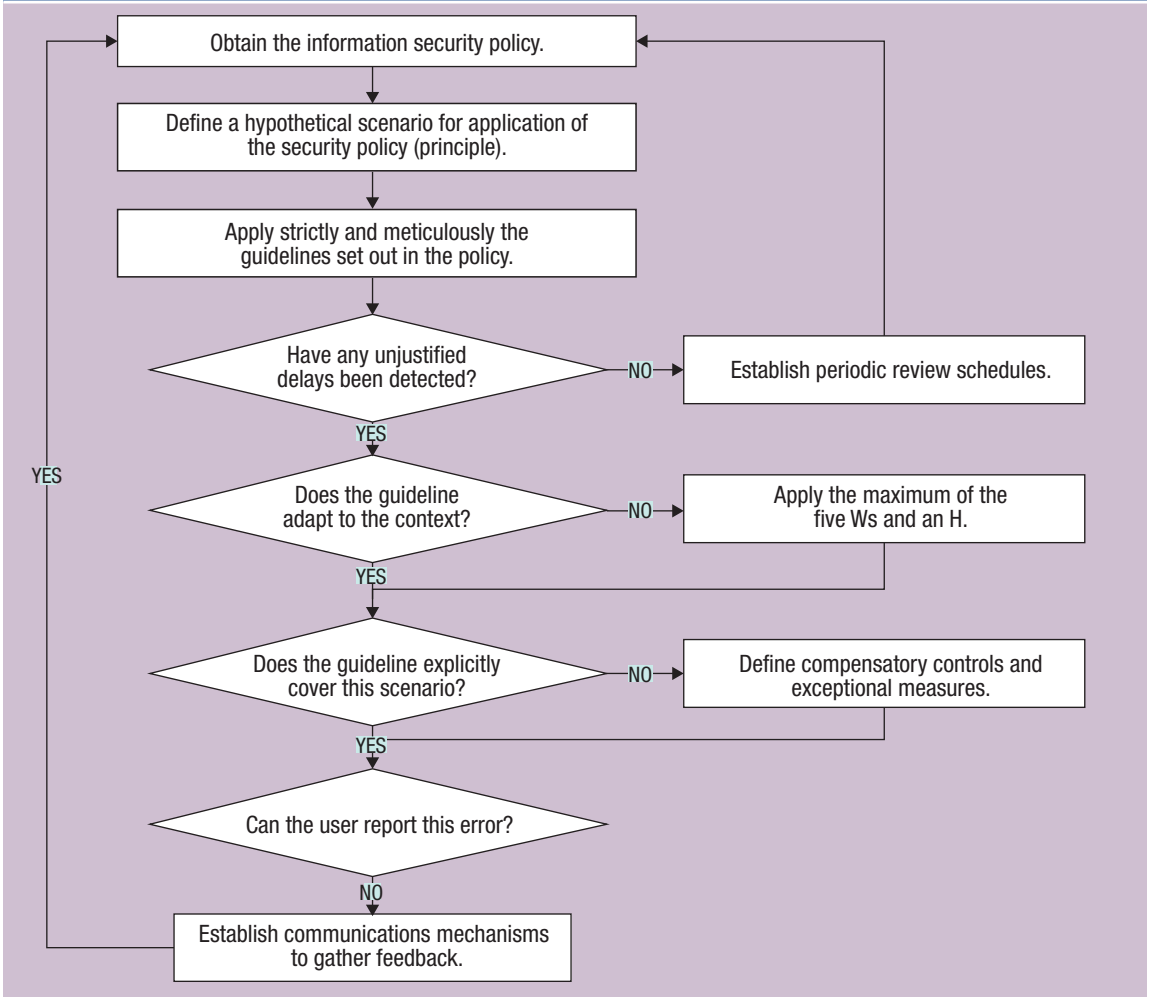
   Broadly speaking, the flow of validation would be as shown in **figure 1**.

Conclusion

Based on the information an organization manages, the security policy should set out the requirements and controls for the protection of the various assets according to their criticality. It is precisely at this point that the phrasing of a policy is a key factor, since, depending on the way in which the aforementioned guidelines are expressed, there can be flaws due to either excessive laxity or restrictiveness. These vulnerabilities can be the objective of abusive bureaucracy on the part of malicious staff using a work-to-rule, where guidelines are followed in their strictest form. If the policy is not up to date or in line with the operational reality of the organization and fails to allow for management of exceptions, the impact of this type of industrial action or sabotage could have grave consequences for the company's handling of information security.

To prevent and manage this problem, there should be methodological application of bidirectional channels of communication with the personnel involved, administration of periodic tests to search out potential incongruities in the document, recurrent reviews of the regulatory document, use of compensatory controls and exceptional measures, and ongoing analysis of the organizational context and definition of the cost/benefit of the guidelines. These tasks will work together to prevent the policy from ending up as a "dead letter" that will, sooner or later, become a threat to the company itself.

Figure 1—Validation Flow for Updates to Security Policy to Avoid Work-to-Rule



Source: David Eduardo Acosta R. Reprinted with permission.

Endnotes

1 ABC España, "Los enfermeros convocan una huelga de celo por el decreto que les impide prescribir medicamentos", 28 October 2015, *www.abc.es/sociedad/abci-enfermeros-convocan-huelga-celo-decreto-impide-prescribir-medicamentos-201510281549_noticia.html*

2 Spencer-Thomas, O.; "Writing a Press Release," 20 March 2012, *www.owenspencer-thomas.com/journalism/media-tips/writing-a-press-release*

3 Williams, B.; "The Art of the Compensating Control," March 2009, *https://www.brandenwilliams.com/brwpubs/TheArtoftheCompensatingControl.pdf*

Using Open Source Tools to Support Technology Governance

Most practitioners are already very accustomed to using technical tools for specific tactical purposes when it comes to security or assurance within their environments. These tools can be open source or commercial: For example, practitioners might employ open-source tools such as Clam, Wireshark or OpenVAS to accomplish specific tasks (antivirus, network analysis and vulnerability assessment, respectively) or they might leverage commercial products to provide anything from intrusion detection systems (IDS) to firewalls to data loss prevention (DLP) to cloud access security broker (CASB) capability (and beyond). In short, tools—the careful selection and the judicious use thereof—are an important part of being a practitioner in these subject areas.

Ed Moyle
Is director of thought leadership and research at ISACA. Prior to joining ISACA, Moyle was senior security strategist with Savvis and a founding partner of the analyst firm Security Curve. In his nearly 20 years in information security, he has held numerous positions including senior manager with CTG's global security practice, vice president and information security officer for Merrill Lynch Investment Managers and senior security analyst with Trintech. Moyle is coauthor of *Cryptographic Libraries for Developers* and a frequent contributor to the information security industry as an author, public speaker and analyst.

However, when it comes to technology governance (governance of enterprise IT [GEIT]), it can often be harder to find specific tools that can assist the practitioner. The reasons for this are not hard to understand. First and foremost, governance is, by definition, an exercise that requires significant customization from organization to organization; how governance is implemented in organization A is likely quite different from organization B. This is due, in part, to differing goals (both enterprisewide goals as well as the technical goals that cascade from stakeholder needs), differing metrics and key performance indicators (KPIs) used to ensure continuous improvement, different culture and risk appetites, and numerous other organization-specific factors. This, in turn, makes it hard to find and use one-size-fits-all tools that can ubiquitously support implementations across a number of organizations.

That said, there are a few tools that practitioners with an eye toward holistic and systematic governance can employ to help them along the path. In this column, some of these tools and how they can be used in a broader governance implementation are highlighted. There are, of course, more tools than can be covered in a cursory overview such as this one; that said, this column calls out a few that can be of use in an organization's governance efforts.

Moreover, since it is a truism that budgetary considerations can be a factor (particularly in times such as these when budgets are lean and scrutiny is high), open-source tools that can be used for this purpose are highlighted. Note that this is not to imply that there are not commercial tools out there that can do similar things or help in different ways; in fact, nothing could be further from the truth as there are hundreds (if not thousands) of commercial products that can assist in GEIT implementation. But, given that not every organization will have the same level of budgetary support available (not to mention that the vendor landscape is often mutable), this column puts the spotlight on open-source options.

For the organization undertaking a GEIT implementation, it can be challenging to get traction and get started. Budgetary considerations can sometimes be a limiting factor in terms of making progress. Where this is the case, open-source tools can have the benefit of a rapid "on ramp" that might not otherwise be the case.

1 Asset Inventory

As every practitioner knows, asset management is challenging to do well. Consequently, leveraging tools that bolster asset management can have broad-reaching benefits in a number of areas. In the context of GEIT specifically, though, tools that support asset management can be particularly valuable. Why? Because during the implementation phases of a GEIT rollout, organizations undertake a few key activities: (i.e., risk assessment and evaluation, establishment of KPIs and performance metrics, setting of appropriate scope). At a macro level, these tasks will not (necessarily) require a component-level awareness of every system, application or node that an environment has fielded. But, as an organization starts scratching the surface and goes beyond the macro level into the more detailed planning of any of these activities, accounting for the unique nuances of an environment (which presupposes one knows what is in it) can mean the difference between success and failure.

With this in mind, tools that support asset inventorying and discovery, such as GLPI *(www.ubuntugeek.com/glpi-it-and-asset-managemet-software.html)* and OCS Inventory NG *(www.ocsinventory-ng.org/en/)* can be beneficial. Organizations can use them to discover what they already have in place to assist in risk management efforts. They can also use them to keep a record of what they have fielded and tie that information together with metrics gathering to assist in establishing ongoing performance improvement metrics. Further, organizations can tie the information contained within that system to support everything involved in the implementation phase of their GEIT planning.

2 Risk Management

ISACA's *Getting Started with GEIT: A Primer for Implementing Governance of Enterprise IT* highlights the need for a risk assessment during the implementation phase of a GEIT rollout: Specifically, the guide outlines that, "Risk assessments and monitoring should also be performed for the implementation of the GEIT initiative to ensure that program risk—whether it is resource commitments, budgeting or schedule—is addressed to keep the program on track."[1] This indicates that assessing risk—and responding accordingly—is part and parcel of the implementation of GEIT itself. It is in this area that free and open-source tools can help support the implementation.

There are few ways in which this is true. First, tools such as SimpleRisk *(https://www.simplerisk.it)* can help keep track of risk at a high level by recording what the areas of risk are, providing a way to track them over time, supporting tying together mitigation strategies to the risk areas themselves and recording remediation progress. Likewise, there are free tools that can help organizations understand what the risk factors are and identify/contextualize them. For example, a tool such as Practical Threat Analysis (PTA) *(www.ptatechnologies.com)* can help develop a systematic threat model to ensure that the organization is looking at risk systemically. Depending on the level that stakeholders want to reach in doing this, they can, potentially, leverage tools such as OpenVAS or Vega to help identify vulnerabilities in the surface of applications and infrastructure that can inform the risk profiling that they do. Granted, not every GEIT implementation will take the risk assessment portion of the implementation to this granular a level, but the option is there should the organization choose to do so.

3 Monitoring

The goal of a GEIT implementation is to get to a feedback loop of continuous improvement. Meaning, by monitoring the organization in an ongoing way—and being alert to the metrics and KPIs that tie back to stakeholder requirements—organizations can see areas of improvement and build upon them to get better. It is here where there are a number of options that can assist.

First, there are a number of tools out there to support performance monitoring. This includes tools such as Icinga 2 *(https://www.icinga.com/products/icinga-2/)*, Nagios *(https://www.nagios.org)*, OpenNMS *(https://www.opennms.org/en)* and Zabbix *(www.zabbix.com)*. Any information about performance can directly speak to reliability and accessibility information that will likely be of interest as the organization completes a governance implementation. Thinking more broadly, though, tools that build upon this such as Observium *(https://www.observium.org)* or Cacti *(www.cacti.net)* can provide additional layers of detail depending on how deep the organization intends to go. Of course, some organizations may already have tools in place that provide similar information, but for those that do not, this might provide the needed information.

Doing the monitoring is important, of course, but so is the ability to render monitoring information into a format that enables the organization to act upon it. Tools that assist in data visualization, for example, Datawrapper *(https://www.datawrapper.de/gallery)* and the like, can likewise be of benefit to an organization from a governance point of view.

Endnotes

1 ISACA®, *Getting Started with GEIT: A Primer for Implementing Governance of Enterprise IT*, USA, 2016, *www.isaca.org/getting-started-with-GEIT*

help source

Q I have heard from vendors that cognitive technologies such as machine learning can assist in my risk management and security efforts. Is this the case? If so, how do I measure and evaluate their performance? Are there any standards, tools or information sources that can help?

A An effective risk management process requires a risk response decision that is based on earlier knowledge about the possibility of threats exploiting vulnerabilities within the system. A normal risk management process identifies a threat and assesses it for relevance to the organization. Based on these assessment results, the organization makes a decision on how to respond. However, with the automation of information management, the speed of information processing is continuously increasing and the organization requires faster responses. The challenge the normal risk management process presents to organizations today is its ability (or lack thereof) to meet the need for timely detection of risk materialization and response to those risk items.

Detection of risk materialization is currently being done using structured data analysis. A good example is security incident and event management (SIEM) tools used for log analysis and determining possible risk materialization. Another good example is financial institutions using transaction analysis and unstructured (text) data analysis utilizing tools with analytics capabilities to detect possible fraud or attacks. However, these technologies suffer from false-positive alerts, and human intervention is required to make a response decision. To date, there have been two distinct eras of cyber security: perimeter controls[1] and security intelligence. These serve as building blocks as we enter the third era—cognitive security.

Cognitive systems are self-learning systems that use data mining, machine learning, natural language processing and human-computer interaction to mimic the way the human brain works. If used for detecting risk materialization, these systems can learn from the decisions made by humans and update their knowledge engine.

There are a few products for the financial sector being used for detecting possible fraud; however, these products are still not mature enough to be used for risk management in all sectors. Another challenge is that the review of new threats and risk that forms the basis for risk management is not yet mature enough for cognitive technologies to adopt. There are some tools available that can understand the updated risk database and provide dashboards to management for review, but risk assessment, which is human judgment based on experience, will take more time to be available for self-learning systems.

Today, the use of cognitive technologies in risk management and security is limited to:

- Analyzing security trends and distilling enormous volumes of structured and unstructured data into information and then into actionable knowledge to enable continuous security and business improvement[2]
- The use of automated, data-driven security technologies, techniques and processes that support cognitive systems' having the highest level of context and accuracy[3]

In the future, cognitive systems could analyze interactions, their nature and susceptibility, to develop risk profiles for organizations, corporate actions, training and reeducation. Cognitive systems could also use natural language processing to find and redact sensitive data in an organization.

Q How important is threat intelligence to my risk management efforts? Is this something that we should implement? If so, how do I do this?

A Organizations suffer attacks every day and are able to respond to most of them with the knowledge available. However, the adversaries are always ahead and keep devising new attacks using new techniques. The result? Organizations miss the attack and come to know about it only when

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant and visiting faculty member at the National Institute of Bank Management, India.

the damage is done. Zero-day attacks or advanced persistent threats (APTs) are known examples. In other words, organizations are defenseless against new attacks.

Threat intelligence, in simple words, is information an organization can use to enhance its detection capabilities. It helps to detect an attack before it materializes. Primitive examples of threat intelligence can be heuristic scanning by antivirus tools, intrusion prevention system (IPS) or the virus signature update provided by the antivirus vendor. In other words, threat intelligence is information that helps organizations in enhancing the ability to detect, prevent and/or investigate possible attacks before an attack actually takes place or in the early stages of an attack before it impacts business.

Because early detection of an attack helps organizations control the attack's impact and threat intelligence supports earlier detections, organizations would be wise to consider implementing threat intelligence. However, they should also understand that implementing threat intelligence is not a one-time project. It is an ongoing endeavor, as new threats are constantly emerging. To implement threat intelligence, these steps may be considered:

- Build a threat profile that includes possible perpetrators/attackers. This can be done by building possible risk scenarios (refer to *COBIT® 5 for Risk*[4] for generic IT risk scenarios).
- Collect information, particularly about past incidences, within the organization and within the industry: malware indicators and incidents, Internet Protocol (IP)/URL reputation, information from command and control networks, and so on. There are a number of data sources available that can provide this information.
- Form an internal group that analyzes information received from internal and external sources for relevance for the organization.
- Aggregate and analyze the data received, particularly considering the volume and duplicate information. Identify the data that might prompt actions such as updating the existing controls or implementing new controls, and identify possible false-positives. The information posted by possible attackers can especially mislead the response decision.
- Based on information analysis, identify the areas that require changes, particularly the policies, processes, rules for monitoring the events (risk indicators/risk thresholds), firewall rules, etc.
- Validate the rules and implement processes for ongoing threat intelligence information gathering and updating rules and processes.
- Automate the process. For example, in the event of a data breach, lockdown or zero-day attack, implement temporary blocks automatically based on predefined policies. Or, if a device starts behaving abnormally, have it automatically removed from the network for investigation.

"Because early detection of an attack helps organizations control the attack's impact and threat intelligence supports earlier detections, organizations would be wise to consider implementing threat intelligence."

The key point to be noted is that implementing threat intelligence is a mammoth task, so it must be undertaken in small steps.

Endnotes

1 IBM, *Cognitive Security White Paper*, USA, 2016, *http://cognitivesecuritywhitepaper.mybluemix.net/*
2 *Ibid*.
3 *Ibid.*
4 ISACA®, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

crossword puzzle

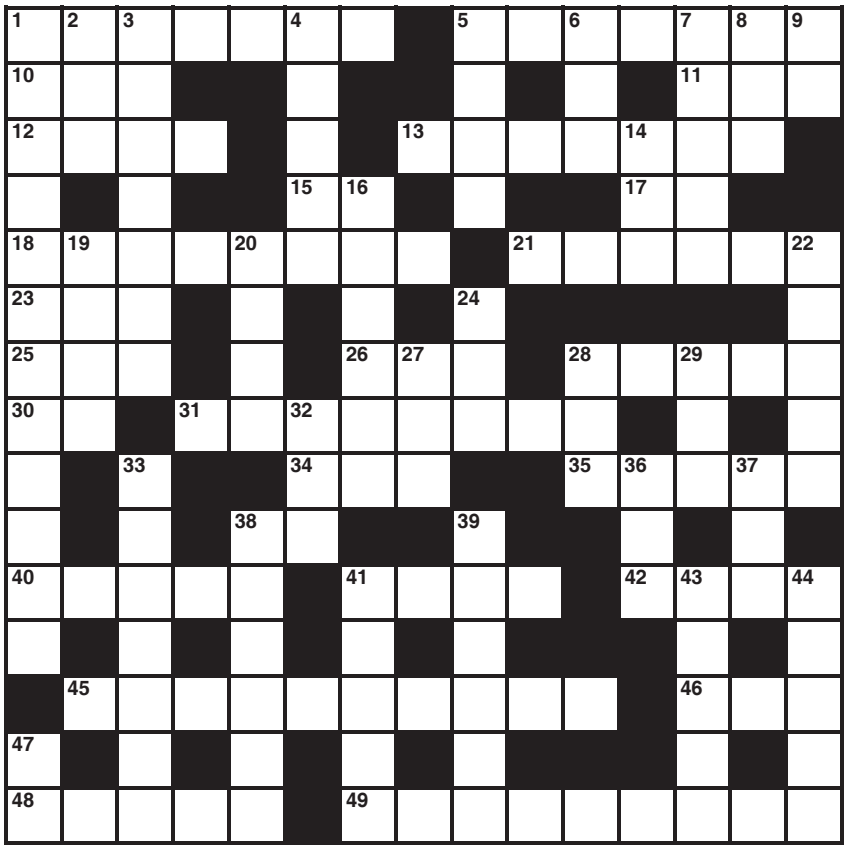
by Myles Mellor
www.themecrosswords.com

ACROSS

1 Moniker for cyberattacks on Iranian nuclear facilities
5 One of the emerging IS/IT risk domains, 2 words
10 Large number, in slang
11 Catch a criminal
12 Easy to buy and install on mobile devices, but may contain malware
13 Slang term for removing restrictions vendors placed on an Android device
15 Close to, abbr.
17 Letters with operate and pilot
18 Trains
21 Took advantage of, with "on"
23 Website address ending
25 Discouraging words
26 Historical time
28 Storage of critical data in this medium may have no provision for how the provider will prevent unauthorized access to it
30 Spanish, for short
31 ISACA's book, *Responding to ____ Cyberattacks*
34 Innovative "talks"
35 Mold
38 French for of
40 Find the source of
41 Role originally accused of putting the "no" in knowledge, abbr.
42 *Death in Venice* writer, Thomas
45 Military strategist who regarded war as an extension of diplomacy
46 Acronym for ISACA's Cybersecurity Nexus Program
48 Memory units
49 Possible outcomes

DOWN

1 Phrase describing cyberconflicts between nations, 3 words
2 Zenith
3 Disconnects, in a way
4 Incident
5 Abbreviation related to offering employees the option of using their own mobile devices at work
6 Secure
7 Plague
8 Meta follower
9 Blood group
14 Winter coat



16 Take back
19 Fall
20 Subject
22 Evade
24 Convened
27 Flag color, metaphorically
28 Musical items
29 ___ roll (winning)
32 Road sign abbr.
33 New term referring to the merging of the mobile phone and tablet
36 Run smoothly
37 Banks' security measure
38 Fixes, as software
39 Senior managers, 2 words
41 Strategy game
43 High-tech code acronym
44 Meeting point
47 Trucker's radio

Answers on page 58

quiz#170

Based on Volume 5, 2016—Cybersecurity
Value—1 Hour of CISA/CRISC/CISM/CGEIT Continuing Professional Education (CPE) Credit

TRUE OR FALSE

RAVAL ARTICLE

1. One of the two observation that emerges from the conflict between emerging new platforms such as Uber and Airbnb models and the regulations is that they left the sensitive human components (drivers, hosts) largely outside of their own perimeters.
2. The concept of "bounded awareness" can be explained as the common tendency to exclude relevant information from our decisions by placing arbitrary bounds around our definition of a problem, resulting in systematic failure to see important information.
3. Both an intuitivist framework and a dominant-value framework identify appropriate moral actions by generating conviction about the most dominant value from among the competing values in a moral dilemma.

PENDERGAST ARTICLE

4. The best awareness programs assess and analyze the real human performance within the organization; they create a plan for sustained improvement; and they introduce a series of educational interventions targeted at changing behavior and encouraging a risk-aware culture.
5. An exciting emerging use for user and entity behavioral analytics (UEBA) is tying it directly to "just-in-time-training" at the spot of the foul.
6. The NIST's Cybersecurity Framework (CSF) defines a truly mature organization as adhering to the principles of being risk informed, and approaches training as an annual event.

ISHAQ ARTICLE

7. A 2015 Centrify Consumer Trust Survey found 75 percent of UK, 66 percent of US and 50 percent of German respondents were likely to stop doing business with a hacked organization. National Cyber Security Alliance reported in 2016 that there are approximately 40 global insurers offering cybercoverage, 30 of which are in the United States.
8. A 2015 Ponemon Institute study found that cyberattacks go undetected for an average of eight months, which is more than enough time for purveyors of data to erase audit logs to impede forensic analysis and wipe out legal evidence.
9. A strong compliance program does not equate to an effective information security program, and *vice versa*. Moreover, an adoption of either program does not necessarily correspond to a reduction of risk.
10. In a report by Reuters, for the few businesses that get hacked, their premiums triple at renewal time. Nevertheless, shareholders expect the board and management to meet their fiduciary requirements to protect company interests.

CALLISKAN ARTICLE

11. Example actions of the "Weaponization" step of the Cyber Kill Chain include spear phishing, man-in-the-middle attacks (MitM), Universal Serial Bus (USB) and infected websites.
12. One of the most notable features of Security Onion (SO) is its packet capture capability using the netsniffing tool. Since capturing all traffic consumes a large amount of hard disk capacity, organizations should plan carefully before installing their system.
13. While an attacker is attempting a breach, honeypots report the event to the central security monitoring servers and help defend the production infrastructures. When used effectively, honeypots can help organizations detect attack attempts in step 1 of the Cyber Kill Chain.

KORPELA AND WEATHERHEAD ARTICLE

14. Grey Box simulates an external attack where testers will spend more time in the reconnaissance phase, and because of that, it tends to take more time and be more expensive.
15. Reporting to management must be part of the pen-test engagement. Best practice is to have one technical, detailed presentation to the IT team and a separate, shorter presentation for the executives that summarizes the tests and focuses on business risk impact and mitigation plan.
16. Obtaining consent from upper management before conducting a pen-test is vital. Depending upon organizational legal requirements, a separate release and authorization form may be required that states that the assessing organization will be held harmless and not criminally liable for unintentional interruptions and loss or damage to equipment.

CPE quiz

Prepared by
Sally Chan
CGEIT, ACIS, CMA, CPA

Take the quiz online

CPE quiz #170

THE ANSWER FORM

Based on Volume 5, 2016

TRUE OR FALSE

RAVAL ARTICLE

1. _____
2. _____
3. _____

PENDERGAST ARTICLE

4. _____
5. _____
6. _____

ISHAQ ARTICLE

7. _____
8. _____
9. _____
10. _____

CALLISKAN ARTICLE

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

KORPELA AND WEATHERHEAD ARTICLE

14. _____
15. _____
16. _____

Name _____

PLEASE PRINT OR TYPE

Address _____

CISA, CRISC, CISM or CGEIT # _____

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, CRISC, CISM or CGEIT CPE credit.

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

1 S	2 T	3 U	X	N	4 E	T	■	5 B	I	6 G	D	7 A	8 T	9 A
10 T	O	N	■	■	V	■	■	Y	■	E	■	11 N	A	B
12 A	P	P	S	■	E	■	13 R	O	O	T	14 I	N	G	■
T	■	L	■	■	15 N	16 R	■	D	■	■	17 C	O	■	■
18 E	19 D	U	C	20 A	T	E	S	■	21 P	R	E	Y	E	22 D
23 O	R	G	■	R	■	N	■	24 S	■	■	■	■	■	O
25 N	O	S	■	E	■	26 E	27 R	A	■	28 C	L	29 O	U	D
30 S	P	■	31 T	A	32 R	G	E	T	E	D	■	N	■	G
T	■	33 P	■	■	34 T	E	D	■	■	35 S	36 H	A	37 P	E
A	■	H	■	38 D	E	■	■	39 C	■	■	U	■	I	■
40 T	R	A	C	E	■	41 C	I	S	O	■	42 M	43 A	N	44 N
E	■	B	■	B	■	H	■	U	■	■	■	S	■	E
■	45 C	L	A	U	S	E	W	I	T	Z	■	46 C	S	X
47 C	■	E	■	G	■	S	■	T	■	■	■	I	■	U
48 B	Y	T	E	S	■	49 S	C	E	N	A	R	I	O	S

standards guidelines tools and techniques

ISACA Member and Certification Holder Compliance

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

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

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

ITAF™, 3rd Edition

(www.isaca.org/itaf) provides a framework for multiple levels of guidance:

IS Audit and Assurance Standards

The standards are divided into three categories:

- **General standards (1000 series)**—Are the guiding principles under which the IS assurance profession operates. They apply to the conduct of all assignments and deal with the IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- **Performance standards (1200 series)**—Deal with the conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and the exercising of professional judgment and due care.
- **Reporting standards (1400 series)**—Address the types of reports, means of communication and the information communicated.

Please note that the guidelines are effective 1 September 2014.

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

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

Reporting
1401 Reporting
1402 Follow-up Activities

IS Audit and Assurance Guidelines

The guidelines are designed to directly support the standards and help practitioners achieve alignment with the standards. They follow the same categorization as the standards (also divided into three categories):

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

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

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

Reporting
2401 Reporting
2402 Follow-up Activities

IS Audit and Assurance Tools and Techniques

These documents provide additional guidance for IS audit and assurance professionals and consist, among other things, of white papers, IS audit/assurance programs, reference books and the COBIT® 5 family of products. Tools and techniques are listed under *www.isaca.org/itaf*.

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

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

Comments may also be submitted to the attention of the Director, Thought Leadership and Research via email (standards@isaca.org); fax (+1.847.253.1443) or postal mail (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

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

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

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

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

ISSN 1944-1967

advertisers/websites

leaders and supporters

ISACA®
Trust in, and value from, information systems

ISACA BOOKSTORE

RESOURCES FOR YOUR PROFESSIONAL DEVELOPMENT

www.isaca.org/bookstore

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

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

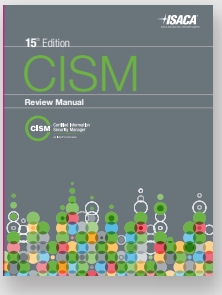
- Searchable content for greater ease-of-use
- Time-saving internal and external hyperlinks
- Interactive features within the table of contents
- Available for immediate download after purchase—with no waiting and no shipping cost anywhere in the world!

CISA® CISM® CGEIT® CRISC™

Browse all of our publications featuring the latest research and expert thinking on standards, best practices, emerging trends and more at ***https://support.isaca.org***

FEATURED BOOKS

CISM Review Manual 15th Edition



by ISACA

PRINT
Product Code: CM15ED
Member / Nonmember:
$105.00 / $135.00

eBOOK
Product Code: EPUB_CM15ED
Member / Nonmember:
$105.00 / $135.00

Updated for the 2017 CISM Job Practice with additional features!

The *CISM Review Manual 15th Edition* is designed to help you prepare for the CISM® exam. This comprehensive, easy-to-navigate manual is organized into chapters that correspond to the four job practice areas covered in the CISM exam. New to the 15th Edition:

- **In Practice Questions** help you explore the concepts in the CISM Review Manual in your own practice.
- **Knowledge Checks** are designed to help reinforce important concepts from the Review Manual.
- **Case Studies** provide real-world scenarios to help you gain a practical perspective on the Review Manual content and how it relates to the CISM's practice.
- **Comprehensive Index** has been updated to make navigating the easier and more intuitive.

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

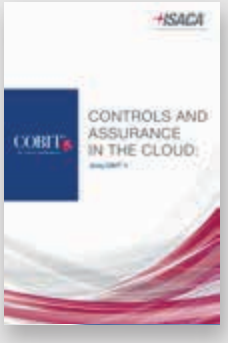
by MacDonnell Ulsch

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

Conquering cyber attacks requires a multi-sector, multi-modal approach

Cyber Threat! How to Manage the Growing Risk of Cyber Attacks is an in-depth examination of the very real cyber security risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. Written by one of the nation's most highly respected cyber risk analysts, the book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences. Much more than just cyber security, the necessary solutions require government and industry to work cooperatively and intelligently. This resource reveals the extent of the problem, and provides a plan to change course and better manage and protect critical information.

Controls & Assurance in the Cloud: Using COBIT® 5



by ISACA

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

WEB DOWNLOAD
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. In addition, it provides a list of available publications and resources that can help determine if cloud computing is the appropriate solution for data and processes in scope.

COBIT® 5 for Business Benefits Realization

by ISACA

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

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

Enterprises make technology-enabled investments as a matter of daily operations. The need for business benefits realization from those investments is always present-from the time that the assets from such investments are being planned, until they are retired from use.

COBIT 5 for Business Benefits Realization builds on the COBIT 5 framework by focusing on governance and management dimensions of business benefits realization and providing contextualized guidance to COBIT 5 for consultants, experts in governance and business management, IT professionals, and other interested parties at all levels of the enterprise. This publication can be used as a practical guide for various aspects of business benefits realization in relation to COBIT 5.

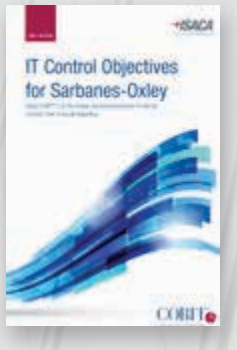
2 EASY WAYS TO ORDER:

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

2. Phone—Contact us M–F between 8:00AM – 5:00PM Central Time (CT) at +1.847.660.5505

IT Control Objectives for Sarbanes-Oxley:

Using COBIT® 5 in the Design and Implementation of Internal Controls Over Financial Reporting, 3rd Edition



by ISACA

PRINT
Product Code: PSOX3
Member / Nonmember: $35.00 / $60.00

WEB DOWNLOAD
Product Code: WPSOX3
Member / Nonmember: FREE / $60.00

This publication provides CIOs, IT managers, and control and assurance professionals with scoping and assessment ideas, approaches and guidance in support of the IT-related Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control objectives for financial reporting. Enhancements include:

- The requirements of the PCAOB's Auditing Standard No. 5 (AS 5)
- Mappings of the role of the COSO framework and its relationship to COBIT 5
- Detailed examples of application controls
- Issues in using SSAE 16 SOC 1 Examination reports
- IT Sarbanes-Oxley compliance road map

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

by ISACA

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

WEB DOWNLOAD
Product Code: WAPG
Member / Nonmember: $35.00 / $60.00

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

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

Reverse Deception: Organized Cyber Threat Counter Exploitation

by Sean Bodmer, Dr. Mak Kilger, Gregory Carpenter, Jade Jones and Jeff Jones

PRINT
Product Code: 31MRDO
Member / Nonmember: $40.00 / $50.00

"A comprehensive and unparalleled overview of the topic by experts in the field." – Slashdot

Expose, pursue, and prosecute the perpetrators of advanced persistent threats (APTs) using the tested security techniques and real-world case studies featured in this one-of-a-kind guide. Reverse Deception: Organized Cyber Threat Counter-Exploitation shows how to assess your network's vulnerabilities, zero in on targets, and effectively block intruders. Discover how to set up digital traps, misdirect and divert attackers, configure honeypots, mitigate encrypted crimeware, and identify malicious software groups. The expert authors provide full coverage of legal and ethical issues, operational vetting, and security team management.

Securing Mobile Devices

by ISACA

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

WEB DOWNLOAD
Product Code: WCB5SMD1
Member / Nonmember: FREE / $75.00

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. The secondary purpose is to provide guidance on how to embed security for mobile devices in a corporate governance, risk management and compliance (GRC) strategy using COBIT 5 as the overarching framework for GRC.

CISA® Online Review Course

Certified Information Systems Auditor®
An ISACA® Certification

DELIVERY METHOD
Online, self-paced

DURATION
Approximately
23 hours & 20 minutes

SUBSCRIPTION
1 year access to the course

PRICE
ISACA Members: $795
Nonmembers: $895

COURSE DESCRIPTION
This online review course prepares anyone registered for the CISA certification exam using proven instructional design techniques in an interactive environment. The course covers all five of the CISA domains — each section corresponding directly to a different CISA job practice. The course incorporates video; interactive eLearning modules; downloadable, interactive workbooks; downloadable job aids; case study activities and pre-and-post-course assessments. Navigate this course at your own pace, either following the recommended structure, or targeting your preferred job practice areas. Be free to start and stop the course based on your study schedule, picking up exactly where you leave off.

LEARNING OBJECTIVES
At the end of this course, you will:

- Be familiar with the benefits of CISA certification and the CISA exam structure
- Have valuable success strategies for passing the CISA exam
- Understand, in-depth, the CISA task statements and how they relate to CISA knowledge statements
- Be able to practically apply IS audit and assurance concepts

WHO SHOULD ATTEND

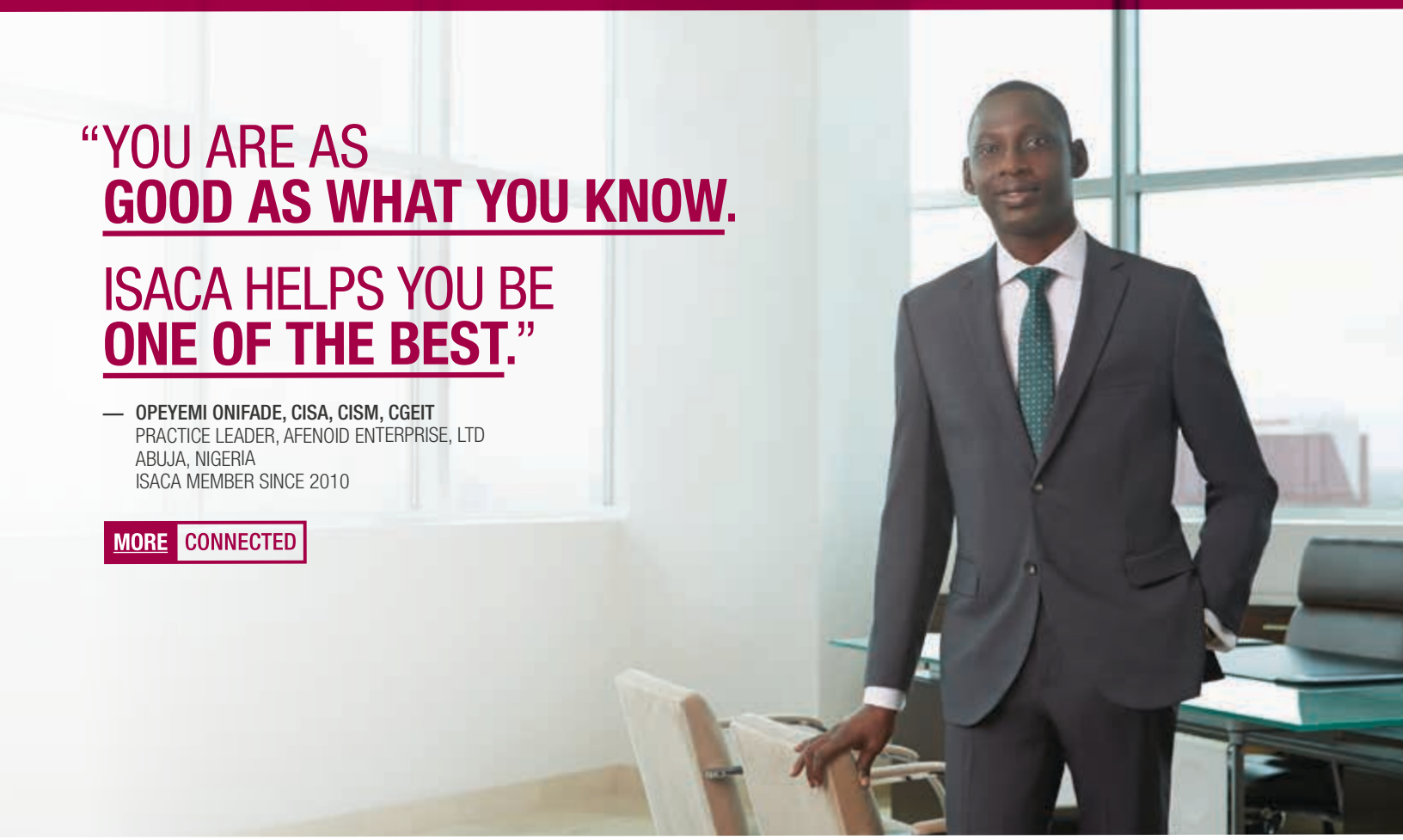
- Professionals with 3-5 years' experience; preparing to become CISA certified
- Professionals with 5+ years of experience who want the CISA credential for career development
- Financial auditors moving into IT audit
- IT generalist moving into IT audit
- Mid-level career change
- Students or recent graduates

CPE HOURS
28

LEVEL
Beginner – Intermediate

FOR MORE INFORMATION
https://support.isaca.org

SUCCESS DEMANDS AN EDGE. ISACA® IS THAT EDGE.



"YOU ARE AS **GOOD AS WHAT YOU KNOW.**

ISACA HELPS YOU BE **ONE OF THE BEST."**

— **OPEYEMI ONIFADE, CISA, CISM, CGEIT**
PRACTICE LEADER, AFENOID ENTERPRISE, LTD
ABUJA, NIGERIA
ISACA MEMBER SINCE 2010

MORE CONNECTED

TECHNOLOGY IS ALWAYS EVOLVING.

Established more than 45 years ago, ISACA is a trusted source of knowledge, networking, education and career development for IS/IT audit, control, compliance, security, cyber security, risk, privacy and governance professionals. Through our global community, we inspire and equip individuals to be more capable, valued and successful in the ever-changing world of information systems, information technology and business.

Continue to be a part of our global community of talent—Renew today!
www.isaca.org/renew17-Jv1

MAINTAIN YOUR EDGE!

Renew your ISACA membership today!

www.isaca.org/renew17-Jv1

ISACA®
Trust in, and value from, information systems

Networking | Certifications | Research and Best Practices | Continuing Education | COBIT® 5 | And much more!

TOMORROW'S SECURITY IS HERE

Do more with integrated security management solutions — the Skybox® Security Suite

SKYBOX™ SECURITY

Total Visibility. Focused Protection.™

www.skyboxsecurity.com

Evolve and see what you're missing.

Unify data from 90+ security vendors. Gain end-to-end attack surface visibility using network modeling, attack simulation and analytics. Automate the prioritization of critical exposures in context.

Threat and Vulnerability Management | Security Policy Managment