ISACA

Journal

VOLUME 4, 2023

THE EVOLUTION OF THE GLOBAL INFORMATION ENVIRONMENT

EFFECTIVE GOVERNANCE AND BOARD OVERSIGHT IN A GLOBALIZED INFORMATION ENVIRONMENT

INTERNAL AUDIT AS A DRIVER OF INNOVATION

SOLVING STANDARDS IMPLEMENTATION ISSUES WITH A GLOBAL ISMS

ISACA.ORG

Become Empowered to Advance Digital Trust

Join ISACA® in Dublin, Ireland on 17–19 October for ISACA Europe Conference 2023: Digital Trust World

Expand your knowledge. Connect with influential industry leaders. Find inspiration from the world's brightest minds in digital trust. Forge your own path with a customizable program of dozens of interactive sessions. Earn up to 20.25 CPE credits. Empower yourself with the knowledge to advance digital trust in your organization. Plus, save US$300 off your registration through 1 September.

www.isaca.org/Dublin-jv4

DIGITAL TRUST WORLD

An ISACA® Conference

Thank You to Our Digital Trust World Premium Sponsors!

ISACA® wishes to send a big THANK YOU to all of our ISACA North America Conference 2023: Digital Trust World Sponsors! Your hard work and support helps our vision of working to create a safe digital space for all become a reality. We couldn't do this without you and greatly appreciate your partnership with us!

A-LIGN · Accedere · Adobe · ARCHER · AUDITBOARD

BDO · bringa · cisco · Cobalt · COHESITY · digicert

Diligent · hyperproof · IANS · INFOSEC · LEVEL 6 CYBERSECURITY INC

levelup CONSULTING PARTNERS · LOGICGATE · Microsoft · onetrust · ProcessUnity

protiviti Global Business Consulting · RiskOptics FORMERLY RECIPROCITY · RSM · servicenow · SYNOPSYS · Telos

TESSIAN · THREATLOCKER ZERO TRUST ENDPOINT PROTECTION PLATFORM · TRACEABLE · TRAINING CAMP · VANGUARD INTEGRITY PROFESSIONALS CYBERSECURITY EXPERTS

DIGITAL TRUST WORLD

An ISACA® Conference

To learn more about ISACA sponsors, please visit www.isaca.org/boston-sponsors-jv4.

Contents

DEPARTMENTS

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 July and August:

Analyzing Privacy Policies as Data
THIAGO DE OLIVEIRA TEODORO, CISA, CDPSE

Log Management as an Enabler for Data Protection and Automated Threat Detection
GRANT HUGHES, CISA, CISM, CDPSE, CCSP, CEH, CISSP

Three Lessons From 100 Years of Data Management
GUY PEARCE, CGEIT, CDPSE

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505
Fax: +1.847.253.1755
Web: www.isaca.org

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 information technology, IT audit, risk, governance, privacy, security, assurance and emerging technology.

READ MORE FROM THESE *JOURNAL* AUTHORS...

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

/ISACANews

/ISACAOfficial

ISACAHQ

/isacanews/

Selling Security's Value Proposition

In the recent past, three things occurred at roughly the same time. I recorded an interview concerning a recent article in this space about advertising information security.[1] ISACA® issued a survey report on the state of privacy in 2023.[2] And some colleagues of mine published an article entitled, "ESG Is Dead—Long Live ESG."[3] This confluence of events kicked off some thoughts in my mind, which I would like to share.

> Privacy specifically and information security generally should always be considered as part of any organization's achievement of its mission.

Advertising Information Security

To recap the interview and the article it was based on, I had noticed that vendors of hardware, software and information technology services were advertising the security of their products on television. I wondered why businesses that implemented these products were not touting the ways that they secured information, especially that of their customers. My opinion is that these organizations were fearful that the goodwill that such ads might generate could be wiped out by a single cyberattack. In conclusion, I wrote that information security professionals "should aid their marketing departments in developing ad campaigns featuring what is being done to protect customers' information."[4]

Privacy and Profit

In the privacy report, there is an analysis of survey results on how boards of directors view privacy programs. The alternatives given were compliance-driven and ethics-driven. I was intrigued by the question not asked: There was no option for *profit-driven*.[5] I believe that directors of private-sector companies should always be considering profits, with no disrespect to compliance or ethics. Those organizations that are not driven to make money (e.g., the public sector, nongovernment organizations [NGOs]) should be *mission-driven*. The point is that privacy specifically and information security generally should always be considered as part of any organization's achievement of its mission.

Environmental, Social and Governance

ESG is a common acronym (at least in investment circles) for environmental, social and governance. The term implies that investments should be made with consideration of factors that go beyond financial returns. In some political circles, this is said to be "woke capitalism." In others, it is thought that investors should be doing good as well as making money. Just as I would never offer legal advice, I will not give investment advice. (Believe me, you do not want my investment advice.) But I will frame the argument in terms that are relevant to information security.

STEVEN J. ROSS | CISA, CDPSE, AFBCI, MBCP

Is executive principal of Risk Masters International LLC. He has been writing one of the *Journal*'s most popular columns since 1998. Ross was inducted into the ISACA® Hall of Fame in 2022. He can be reached at stross@riskmastersintl.com.

LOOKING FOR MORE?

- Read *Governance Roundup–What Are You Doing About Environmental, Social and Governance Factors in Your Enterprise? www.isaca.org/governance-roundup-esg*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

I believe that information security contributes both socially and in terms of governance. We humans cannot maintain meaningful social coherence without security overall. To the degree that our digitized world is fueled by information, much of it personal information, security provides the sinews that hold the body politic together. To those who argue against ESG, I would ask: Would you invest in a company that did not have sufficient security? Would you run a company that way?

As I see it, information security may or may not be tied directly to profits, but it definitely adds value to an enterprise: shareholder value in the case of publicly traded corporations; taxpayer value for the public sector. The problem is that we who specialize in the field have done a poor job of demonstrating that value. I suggest that we have been valuing and evaluating security based on the absence of breaches. In other words, we have put the burden of proof for information security into the hands of criminals. This is not an ideal marketing strategy. A much more positive approach is to project the value of security in terms of quality, reliability and value to the customer.

It is a truism—or at least it ought to be—that secure systems are better systems.

Security and Quality

Quality sells. This is true for everything from automobiles to zippers. It is a truism—or at least it ought to be—that secure systems are better systems. To achieve an acceptable level of security, designers must first reach a consensus on how secure their systems must be. Those that contribute to national defense require a higher level of security than those that, say, keep the bowling league scores. Software developers must work toward that consensus, while balancing factors including cost, time to market, customer demand, minimum customer acceptance and ease of use. Seeing security as a critical attribute[6] of systems leads to greater care in design, coding, testing and distribution. Hence my statement about the quality of secure systems.

It follows that the quality of security is, from a customer perspective, a leading indicator of overall quality. Sales representatives need not claim that their products are impervious to all threats. They need only demonstrate the features and functionality that contribute to security to aid in the sale, if not to close the deal, and to assist buyers in justifying the purchase to their management.

Security and Reliability

I have written before that downtime is "the most significant metric of contemporary cyberattacks."[7] Nearly every enterprise does some business on the Internet, if only to display its advertising. If its Internet presence is down, it is effectively closing shop until the site can be restored. Now multiply that impact one hundredfold if a cyberattacker should close down all its systems.

From a business perspective, the issue is not so much availability as reliability of the enterprise for its customers and, to a lesser degree, for its suppliers. As long as systems are secure and can be protected from going down, the private sector can continue to make money and the public sector to carry out its missions. And if the preventive measures fail, rapid recovery is the next best thing. Reliability is a business objective in a way that fending off the bad guys can never be, and it is one that carries value in the marketplace.

Value to the Customer

An enterprise's customers will never know about the security software, the access controls, the disaster recovery plan, the network configuration, or any of the myriad controls and protections in their supplier's systems. Nor are customers really interested in these things. Their interest is in having some reasonable assurance that the data they give to the enterprise will not be disclosed; that the money they have deposited will not be stolen; that the products they order will arrive on time; and that the transactions they entered today will still be there tomorrow, unchanged. This implicit contract is the basis for customer loyalty, more enduring than free samples. Any salesperson knows the importance of retaining satisfied customers. To the degree that security is a contributor to retention, it adds to the bottom line.

If security professionals do not state profit and mission achievement as *raisons d'etre* for information security, no one else will do it. These factors are more comprehensible to people not attuned to the daily grind of keeping information in the hands of those authorized to use it and out of everyone else's. It is our story, and we should tell it.

Endnotes

1 Ross, S.; S. Kazi, "Advertising Information Security," ISACA® Page to Podcast, 28 February 2023, *https://www.youtube.com/watch?v=3tEZ8dF8z4k*. ISACA, thinking that I have not subtracted enough from the sum of human knowledge with my bimonthly column, has of late been recording interviews about the articles with me on its podcast.

2 ISACA, *Privacy in Practice 2023*, USA, 2023, *https://www.isaca.org/resources/reports/privacy-in-practice-2023-report*

3 Johnson, K.; R. Funston; T. Reeves; "ESG Is Dead—Long Live ESG: Guidance for US Pension Fiduciaries," Funston Advisory Services, 2023, *https://www.funstonadv.com/in-the-news/esg-is-dead-long-live-esg-guidance-for-us-pension-fiduciaries*

4 Ross, S.; "Advertising Information Security," *ISACA® Journal* vol. 1 2023, *https://www.isaca.org/archives*

5 I have addressed this general topic before in this space: Ross, S.; "What Is the Value of Security?" *ISACA Journal*, vol. 2, 2011, *https://www.isaca.org/archives*. I came from a different starting point at that time.

6 Security by design, if you will allow my borrowing the term.

7 Ross, S.; "It's About (Down) Time," *ISACA Journal*, vol. 5, 2022, *https://www.isaca.org/archives*

Changing the Healthcare Paradigm

Risk Challenges With Interactive EHRs

The medical paper trail is one that many have closely safeguarded over the course of their lives. Somewhere, I still have paper records that my parents carefully preserved related to eyesight issues, childhood inoculations, fractures and irregularities that doctors and dentists considered worthy of documenting. With healthcare very much a specialty-driven industry, maintaining one's own paper records was hard enough to coordinate. Going further to get relevant medical data from relatives was often impossible. That changed in the United States in 2014 when the US American Recovery and Reinvestment Act mandated the "meaningful use" of electronic health records (EHRs) to:

- Improve quality, safety and efficiency and reduce health disparities.
- Engage patients and families.
- Improve case coordination.
- Maintain the privacy and security of patient health information.[1]

Now, almost 10 years after the mandate, case coordination and patient and family engagement in the United States has changed dramatically from the prior exchange of paper folders and notes to portal-enabled access to patient information. As Jenna, a healthcare worker who is diligent about managing her own records told me, "I want to know all the options the medical teams are considering about me, not just their final choices of care."

There are many benefits of this technology revolution, but are the data being used with an eye toward understanding the risk involved? Do healthcare providers adequately inform their patients to build digital trust with patients and families? Has the industry become better at effective collaboration because of the availability of EHRs? These are questions the risk manager needs to assess with the business team. An integrated approach allows much needed collaboration between the medical team users and the IT software developers, while ensuring that risk managers and the first line of defense (FLOD) are able to build a governance model with appropriate controls so critical healthcare uses receive due attention.

Fast Forward From the Paper Trail

The world of portal-enabled access to patient information is a two-way street, bringing patient care teams together for better patient outcomes and bringing family members together to collaborate on choices their loved ones may have to make. Connected healthcare institutions can generate full patient data profiles that include test results, appointment records from participating care providers, medication lists, medical questions and answers, and medical instructions given to the patient from all parties involved. Test results are often accessible to patients even before they are contacted by their doctors.

In addition, it is not only hospitals, doctors and labs that can get authorization to access and collaborate on the data. The data can also be made available on sites such as Ancestry.com and to research programs such

CINDY BAXTER | CISA, ITIL FOUNDATION

Is director at What's the Risk, LLC. Her practice focuses on integrated risk control and process assessments for cybersecurity, privacy and business continuity/disaster recovery. She views risk management and control assessment as opportunities to learn the nuts and bolts of a business and help her clients worry less because gaps have been uncovered and a stronger operating model can be built. Baxter draws upon her experience in banking, insurance, healthcare and technology after holding compliance and management roles at State Street Corporation, American International Group (AIG), Johnson & Johnson and AT&T. When she is not doing risk and audit work, she enjoys volunteering on climate and environmental issues that impact her community.

the US National Institutes of Health (NIH) All of Us Program[2] if the patient authorizes access. No longer does one need to maintain a paper file. Now, data from DNA results to x-rays to blood tests can be retrieved online and stored as soft copies.

How EHRs Work

Epic, a popular software provider,[3] uses Software-as-a-Service (SaaS) technology to provide cloud-based EHRs with open-source integration that complies with HL7 requirements.[4] The HL7 standards cover the full healthcare cycle with regard to taxonomy, implementation guides, document architecture, interoperability and templates for clinical notes.[5] With portal-based entry to a cached database, Epic has both web and application-based access available to users and is, therefore, agnostic to the browser or hardware access method used. Standard security on the patient side allows for a login ID and password, with multifactor authentication (MFA) available if desired by the users and institutions. Institutional users must meet the regulatory requirements of the US Health Insurance Portability and Accountability Act (HIPAA). Some healthcare providers choose to go above and beyond the standard HL7 requirements. The programming language used by Epic is a version of the Massachusetts General Hospital Utility Multi-Programing System (MUMPS).[6]

Establishment of appropriate risk profiles and controls for the software that enables the EHR information exchange is critical.

Getting User Risk Right

There are several challenges that come with extending EHR use beyond the strict regulatory climate that dictates software security, privacy and accessibility. The audiences are often nontechnical, and even when they are familiar with technology, they are not expert coordinators or collaborators. With diverse user groups that include patients and family members, medical staff across multiple institutions who have knowledge in varying disciplines, and researchers that include student populations and experts in the field, there is not one single road map for ensuring appropriate use.

Instead, multiple risk models, control sets and audit programs need to be considered. Establishment of appropriate risk profiles and controls for the software that enables the EHR information exchange is critical. ISACA® professionals can guide the audiences that use the provided risk assessments and audit results.

Given the mandated use of EHRs, the risk question is not to assess whether to provide electronic documentation, but rather to assess the choices made when selecting providers, managing compliant implementations and establishing governance models that monitor user audiences. Tackling user risk assessment and control development presents special challenges, meaning the practitioner must understand the user operating model and offer an interactive control framework for healthcare providers and governance managers. As information providers, medical users can present a risk to their client base of patient users if they do not recognize and use the software as intended based on the HL7 requirements of "meaningful use."

The patient-doctor relationship is recognized as a key component of collaborative care, yet electronic data typically do not get the relationship attention to ensure that the data are understood, creating a high risk. The other key user communities are the specialist teams themselves, who, in the best case scenario, consume data and interact on behalf of the patient with other care team members. Facilitation through the lead or coordinating physician, if there is one, is equally important to assess whether the massive amounts of data are being used efficiently and effectively. If not, the risk of inappropriate data use can occur. Risk assessment and governance controls should be used to examine both the

Governance and controls must evaluate the effectiveness of building a collaborative model instead of simply a model that ensures that the patient understands the medical recommendation under review.

patient-doctor user group and the medical team user group not only to assess whether the most benefit is being derived from the software, but to live up to the EHR "meaningful use" requirements for all users involved.

Mitigating Risk by Assessing Care Provider Collaboration

Gone are the days when nurses needed to page doctors during off hours to interpret bad penmanship on patient records. But EHRs, with large quantities of data and the high number of specialists consuming the data, can create a knowledge silo effect with different pieces of data used to arrive at potentially incomplete or incorrect conclusions based on the user's backgrounds and skill sets. Two questions arise:

1. Are data being overlooked or misunderstood?
2. Is there actually time to strive for the kind of medical team collaboration that can bring about more robust patient outcomes?

These two risk scenarios must be evaluated by the risk manager by walking in the shoes of the medical user, with sufficient knowledge to understand the options and environments in which the care teams must work. This is where working with the business partners to secure knowledge for a risk walkthrough is critical. A careful risk assessment review can garner advantages, for example:

- Baseline requirements can be assessed by the IT team and the healthcare specialist team. Their input can expose difficulties the care team may encounter in utilizing the full data set. Reviews of user requirements across all providers within the care team help outline data consolidation opportunities that may reduce the risk of unused or misunderstood data.
- Information delivery can be refined to a model that allows push and query. Information that is necessary for timely diagnosis should be evaluated as high risk if not reviewed and pushed to users at a frequency that meets their needs. Other information can be considered for query availability—visible as soundbites to users but available via a link on the web portal if desired vs. added to the mountain of information.
- Risk factors can be assessed based on case complexity. A patient case requiring x-rays for a potential bone fracture carries a low risk of data being ignored or misunderstood, while a patient case involving potential transplant, with existing conditions such as diabetes and cardiovascular complications, is high risk for misuse of data—not only because the team of specialists is exponentially larger, but also because the data lake grows to monumental proportions when multiple tests are ordered to determine next steps.

Understanding the risk factors of ubiquitous data and creating a governance model with controls that mitigate data overload for the medical community is an important contribution for risk professionals to make. But it is only the start. Step one of the patient user risk assessment is an evaluation of healthcare provider knowledge of the software and the governance model used to build awareness and knowledge with patients. Governance and controls must evaluate the effectiveness of building a collaborative model instead of simply a model that ensures that the patient understands the medical recommendation under review.

In fact, awareness is the key control point for successful collaboration not only to foster a solid understanding of the data, but to allow patients to make appropriate decisions regarding granting access of their information to others, whether it is for research by the medical community or for inclusion of family members and friends in the decision-making process. The risk of choice has always been a hot topic, but with the need for data accuracy evaluation and the risk and opportunity of new software enhancements, including artificial intelligence (AI), to manage patient data information, proper risk assessment and establishment of tight control environments are essential, while making sure data are delivered as quickly as needed.

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Conclusion

Medicine in the 21st century is still science and art. Each time a data model points to predictability in terms of potential treatments and next steps for care, there are nuances because, after all, we are all unique. Some ways audit and risk professionals can help include:

- Walk in the shoes of all user communities. Make sure the system and software are designed with intuitive instructions.
- Dig into the end-user patient experience. Has access been granted by the patient to others because of appropriate patient awareness and knowledge?
- Probe to find out whether the risk of obtaining data has been adequately explained and vetted. Have implications such as health insurability been discussed?
- Understand the dynamics of the care team user community. Does the lead clinician involve the patient in reviewing all options? Does involvement of family members aid or detract from patient acceptance of treatment? Have treatment decisions been made as a result of collaboration, or is there too much data for the care team to humanly process and only a handful are making decisions?
- After evaluating the risk and examining where controls can be most effective, document the gaps where the system or software can be improved. Highlight the software elements that are most appealing and most often used by the user communities.

As in many other fields, advances in medical technology are occurring at a breakneck pace. Risk management, governance and controls, audit verification, and validation that the intended use and benefits of the software are achieved help elevate the maturity of the healthcare information flow and benefit both medical users and patient users alike.

Endnotes

1 HealthIT.gov, "Meaningful Use," Office of the National Coordinator for Health Information Technology (ONC), USA, *https://www.healthit.gov/faq/what-meaningful-use*
2 National Institutes of Health, All of Us Research Program, USA, *https://allofus.nih.gov/*
3 Epic, "In a Nutshell," *https://www.epic.com/about*
4 HL7 International, Standards-Based Product Grid, *https://www.hl7.org/implement/standards/product_matrix.cfm*
5 *Ibid.*
6 Epic, "From Healthcare to Mapping the Milky Way: Five Things You Didn't Know About Epic's Tech," 10 February 2020, *https://www.epic.com/epic/post/healthcare-mapping-milky-way-5-things-didnt-know-epics-tech*

Balancing Risk and Innovation

JOHN DE SANTIS

Is a company builder with experience in the software, networking and information security domains. He has more than 40 years of international and US-based experience at venture-backed technology start-ups and large global public companies in the telecom and IT fields. He serves on the boards of directors in fiduciary or advisory capacities for organizations active in cybersecurity, artificial intelligence, professional development and learning innovation, including Paladin Cloud, Cequence Security and ValiMail, leading innovators in the cybersecurity space, and NoHold and Tweelin, early stage innovators in the application of artificial intelligence. De Santis is a dual citizen of Italy and the United States and maintains homes in both countries. He has lived and worked in Europe and the United Kingdom for more than 20 years.

Q: As the incoming chair of the ISACA® Board of Directors, how do you see ISACA growing and adapting to the constantly changing workplace and needs of its constituents over the next year?

A: The careers we have chosen have placed us in the center of a relentless and dizzying whirlwind of innovation and creativity. Every day we learn of some new technological breakthrough—new gadgets, new applications, new infrastructure models and new tools. Physical borders are artificial constructs that mean nothing in a cloud-based world. Cars are Internet-connected and have dozens of microprocessors managing their performance. Software programs are diagnosing our health, customer service is delivered by intelligent bots, your calendar is optimized by algorithms, news services have become real-time data analysts and deliver content services meant to entertain rather than inform. If unburdened by principles, these new things can do harm either by intent or by omission.

I see the work of ISACA as the rock, the true north, in this whirlwind. We have to work diligently and curiously to first understand these new ideas, thoughtfully predict and prepare for their implications, and then apply timeless principles and frameworks to help our enterprises, our innovators, and our government agencies ensure outcomes that are good and trustworthy.

Q: What in your past experience has best prepared you for this position on the ISACA Board?

A: I have held senior positions in companies and on boards since the early 2000s at for-profit and not-for-profit organizations, both small and large, in a wide variety of domains including technology, education, sports and religious organizations. Board roles have been a great source of personal satisfaction for me providing opportunities for strategic thinking, collaboration with very smart people, big problem solving, and learning how to ask important probing questions with grace, tact, and respect. I pride myself on being able to influence direction and action by not being directive or prescriptive, but by asking thoughtfully crafted questions and letting the listener learn from the question and find the right path forward themselves. Some call it the Socratic method—my wife calls it nonintrusive brain surgery. I have had some great board mentors along the way, and I have seen some very bad board members too, and both have been helpful in shaping and preparing me for this role.

Q: What do you see as the biggest risk factors being addressed by ISACA constituents? How can organizations protect themselves?

A: New technologies, tools and applications are exciting and fun to build, implement and use. Sometimes, their usage can lead to unintended consequences (e.g., compromised privacy, data leakage, compliance violations, back doors left open), and for me, not being able to discern between good and bad is the biggest risk. For many, it is easier to just say no to these innovations, but opportunities may be missed. I believe ISACA has a role to play to quickly identify both the benefits and risk of using these new things, and then quickly suggest or recommend ways to respond to the risk while allowing the benefits of innovation to be harvested. And then do it again and again, because technology does not stand still.

Q: How do you see the role of executives changing to meet the challenges of information and cybersecurity?

A: It starts with good systems hygiene maintained by continuous monitoring and remediation, and when (not if) something bad happens, being prepared to respond quickly and effectively. Much like building a home, one needs to budget not only for good foundations, insulation, doors, windows, and locks, but also for their upkeep—to set aside reserves for unknown new challenges and opportunities, and to plan what to do when something threatens the house (i.e., weather, infrastructure services interruptions, and so on).

Systems are the same way. Ample thought should be given to analysis of not only how the system is built, but also how it is maintained, how threats may find their way in, how teams can respond to those threats, and how, eventually, the system may be decommissioned and data transferred to inform the next technological wave. Executives should have the wisdom and foresight to challenge their teams' thinking throughout this life cycle, develop plans and fight for budgets supporting those plans.

Q: What do you think are the most effective ways to address the skills and gender gaps in the technology space?

A: I believe, in the short term, that addressing the skills and gender gaps starts with anticipating where and what the jobs will be in the near future, offering easy on-ramps to professional educational opportunities to address those needs, generating enthusiasm and excitement to participate, and helping younger and returning workers identify if they have an aptitude and inclination to enjoy that type of work. We should encourage and motivate employers to invest in their people's skill development to adapt to rapidly changing technologies.

Regarding gender—and even race—gaps, I find it incredibly frustrating that in 2023, we still have cultural speed bumps, roadblocks and income disparities. We should celebrate and hold up as exemplars leaders who have overcome those challenges. More important, we should be good colleagues and mentors who "pull up" those who show interest, enthusiasm and ambition, and help them find their unique paths to success.

Q: How do you view certifications and the impact they have on careers?

A: The certification world is a new one for me. ISACA has opened my eyes to the consummate professionalism of this community and the generosity of sharing time, talent and expertise to improve our world.

I must admit, in the past I was skeptical about folks who had too many acronyms after their names on their business cards, but I have come to realize how amazingly efficient and effective ISACA professionals are. When first approached to join the ISACA board, I became hungry to learn more. If the kind of training ISACA offers was provided to the software development teams I managed, how much time we would have saved building stronger products. And how helpful it would have been if my software developers had some inkling of the rigors needed to pass audits! I am a believer now.

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

A: In my first CEO role, I was just closing a critical round of funding in early September of 2001 when we only had two weeks of cash left in the bank—just in time, right? In the short span of a few days, our competitors tried to stop the funding by suing us for patent infringement, my oldest son was diagnosed with cancer, the 9/11 tragedy happened in the United States, and my best friend was on the second plane to fly into the World Trade Center towers. The venture fund leading the round panicked and pulled out leaving us broke and almost broken. Frankly, I do not know how I got through it all.

Buckling down and ferociously compartmentalizing, I took money out of our home equity line of credit to make payroll—twice—and then told my wife. Fortunately, our marriage survived that lack of judgment on my part and the courage to fund the company myself attracted even better investors. Although my son eventually passed away, the ordeal did bring our family closer together. That loving bond—born of shared adversity and mutual comfort—holds us tight to this day. Our company fought back and our competitors eventually agreed to a settlement, which immediately triggered a very advantageous sale with an outstanding outcome for our employees and shareholders. I still grieve the loss of my friend, but his family and ours remain very connected, and we visit each other often, creating happy new memories.

1 **What is the biggest information security challenge being faced in 2023 and how should it be addressed?**

We are being inundated by real and imagined threats and countless solutions claiming to be silver bullets. Each of us must use our intellect, experience and wisdom—leveraging the amazing combined knowledge of the ISACA community—to determine what specific challenges to our organizations are probable, real and imminent, and what we should do about them.

2 **What are your three goals for 2023?**

- Help ISACA's new CEO get oriented to understand the organization and assess how to move forward
- Help new board members gain a deep understanding of the opportunities, risk areas, strengths and weaknesses of the organization, and apply their experience and skills to help ISACA succeed
- Ensure and maintain ISACA's well-established board governance hygiene and sound decision-making

3 **What is on your desk right now?**

A long list of to-do items. Also, a book: *The VC Field Guide: Fundamentals of Venture Capital* by William Lin, who provides an excellent framework for how to think about investing in innovative ideas and teams, and getting the timing right.

4 **What is your number-one piece of advice for cybersecurity professionals?**

Focus on discovering first principles—understand the fundamental assumptions underlying decisions or conclusions, and then build from there.

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

All my life, my hedge against technology has been agriculture. My brother and I share a home and olive orchards in Italy, and we make a little olive oil for our friends and extended family. Also, my wife and I are restoring an old family farm in the US State of Vermont close to the Canadian border. We make maple syrup, harvest timber, clear fields and put up fencing to prepare for raising beef cattle. And we are bringing a cozy little mid-1800s farmhouse and barn back to life. It is a wild and beautiful place that keeps me grounded, healthy, outside—and I get to drive a tractor!

Digital Trust—An Enterprise Approach

The first time I looked at the details of the Digital Trust Ecosystem Framework (DTEF),[1] I was struck with how many parts of the enterprise are included in the overall effort. Logically, standard IT and information security play crucial roles. However, a full implementation includes human resources (HR), communications/marketing, and enterprise architecture (EA). Since an organization's digital trustworthiness is partially based on how its brand is perceived, communications/marketing makes sense. But what about HR? Yes, even HR has a role to play in this framework because the DTEF includes culture as an important aspect, marking it as one of the domains for the framework. If one peels back the layers of the DTEF, one can readily see that no part of the enterprise is insignificant or exempt from the framework.

K. BRIAN KELLEY | CISA, CDPSE, CSPO, MCSE, SECURITY+

Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server and Windows Server. He has served in a myriad of other positions, including senior database administrator, data warehouse architect, web developer, incident response team lead and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camps and user groups.

Regarding the enterprise, it is important to focus on two domains that expect the full participation of every part of the enterprise in any organization: *Culture* and *Architecture*.

The Culture Domain

Part of what the DTEF defines as culture is a typical HR responsibility: managing skills and competencies. *Manage Skills and Competencies* is one of the three trust factors in the *Culture* domain. If you are not familiar with trust factors, they represent specific portions of the domain on which an organization is able to act. The actions for the *Manage Skills and Competencies* trust factor are similar to other capability maturity models (CMM): identifying the necessary skills for the CMM, providing resources to ensure that employees are able to gain those necessary skills, identifying gaps in employees' skill sets, and providing the required training using the identified resources.

There are two additional trust factors in the *Culture* domain: *Manage Culture* and *Create and Manage the Digital Trust Cultural Environment*. When looking at these two trust factors, one can start to see responsibilities across the enterprise.

Manage Culture

The first trust factor, *Manage Culture*, starts with identifying the organization's current culture, evaluating it against what the target culture should be, and continually measuring, evaluating and adjusting it by promoting what the target state should be. How is the target culture promoted? Part of it is communicating what that culture should be, but the framework also includes activities to communicate decisions, helpful behaviors, results from attempts to adjust toward the target state, and lessons learned from those decisions. Also, there is an expectation of senior management backing the culture change and

modeling "trust-strengthening behaviors at all levels of the organization,"[2] which are typically necessary to affect change.

Create and Manage the Digital Trust Cultural Environment

The second trust factor, *Create and Manage the Digital Trust Cultural Environment*, starts with designing the digital trust cultural context—that is, evaluating the organization's current state in conjunction with where the organization wants to be as its target state. The communications factor is addressed next, and it is heavy. Each trust factor is further broken down into practices, and within those practices there are activities. The practice around communications has a number of key activities that focus on understanding what to communicate, how to communicate, the importance of communicating continually, and how to ensure that what is communicated can be tied back to the mission, goals, objectives, processes and procedures, and other aspects that are part of the operations and expectations of the organization.

Naturally, if an organization is going to focus on culture, it needs to be structured effectively for that culture. Roles and responsibilities should be well defined. The skills needed for each role should also be clearly understood and documented. This meshes with the trust factor of *Manage Skills and Competencies* and there are a great deal of interwoven expectations with the DTEF, much as one would see in other frameworks. The *Culture* domain is also where branding comes in, and efforts around managing reputation. All of these are part of the trust factor *Create and Manage the Digital Trust Cultural Environment*. And all of these encompass every level and structure within an organization. For instance, if IT is not able to deliver on services, organizational reputation is going to be negatively affected. Communications and marketing can only do so much. If customer support is lacking, customers will complain, and the organization's brand and reputation will be damaged despite heroic efforts in other areas of the organization.

The Architecture Domain

I have been a member of an organization's EA group and, in my experience, there are a few well-known frameworks for different aspects of architecture. However, the most well known is arguably The Open Group Architectural Framework (TOGAF).[3] TOGAF is now more than a framework. It also includes a methodology, the Architectural Development Method (ADM), but here the focus is on the framework component. In the TOGAF framework, there are four domains: business, data, application and technology (BDAT). The business, data and application domains are what one would surmise. The technology domain may require a bit more explanation. Basically, technology comprises the underlying hardware and infrastructure to make the other domains work. Not surprisingly, the first trust factor in the DTEF *Architecture* domain, *Create Enterprise Trust Architecture*, includes a separate practice for each BDAT domain. The DTEF was designed to mesh well with other existing frameworks and the focus on BDAT is a great example of how the DTEF overlaps with TOGAF for EA.

Looking at each trust factor, it is clear that each aligns with the traditional expectations of what EA is intended to perform for an enterprise organization.

The other trust factors in *Architecture* are *Manage Information and Technology Architecture, Manage Digital Trust Resources*, and *Align Digital Trust Technology With Organizational Needs*. Looking at each trust factor, it is clear that each aligns with the traditional expectations of what EA is intended to perform for an enterprise organization.

Manage Information and Technology Architecture

Manage Information and Technology Architecture concerns itself with the life cycle of assets—whether those assets are properly fulfilling the role they should be performing in the organization; whether they are available, recoverable and resilient to the requirements of the enterprise; and whether integrity is maintained at all levels of the information and technology stack, including the supply chain. Again, all levels and parts of the enterprise are involved in this trust factor.

Manage Digital Trust Resources

Manage Digital Trust Resources focuses on the maintenance and day-to-day health of the various information and technology assets. Are patches being applied? Is performance sufficient? Are appropriate

LOOKING FOR MORE?

- Read In *Pursuit of Digital Trust. www.isaca.org/digital-trust*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

> Where there are gaps between current architecture and target architecture, EA should be driving the organization to eliminate those gaps.

controls and monitoring in place? Is the physical infrastructure, including facilities, functioning to meet the needs of the organization? What about cloud and outsourced resources? Are they sufficient, and does the organization have reasonable assurance around their health and security? Once again, these efforts reach out to most, if not all, parts of the enterprise.

Align Digital Trust Technology With Organizational Needs

Finally, *Align Digital Trust Technology With Organizational Needs* is a key responsibility for EA in general. EA should be aligning technology to meet the business needs, both in the present (current architecture) and for the future (target architecture). Where there are gaps between current and target architecture, EA should be driving the organizational change to eliminate those gaps. Within the DTEF, EA is expected to do the same.

The DTEF Involves the Entire Enterprise

There are frameworks that basically sit in one or two departments within an enterprise organization. The DTEF is not one of those frameworks. The DTEF spans all parts of the enterprise, as can be clearly seen by examining either the *Culture* or *Architecture* domains. The *Culture* domain makes it clear that a digital trust culture has to be backed by senior management, communicated well and often throughout the organization, and modeled at all levels of the enterprise. Adopting a digital trust culture requires key decisions for change, and each of those decisions requires analysis with proper communication of results and lessons learned. The organization may need to be reshaped with new roles and responsibilities defined along with the skills required for those new roles. HR will need to ensure that proper training is available and that there is a program to eliminate gaps between the skill sets that are currently present within the organization and what the target state should be.

Likewise, *Architecture* focuses on information, infrastructure and technology assets for the organization. Those assets should meet the needs of the business, be properly maintained, and be designed to meet expectations around availability, recoverability and resilience. Where there are gaps between current architecture and target architecture, EA should be driving the organization to eliminate those gaps, much in the same way that HR should be working to eliminate gaps in skill sets. EA should also drive technology to align with the business. This requires a comprehensive effort across the enterprise to be successful.

And those are only two of the six domains of the DTEF. The other four domains have similar expectations for all parts of the enterprise to be engaged. This should not surprise anyone. After all, if one part of the organization is not able to meet expectations, that shortfall will have a negative effect on the organization's brand and reputation. Even if that impact is not seen outside of the organization, it will be felt inside the enterprise. If the issues are not eliminated, eventually a negative effect will be seen outside of the organization. We do not need the DTEF to teach us these axioms. However, the DTEF brings focus to the fact that maintaining or improving an organization's position with respect to brand and reputation, its standing within the digital trust ecosystem, requires every aspect of the enterprise to be successful.

Endnotes

1 ISACA®, Digital Trust Ecosystem Framework (DTEF), USA, 2022. The DTEF is currently in limited release. The most up-to-date information on ISACA's digital trust offerings can be found at *www.isaca.org/digital-trust*.
2 *Ibid.*
3 The Open Group, *TOGAF Standard, 10th Edition,* United Kingdom, 2022, *https://www.opengroup.org/togaf*

Making the Software Supply Chain Practical

The "global information environment"—the theme of this issue of the *ISACA® Journal*—can mean different things to different people. For some, it might mean navigating the complex web of international geopolitics and economics, while for others it might mean fully leveraging the cloud and the Internet of Things (IoT) to tap into new markets in new regions. Some might look at jurisdictional differences in privacy and other legislation, while others might focus on collaboration challenges across regions (e.g., effective productivity in distributed teams.) For me, the biggest elephant in the room is the supply chain—in particular, the software supply chain.

Now, I know what some of you are thinking. Perhaps you may be thinking that the past few years have generated a great deal of hype about the software supply chain, but relatively little in the way of actual practical utility. Or, perhaps less generously, that there has been a veritable nonstop parade of people telling us about how things like a software bill of materials (SBOM) will solve all software supply chain problems, and that this talk has translated into relatively little payoff for those of us in the trenches with actual problems to fix.

While this view is, perhaps, cynical, it is not unfair. It is a fact that there has been much hype about the software supply chain generally, and the SBOM concept specifically. It is also a fact that the SBOM renaissance many predicted has not come to pass. The fact of the matter, though, is that two things can be true at the same time: SBOM is not a panacea (and hype suggesting otherwise is misplaced), and if approached diligently, the exercise of producing and consuming an SBOM pays dividends. The difference, I would argue, is in how you approach it.

With that in mind, then, let us look at the software supply chain through the lens of an SBOM—what it is, how it can help you, and how you can adapt your own program to practically incorporate it.

What Is an SBOM?

In a nutshell, the purpose of an SBOM is to provide transparency into what comprises a particular piece of software, such as a business application, development library, or really any other software package or software component.

As an analogy, consider something like a material safety data sheet (MSDS) or even the ingredient list on a packaged food. For example, if you purchase a granola bar, the bar's packaging will contain a list of ingredients used to manufacture it. If you have a need to know what is in it because, for example, you have a certain dietary restriction, this information can help you make informed decisions. If you have a severe food allergy, such as to peanuts or tree nuts, or a food intolerance or illness such as celiac disease, this information is not just nice to have—it can literally be lifesaving.

The purpose of an SBOM is very similar: In one place, the consumer of a software application learns unambiguously what components are used in it. Why might anyone care what components are used in the creation and execution of the software in their environment? For a whole host of reasons. For example, consider what happens when someone discovers a vulnerability in a ubiquitous component, such as what happened with the Log4Shell vulnerability (CVE-2021-44228) in the popular Apache Log4j component. Many of us still remember the

ED MOYLE | CISSP

Is currently director of Software and Systems Security for Drake Software. In his 20 years in information security, Moyle has held numerous positions including director of thought leadership and research for ISACA®, application security principal for Adaptive Biotechnologies, senior security strategist with Savvis, senior manager with CTG, and vice president and information security officer for Merrill Lynch Investment Managers. Moyle is co-author of *Cryptographic Libraries for Developers* and *Practical Cybersecurity Architecture*, and a frequent contributor to the information security industry as an author, public speaker and analyst.

frustrating exercise of trying to find out from the vendors we use whether or not their software was impacted by it. The more helpful vendors (usually those on the larger side) put together informational resources such as support articles, statements on web pages, customer bulletins, and so on, that explained whether they were using it, and where, and detailing any risk exacerbating (or mitigating) factors that might effect customers. Frankly though, this type of response was uncommon. Most of us had to spend significant time emailing, calling, creating support tickets, and pestering vendors to learn whether the software supporting our businesses was benign or a ticking time bomb.

While most organizations had to go through at least some of those challenges, organizations that actually produced software had it worse. They not only had to engage in the exercise of determining whether or not their vendors used the component like everyone else, but also had to respond to a near-constant drumbeat of customers wanting that information, which is a harder question to answer than one might think. Today, most software employs dozens or hundreds of different components (some open source and some commercial), any of which could contain this particular item. On its own, that would be a difficult problem. But keep in mind that each of those components is, in turn, built using other components, which are, in turn, built using still more components, and so on. If you have never spent more than 120 hours trying to track down whether or not your supplier's supplier's supplier's supplier uses the XYZ open source library, take it from me, it will give you a new perspective when you do.

How You Can Use This

Of course, all of this raises the question of what we might do instead. Looking at it in a manner similar to how the person with a nut allergy views an ingredient list, one can start to see why an SBOM would be desirable. Used this way, an SBOM is like a shipping manifest: You can tell by looking at it what is contained within. You do not have to track anyone down, you do not have to make phone calls, and you do not have to open support tickets. You just look at the report.

For software vendors, the same thing holds true. Rather than having to dig into each individual component, you can instead draw upon the information in the report to readily answer the questions your customers are asking; and instead of having to report the status to each customer individually, you can prepare something once and distribute it to everyone. It reduces issues for both sides of the relationship.

Sounds great, right? Absolutely. Hence, the reason for all the hype.

Of course, the gotcha is that being able to either practically produce or consume SBOMs takes a great deal of work and planning. It requires a bit of automation, a great deal of *temet nosce* (i.e., self-awareness), and it is not something that can simply be concocted. There are some pretty solid logistical and engineering reasons for that. It is true on both sides, by the way—for both producers and consumers. Both sides of the usage equation take planning and effort.

To illustrate why it is true, let us say that tomorrow morning you arrive at the office and have a directory full of data sheets for all of the software you use in your enterprise and all the dependencies they have. This is putting aside the fact that (at least for large organizations) knowing what all that software is in the first place is a monumental piece of engineering in and of itself (let alone what features are in use for each product, how they are used, by whom, etc.), and that knowing what components comprise that software is a practical impossibility. Let us just wave a hand over all that and assume you know the answers to those questions and that somehow the documentation was made available to you with no additional work on your part. How much documentation do you think that would be? Dozens

of applications? Thousands? Tens of thousands? Now, start to consider how many individual and unique components are used in the creation of those applications. How many do you think you would have now? Tens or hundreds of thousands? Now consider how many components might be used to develop those. Millions? More?

At this point, you are only three orders in and you are talking about potentially hundreds of thousands or millions of individual components. Realistically it can "nest" to much more depth than just third order dependencies—meaning that the consumption of SBOMs requires an ability to organize, search and filter.

It is for exactly these reasons that the current SBOM standards require automation. I will not spend much time on the mechanics of the individual standards, but for reference they are:

- **CycloneDX**—An Open Web Application Security Project (OWASP) standard that utilizes XML or JSON to contain dependency information
- **Software Package Data Exchange (SPDX)**—An international standard (International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC] standard ISO/IEC 5962:2021) that specifies the format for codifying components, license information, etc.
- **Software Identification (SWID)**—An international standard (ISO/IEC 19770-2:2015) that provides mechanisms for how to contain and transmit information about software components

The fact that there are two ISO/IEC standards on the list should clue you into the fact that this is by no means a simple process. In large part, the complexity is driven by the incredibly complicated spider web of dependencies woven into even the simplest of applications that might be employed.

In terms of actually producing an SBOM, bear in mind that it almost certainly requires automated support to produce content using the machine-readable standards described herein.

Using an SBOM in Your Program

Despite the practical challenges in production and consumption of SBOMs, there are still compelling ways that you can use them in your software supply chain efforts. First and foremost, If you are an organization that produces software, understand that some of your customers will absolutely ask you for them. That may not be happening yet, but they will eventually. This means that you should have it in the back of your mind as you evaluate the tooling and processes you use. For example, if you are looking into modifications to your DevOps/DevSecOps tool chains, consider incorporating supply chain capability into that just as you would Static Application Security Testing (SAST) or quality assurance (QA) automation. Likewise, as you evaluate other software you might employ in the application space (e.g., SAST, Dynamic Application Security Testing [DAST], software composition analysis [SCA], Code Quality), consider the capabilities offered by those vendors in the supply chain space.

If this is front of mind, you will realize that many of the tools you might already be familiar with and/or use, such as SCA tools, can help—as can those that you might be using for things such as open source licensing compliance. Those tools can help in at least two ways. First, they can help you in the task of identifying what software you are using (and their supporting components). Second, they can assist in the generation of the data structures and packaging outlined in the previously listed standards.

From a process point of view, undertaking the exercise of actually trying to produce an SBOM can be enormously beneficial in a "journey is the destination" kind of way. That is, actually trying to do it forces you to build a better understanding of what you have in play—and it can help you build the automation to get to better levels of understanding and coverage. Your efforts out of the gate may not be comprehensive or easy to get up and running, but they can pay dividends down the road—particularly if you have customers who are demanding higher levels of transparency.

For organizations that consume software but do not necessarily produce it, there can also be benefits in planning around an SBOM. For some of the larger vendors that usually have SBOMs available, it can be helpful to actually try to consume them and extract information from them. Why? Two reasons: First, the information in them can be valuable, and building out the ability to consume them is time well spent. Second, laying the groundwork means that as more and more vendors start to provide them, you can bring them into the fold and build out a searchable database to inform everything from incident response to compliance to architecture and beyond.

LOOKING FOR MORE?

- Explore the *IT Business Continuity/Disaster Recovery Audit Program. www.isaca.org/business-continuity-disaster-audit-program*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Effective Governance and Board Oversight in a Globalized Information Environment

Disponible également en françaiss
www.isaca.org/currentissue

Governance of technology and cybersecurity is increasingly becoming a top strategic priority because of enterprise, client and vendor dependence on Internet-facing technologies that introduce third- and fourth-party risk. Most modern enterprises have Internet-facing systems and interact with consumers, vendors and partners using some Web interface. Many enterprises use cloud services in one form or another, which means some of their data are transported and stored in the cloud on servers scattered around the world, constituting part of a globalized information environment. The use of cloud vendors only exacerbates cybersecurity risk exposure.

ALLEN ARI DZIWA | CISA, CRISC, CCSP, CEH, CISSP

Serves as a risk specialist and subject matter expert (SME) for the US Federal Reserve Bank of Cleveland. He has worked in technology and cybersecurity consulting for 15 years. He previously served on the Information Systems Security Association (ISSA) North Texas (USA) Chapter E-Council's Ethical Hacking Advisory Board and as an SME for the International Information System Security Certification Consortium (ISC)[2]. He is a certified ethical hacker and threat intelligence analyst. This article does not represent the views of his current or previous employers.

Successful enterprises are run by executives who effectively balance taking advantage of opportunities with managing the risk that follows execution of their chosen strategies. The board of directors (BoD) oversees management to ensure that managers implement approved strategies within the established risk appetite. The board has the role of holding senior management accountable and ensuring that management is providing the needed information to help the BoD make optimal, risk-informed decisions. When it comes to technology and cybersecurity, the board is involved in approving budgets, supporting independent risk management and internal audit. The board must also ensure that its members are capable of providing adequate oversight by reviewing strategy, determining risk appetite and overseeing other important enterprise responsibilities.

The globalized information environment is characterized by evolving technologies and fast-paced innovation. Therefore, to preserve confidentiality, integrity and availability of data used in revenue-generating operations, board members must understand how technology advancements affect enterprise data and information security and how the risk taken by management affects information assets:

> *As the board of directors is the key element of corporate governance, it is clear that its composition must be responsive to the basic functions that are assigned to it: supervising and monitoring, avoiding opportunistic behavior on the part of executives, and providing advice to decision makers to improve the management of the business.*[1]

The board must be comprised of people whose fundamental skills include strategic planning, corporate finance, risk management and a clear understanding of legal and regulatory compliance. Most enterprises have BoDs with specifically assigned teams to oversee technology and cybersecurity risk. The most common are the audit, risk and technology committees.

One group of researchers highlighted the perceptions of directors and senior managers regarding the

role of a board in overseeing risk and compliance, strategy, governance, development of senior management and relationships with stakeholders. They found that directors and managers believed that different combinations of these roles determined effectiveness.[2] Because of the complexity of technology and cybersecurity, a superficial understanding of technical concepts is no longer sufficient. A deeper understanding of these issues is necessary so that the board can provide adequate oversight and ensure that proper steps are being taken to manage risk.

Board committees focused on technology and cybersecurity, when properly constituted, can provide effective governance and critical scrutiny, which guides management in identifying and mitigating cyberrisk.

Audit Committee

Although the audit committee is widely known for overseeing the internal audit function, external audit and financial reporting, it also oversees technology and cybersecurity audits. Ideally, some members of the audit committee should have a financial background, and at least one member should be a certified public accountant (CPA). With the ever-increasing complexity of cybersecurity issues, it is imperative to have technically savvy board members with strong backgrounds in computer science or IT. Having at least one member who holds the Certified Information Systems Auditor® (CISA®) credential is ideal. Members who are technically savvy in their areas, such as financial or technical audit, are empowered to challenge assumptions and methodologies used by management.

A technically savvy audit team can easily identify problems such as those that led to the Enron scandal in which:

> *The Enron Board of Directors failed to safeguard Enron shareholders and contributed to the collapse of the seventh largest public company in the United States, by allowing Enron to engage in high risk accounting, inappropriate conflict of interest transactions, extensive undisclosed off-the-books activities, and excessive executive compensation.*[3]

If the board audit committee members are able to read and understand audit reports, they can hold senior management—especially the third line of defense—accountable. While a technical auditor may lead the audit committee in reviewing technical audits, that board member could also be someone who understands business, legal and compliance issues. Technical issues do not occur in isolation—rather, they occur in a business context, which includes business benefits and regulatory compliance.

A deeper understanding of these issues is necessary so that the board can provide adequate oversight and ensure that proper steps are being taken to manage risk.

It has traditionally been the practice to appoint board members who are former or current executives without considering their expertise in technical areas. This must change.

Risk Committee

Board members need to demonstrate a clear understanding of how technology and cybersecurity risk affects operations. The risk committee is responsible for risk management policies and oversight. It must be able to understand and challenge risk updates that are provided by the second line of defense (i.e., managers). The chief risk officer (CRO) must be able to directly access the board risk committee to report activities that pose serious risk to the enterprise without interference from the chief executive officer (CEO). The independence of the CRO is important for the enterprise to effectively identify, monitor and mitigate risk. The risk committee assures this independence.

Members of the risk committee must be equipped with project management skills, change management experience, a reasonable understanding of legal and compliance risk, and knowledge of contingency planning and cybersecurity. They must avoid conflicts of interest and maintain and update written charters, and report to the full board as frequently as quarterly to discuss issues related to their areas of focus. In addition to having technical skills, risk committee members must be able to understand financial statements and processes. The risk committee must be committed to upholding the independence of the enterprise's risk management function.

LOOKING FOR MORE?

- Read *How to Drive Growth, Strategy and Governance Through Design*. *www.isaca.org/growth-through-design*
- Learn more about, discuss and collaborate on governance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

The board of the future must balance value-creation activities and manage risk within the established risk appetite.

In terms of legal and regulatory compliance, risk committee board members may monitor and track compliance by reviewing management reports with appropriate metrics. Board members who have only peripheral knowledge of regulatory requirements may approve and rubber-stamp reports without holding management accountable if metrics indicate the organization is falling out of compliance.

Technology Committee

A technology committee reviews, approves and oversees major technology acquisitions and deployments. Members of such a committee are expected to understand financial statements and be able to review and approve technology budgets. Whenever new acquisitions are planned, the technology committee must be able to discuss the risk associated with the new technology with the risk committee. The committee members must have a clear understanding of project management, change management and the pros and cons of acquiring new technologies. They must hold the senior management who are responsible for the first line of defense accountable.

Conclusion

Rapid changes in technology and anticipated advancements in artificial intelligence (AI), machine learning (ML) and quantum computing are creating disruption in the cybersecurity space. Therefore, enterprises need to have forward-looking board members who are ready to make adjustments and flow with the changes in the global information environment. Board members must have skills in disciplines such as finance, technology and people management to help them see issues beyond their immediate committee responsibilities so they can effectively challenge assumptions made by senior management before they make decisions that affect technology and cybersecurity risk for the enterprise.

The board of the future must balance value-creation activities and manage risk within the established risk appetite. Gone are the days when board members did not know how to use a computer, but made major decisions on technology and cybersecurity risk. The future board should consist of technical experts who can connect technology and cybersecurity issues to business functions including regulatory compliance. Board members serving on the audit, risk and technology committees must be comfortable interpreting key performance indicators (KPIs) and key risk indicators (KRIs) and must demonstrate confidence that the enterprises they govern are in a position to implement necessary and appropriate controls, develop metrics, and report on technology and cybersecurity risk.

The future board must have shrewd members who can easily discuss thorny issues and clarify expectations for their organization's enterprise and cybersecurity culture. They must be capable of self-evaluation and accept responsibility if the strategy and culture they establish from the top fails. If their contribution fails to prevent major cybersecurity attacks that result in enterprise reputational and legal issues, they must be willing to relinquish the privilege of being on the board. Board members must not simply rubber-stamp what management proposes, but rather use critical skills and expertise to scrutinize and challenge assumptions made by management and hold decision makers accountable for all risk-taking activities. The future board is highly analytical, technical, savvy and diverse.

Endnotes

1 Martin, C. J. G.; B. Herrero; "Boards of Directors: Composition and Effects on the Performance of the Firm," *Economic Research-Ekonomska Istraživanja*, vol. 31, iss. 1, 1 May 2018, *https://www.tandfonline.com/doi/full/10.1080/1331677X.2018.1436454*

2 Nicholson, G.; C. Newton; "The Role of the Board of Directors: Perceptions of Managerial Elites," *Journal of Management and Organization*, vol. 16, iss. 2, May 2010, *https://www.cambridge.org/core/journals/journal-of-management-and-organization/article/abs/role-of-the-board-of-directors-perceptions-of-managerial-elites/96D707EB8F784ABC95EB39F5A08C0B2C#*

3 US Senate Committee on Governmental Affairs, *The Role of the Board of Directors in Enron's Collapse,* USA, July 2002, *https://www.govinfo.gov/content/pkg/CPRT-107SPRT80393/html/CPRT-107SPRT80393.htm*

Internal Audit as a Driver of Innovation

Disponible également en françaiss
www.isaca.org/currentissue

On 9 October 1903, an article published in *The New York Times* titled "Flying Machines Which Do Not Fly" estimated that the development of flying machines would take between one million and 10 million years. However, a few weeks later, on 17 December 1903, the first manned flight was successfully achieved by the Wright brothers.[1] But after that, it took commercial airlines 68 years to reach 50 million users. In comparison, it took the popular mobile game *Pokémon Go* only 19 days to reach the same number of users.[2] The growth of *Pokémon Go* is an example of the era referred to as "Turbulent Times."[3]

The Fourth Industrial Revolution (4IR), which began in 2000, is marked by the rapid, exponential pace of change driven by four major digital forces: social, mobile, analytics and cloud (SMAC). These forces, when combined, create the foundation for high-velocity disruptive innovation and the digital transformation of products and services.[4, 5, 6]

However, despite the chaotic and nonlinear nature of the turbulence that depicts this era, its causes are still manageable using internal audit.[7] The internal audit function is instrumental in promoting innovation and cultivating a culture of continuous improvement in organizations. However, to remain relevant and fulfill this role, the internal audit function needs to adjust its activities and value propositions to align with the demands of the 4IR era.

The Intelligent Organization, Digital Business Agility and Flux Mindset

To keep pace with a rapidly changing, turbulent business landscape, organizations strive to develop organizational intelligence. Organizational intelligence encompasses an organization's ability to adapt, transform and proactively influence its environment.[8] To achieve this, intelligent organizations are client-focused, effectively communicate and collaborate, engage in knowledge management, and practice digital business agility.[9, 10, 11]

Digital business agility encompasses three key competencies:

1. **Hyperawareness**—Allows an organization to stay alert to the flux of changes in its internal and external business environments.
2. **Informed decision-making**—Supports data- and knowledge-driven decision-making in a fully automated or semiautomated structured process.
3. **Fast execution**—Ensures that decisions are promptly and efficiently implemented.[12, 13]

> The internal audit function is instrumental in promoting innovation and cultivating a culture of continuous improvement in organizations.

Adopting these practices supports a shift from a fixed to a flux mindset. A flux mindset is rooted in change and embraces change as an ongoing aspect of the business. Organizations that adopt flux mindsets are comfortable with change, highly responsive to

NOAM KORIAT | PH.D., CISA

Is the director of information systems audit at Discount Bank. Previously, he was global chief information officer of the Israeli Ministry of Tourism. Koriat also serves as an adjunct professor at the Graduate School of Business Administration at Bar Ilan University (Ramat Gan, Israel), where he teaches digital transformation and innovation, knowledge management, and information systems practicum courses. Koriat can be contacted on LinkedIn at *https://www.linkedin.com/in/noamkor/.*

changes, and have the ideal environments and digital cultures for engaging in digital transformation and innovation efforts.[14]

Digital Transformation, Digital Culture and Innovation

Digital transformation is a strategy for enterprises to implement change in their business models and ecosystems by utilizing digital competencies while simultaneously cultivating a digital culture within the organization. This shift toward a digital culture is critical to the success of digital transformation as it supports the values and behaviors necessary to drive innovation, agility and responsiveness in a rapidly evolving digital landscape.[15, 16] Digital transformation is about rewriting the organization's business story in the new language of digital natives—that is, the Y, Z and Alpha generations.

There are four core values of digital culture:

1. **Impact**—Underscores the need for radical change through innovation
2. **Speed**—Emphasizes the importance of moving quickly and iterating rather than waiting for a complete understanding of the situation before taking action
3. **Openness**—Highlights the importance of hyperawareness and transparency in both internal and external contexts, and open sharing of information and data
4. **Autonomy**—Emphasizes the importance of decentralization and delegation of authority, which allow for discretion and fluent, prompt execution[17]

Innovation is conceptualized as a process that incorporates the ideation, adoption and execution of new ideas, processes, products and services.[18] Scholars have also defined it as a process that starts with the inception of a new idea and then matches a challenge with a solution through its realization to its impact.[19]

Innovation encompasses two main aspects: innovation speed and innovation quality. Innovation speed refers to the time span to conduct the innovation process from inception to impact. Like the fast execution competency associated with digital business agility, innovation speed is essential to assure the timely implementation of creative ideas for a competitive advantage.[20, 21, 22, 23] Innovation speed is the ability to identify, decide on and execute changes quickly enough to cope with a high-paced, exponentially changing business environment.

Innovation quality encompasses various factors that define the value of services or products, such as functionality, effectiveness, reliability, costs and complexity.[24] This aspect of innovation can be seen as a dimension of a client-centric intelligent organization that strives to provide its customers with the right and relevant value through its products and services.

> Its distinct overall organizational access and perspective, combined with its independence, objectivity and impartiality, allows the audit function to serve as an accurate sensor for gaps in knowledge and competencies.

Innovation extends beyond generating creative, novel and useful ideas. It encompasses their successful execution, which leads to impact. Creative ideas alone are not enough; it is through their implementation that their value is realized.[25, 26] Therefore, effective innovation leadership does not necessarily require individuals with creative competencies, but rather individuals with the ability to get things done.[27]

The Role of Internal Audit in Driving Innovation

The International Professional Practices Framework (IPPF) 2017 defines internal auditing as a systematic process aimed at improving an organization's value through assurance, advisory and insightful activities, while considering the future impact.[28] The audit function is further defined to be independent, objective, unbiased and devoid of any conflicting interest. The internal auditor must remain impartial and maintain objectivity during the provision of consulting services and must not assume management duties.[29]

The internal audit function is well-suited to serve as a key player in promoting and enhancing organizational innovation and providing the necessary means to cope with a fast-paced, changing business environment.

Its distinct overall organizational access and perspective, combined with its independence, objectivity and impartiality, allows the audit function to serve as an accurate sensor for gaps in knowledge and competencies. In addition, it can perform a change audit to determine areas of new business that are yet to be explored.[30]

Socrates famously stated, "All I know is that I know nothing."[31] The role of internal audit is paramount in assisting organizations to understand their areas of ignorance. Internal audit serves as a medium for the expression of unheard internal and external opinions and ideas. This enables internal auditors to facilitate and foster collaborative behaviors such as communication, and balance member contributions to enhance teamwork and knowledge sharing. That, in turn, promotes creativity and innovation.[32, 33]

Moreover, the internal audit function can monitor and motivate informed decision-making, enabling organizations to make sound decisions that are efficient and effective. In situations in which organizational shortcomings hinder innovation, internal auditors can serve as mediators and facilitators to remove bottlenecks, promote decentralization and delegation of authority, get things done, and improve innovation speed. In addition, the internal auditor is well-positioned to examine the quality and method of execution, consider the voice of the customer and gauge the impact on the customer experience.

To effectively fulfill this role, the internal audit function must transition from its traditional focus on retrospective analysis and control examination to a more consultative, predictive and forward-looking approach.

Furthermore, the internal auditor can offer unbiased, forward-looking insights without being constrained by first-line factors such as biases due to prior investments, knowledge limitations or operational incapacity. This enables internal auditors to shed light on complex challenges that arise from the implementation of cutting-edge technologies or the digital transformation of processes and products.

Practical Implications

To transform internal audit, there are several practical approaches.

This transformation necessitates a change in auditing skills and competencies, encompassing the mastery of audit proficiency with a greater emphasis on professional knowledge, hands-on experience and real-time auditing skills.

In addition, the internal audit function should adopt an Agile approach, allowing for greater flexibility and responsiveness. It is recommended that the Agile approach be integrated into the audit work plan process to enable internal auditors to remain alert to changes and to prioritize critical and high-risk issues. In addition, incorporating the Agile approach into audit project management promotes audit programs that are more focused and effective, while increasing efficiency and facilitating rapid execution.[34, 35, 36, 37, 38]

Moreover, internal auditors can adopt content validity approaches, such as an expert panel inter-rater agreement for reconciliation, to overcome hindrances to innovation caused by professional disagreements among decision makers within the organization.[39]

Conclusion

Internal audit has an important role in promoting and fostering organizational innovation and a flux mindset. To effectively fulfill this role, the internal audit

LOOKING FOR MORE?

- Read *Destination: Agile Auditing. www.isaca.org/agile-auditing*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

function must transition from its traditional focus on retrospective analysis and control examination to a more consultative, predictive and forward-looking approach, facilitated by professional and academic research, benchmarking, advanced data analytics and business process analysis methodology.[40]

The internal audit function must align with the new demands of the 4IR era and transform its activities and value propositions accordingly. By adopting an intelligent approach and digital business agility, the internal audit can retain its significance and relevance and act as a driver for innovation.

Endnotes

1 National Air and Space Museum, "1903 Wright Flyer," USA, *https://airandspace.si.edu/collection-objects/1903-wright-flyer/nasm_A19610048000*

2 Desjardins, J.; "How Long Does It Take to Hit 50 Million Users?" Visual Capitalist, 8 June 2018, *https://www.visualcapitalist.com/how-long-does-it-take-to-hit-50-million-users/*

3 Drucker, P.; *Managing in Turbulent Times*, Harper and Rowe, USA, 1980

4 Schwab, K.; *The Fourth Industrial Revolution*, Currency Press, Australia, 2017

5 Schwertner, K.; "Digital Transformation of Business," *Trakia Journal of Sciences,* vol. 15, iss. 1, Bulgaria, 2017, *https://www.studocu.com/en-gb/document/university-of-greenwich/human-resource-management/digital-transformation-of-business/48207449*

6 Xu, M., J. David *et al.*; "The Fourth Industrial Revolution: Opportunities and Challenges," *International Journal of Financial Research*, vol. 9, iss. 2, April 2018, *https://ideas.repec.org/a/jfr/ijfr11/v9y2018i2p90-95.html*

7 *Op cit* Drucker

8 Schwaninger, M.; "Managing Complexity—The Path Toward Intelligent Organizations," *Systemic Practice and Action Research*, vol. 13, 1 April 2000, *https://www.alexandria.unisg.ch/publications/8623*

9 Pinchot, G.; E. Pinchot; *The End of Bureaucracy and the Rise of the Intelligent Organization*, Berrett-Koehler Publishers, Inc., USA, 1994

10 Wade, M.; A. Tarling; "The Digital Business Agility Imperative: How Companies Can Fight Digital Disruption," *International Institute for Management Development*, Switzerland, 2016

11 Wade, M.; A. Noronha *et al.*; "Orchestrating Digital Business Transformation: Working in Concert to Achieve Digital Excellence," Global Center for Digital Business Transformation, Switzerland, 2017

12 *Op cit* Wade, 2016

13 *Op cit* Wade, 2017

14 Rinne, A.; "A Futurist's Guide to Preparing Your Company for Constant Change," *Harvard Business Review*, 22 September 2021, *https://hbr.org/2021/09/a-futurists-guide-to-preparing-your-company-for-constant-change*

15 Whalen, M.; *A Digital Transformation Maturity Model and Your Digital Roadmap*, IDC, 2014 *http://www.agendaconference.com/wp-content/uploads/2014/12/Whalen_IDC.pdf*

16 Westerman, G.; D. Soule; A. Eswaran; "Building Digital-Ready Culture in Traditional Organizations," *MIT Sloan Management Review*, vol. 60, iss. 4, 21 May 2019, *https://sloanreview.mit.edu/article/building-digital-ready-culture-in-traditional-organizations/*

17 *Ibid*.

18 Thompson, V.; "Bureaucracy and Innovation," *Administrative Science Quarterly*, 1965, *https://doi.org/10.2307/2391646*

19 Budden, P.; F. Murray; *An MIT Framework for Innovation Ecosystem Policy: Developing Policies to Support Vibrant Innovation Ecosystems (iEcosystems)*, MIT Lab for Innovation Science and Policy, USA, October 2018, *https://innovation.mit.edu/assets/Framework-Ecosystem-Policy_Oct18.pdf*

20 Kessler, E.; A. Chakrabarti; "Innovation Speed: A Conceptual Model of Context, Antecedents, and Outcomes," *The Academy of Management Review*, vol. 21, iss. 4, October 1996, *https://www.jstor.org/stable/259167?origin=crossref*

21 Kessler, E.; P. Bierly; "Is Faster Really Better? An Empirical Test of the Implications of Innovation Speed," *IEEE Transactions on Engineering Management*, vol. 49, iss. 1, February 2002, *https://ieeexplore.ieee.org/document/985742*

22 Allocca, M.; E. Kessler; "Innovation Speed in Small and Medium-Sized Enterprises," *Creativity and Innovation Management*, vol. 15, iss. 3, January 2003, *https://www.researchgate.net/publication/35230802_Innovation_Speed_in_Small_and_Medium-Sized_Enterprises*

23 Carbonell, P.; A. Rodriguez; "The Impact of Market Characteristics and Innovation Speed on Perceptions of Positional Advantage and New

Product Performance," *International Journal of Research in Marketing,* vol. 23, iss. 1, March 2006, *https://www.sciencedirect.com/science/article/abs/pii/S0167811606000024*

24 Haner, U.; "Innovation Quality—A Conceptual Framework," *International Journal of Production Economics*, vol. 80, iss. 1, November 2002, *https://doi.org/10.1016/S0925-5273(02)00240-2*

25 Levitt, T.; "Creativity Is Not Enough," *Harvard Business Review*, vol. 80, iss. 8, August 2002, *https://hbr.org/2002/08/creativity-is-not-enough*

26 Erez, M.; R. Nouri; "Creativity: The Influence of Cultural, Social, and Work Contexts, *Management and Organization Review,* vol. 6, iss. 3, November 2010, *https://doi.org/10.1111/j.1740-8784.2010.00191.x*

27 *Op cit* Levitt

28 Institute of Internal Auditors, *The International Professional Practices Framework (IPPF)*, USA, 2017, *https://www.theiia.org/en/standards/international-professional-practices-framework/*

29 *Ibid*.

30 *Op cit* Rinne

31 Plato, *The Apology of Socrates*, 399 BC

32 Hoegl, M.; H. Gemuenden; "Teamwork Quality and the Success of Innovative Projects: A Theoretical Concept and Empirical Evidence," *Organization Science*, vol. 12, iss. 4, August 2001, *https://pubsonline.informs.org/doi/10.1287/orsc.12.4.435.10635*

33 Koriat, N.; R. Gelbard; "Knowledge Sharing Motivation Among IT Personnel: Integrated Model and Implications of Employment Contracts," *International Journal of Information Management*, vol. 34, iss. 5, October 2014, *https://www.sciencedirect.com/science/article/abs/pii/S0268401214000474?via%3Dihub*

34 Serrador, P.; J. Pinto; "Does Agile Work?—A Quantitative Analysis of Agile Project Success," *International Journal of Project Management,* vol. 33, iss. 5, July 2015, *https://www.sciencedirect.com/science/article/abs/pii/S0263786315000071*

35 Kisielnicki, J.; A. Misiak; "Effectiveness of Agile Compared to Waterfall Implementation Methods in IT Projects: Analysis Based on Business Intelligence Projects," *Foundations of Management*, vol. 9, iss. 1, 27 October 2017, *https://doi.org/10.1515/fman-2017-0021*

36 Ambler, S.; "2018 IT Project Success Rates Survey Results," Disciplined Agile Consortium, 2018, *http://ambysoft.com/downloads/surveys/Success2018.pptx*

37 Khoza, L.; C. Marnewick; "Waterfall and Agile Information System Project Success Rates—A South African Perspective," *South African Computer Journal*, vol. 32, iss. 1, July 2020, *https://www.researchgate.net/publication/343138568_Waterfall_and_Agile_information_system_project_success_rates_-_A_South_African_perspective*

38 Koriat, N; "Agile Audit—Buzzword or Future?" *The Internal Auditor Journal*, 16 September 2022, *https://mba.biu.ac.il/en/node/971*

39 Rubio, D.; M. Berg-Weger *et al*.; "Objectifying Content Validity: Conducting a Content Validity Study in Social Work Research," *Social Work Research*, vol. 27, iss. 2, June 2003, *https://academic.oup.com/swr/article-abstract/27/2/94/1659075*

40 Deloitte, *Internal Audit 3.0: The Future of Internal Audit Is Now,* United Kingdom, 2018, *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-internal-audit-3.0-the-future-of-internal-audit-is-now.pdf*

Solving Standards Implementation Issues With a Global ISMS

Disponible également en françaiss
www.isaca.org/currentissue

There is an abundance of information security standards or frameworks available to help enterprises secure their data and operations. Implementing these standards involves reading not only the requirements of the standards themselves, but also the accompanying implementation guides and myriad online documents regarding the challenges to be overcome. This becomes more difficult if an enterprise is required to be aligned with more than one standard due to its global footprint. The solution is a global information security management system (ISMS) that fulfills a combination of requirements from multiple standards.

ISMS

The ISMS was introduced by International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001, which states that:

> *[T]he establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used and the size and structure of the organization.*[1]

This means that, for a global enterprise, the ISMS must cover all internal and external requirements at the global and the local country level, while ensuring that it also covers critical operations and follows the enterprise's governance structure.

Aligning a global enterprise's ISMS with several standards and certifying compliance with those standards have become necessary because enterprises have interested parties worldwide, each of which may recognize different security frameworks. Each country's legal and regulatory requirements may also mandate an enterprise's alignment with a combination of standards, making local hurdles unavoidable.

When an enterprise makes the effort to achieve alignment with globally accepted standards and can prove it, it increases the trust of third parties and may lead to more business. As Webhelp's Group Chief Information Security Officer (GCISO) Ivan Milenkovic notes, "Implementing an ISMS provides multiple benefits: It is an 'invitation to the party' with clients, represents the basis for the common language and showcases the willingness to constantly improve company culture. On one side—clients understand what they get; on the other—we break the vicious circle of questionnaires and audits."

SARANTOS KEFALAS | CISA, CISM, CCSP, CISSP, ISO 27001 LI

Is the group infosec risk and compliance director at Webhelp and is responsible for maintaining its global information security management system (ISMS). Previously, he held auditing and consulting roles at PricewaterhouseCoopers (PwC) in Greece and the United Kingdom, working on information security and cybersecurity primarily in the financial services sector, shipping and telecommunications. He has more than 10 years of experience in information security, including training and coaching younger professionals and students. Kefalas is a member of ISACA® and other professional organizations.

Implementing a Global ISMS

Once an enterprise's global ISMS requirements have been identified, standards have been selected, a team of experts has been engaged and the enterprise's leadership is on board, implementation can begin.

In most, if not all, cases, there is more than one way to implement a measure (i.e., control) to achieve a security objective. And standard requirements always have an ultimate security objective to be achieved, no matter how prescriptive they are. Therefore, it is a good idea to develop a baseline of measures that are tailored to the enterprise and can cover objectives from multiple standards. If that baseline is accompanied by a means of mapping to each standard, along with the rationale behind why and how the baseline measures fulfill the standard requirements, this ensures that nothing has been missed.

Certifying a Global ISMS

Once the baseline for the global ISMS has been implemented, the next step is certification. The ISMS can typically be certified for only one standard at a time and, in most cases, one country at a time. Although the ISMS meets a number of requirements, it must be shown that it conforms to each specific standard. This requires information security experts with a working knowledge of the relevant standards who can initiate a program with a road map that includes:

- Enterprise strategy
- Client requirements
- Information security objectives
- Country specifics
- Other internal compliance requirements

These requirements must be balanced and met within specified deadlines. Unexpected changes may also occur during the journey to certification, including:

- New requirements from prospective or existing clients
- Scope expansion due to the enterprise's growth in new countries or new sites in existing countries
- Acquisition of an enterprise to be included in the certification scope
- New regulations in one or more countries
- Unplanned unavailability of resources
- New versions of a standard

> Auditors should be used as enablers, and their advice should be taken as if they were consultants.

It may seem like an impossible undertaking, but it is not.

Certification in a new country where the enterprise operates is much easier (assuming that local information security resources exist) if it has a blueprint outlining the steps necessary to achieve certification for each standard using the previously developed baseline. To ensure efficiency, the blueprint should include:

- Steps toward certification expressed in plain language, including what steps to take to implement the baseline
- Estimated effort required for the implementation of each step
- Anticipated owner
- Useful internal resources, such as globally developed policies, standards, procedures, frameworks or templates that allow standardization across different countries

At this point, the enterprise should have a baseline that covers all relevant standards and a blueprint for achieving certification for each of those standards.

Choosing a Certification Body and Certification Auditors

A global enterprise should select a global certification body that can support all countries in which certification is desired. The lead auditor assigned to an enterprise's account should examine the baseline and blueprint for the relevant certification to confirm acceptance of the chosen approach, even before the audit starts.

Certification auditors play an incredibly important role. Experience has shown that every auditor is different. Although all local representatives of the certification body follow the same standard requirements and guidelines, they may focus on different areas based on their experiences. It is likely

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

For most enterprises, maintenance of the certified ISMS and the relevant baseline is more difficult than developing them in the first place.

that certain issues identified in one country because of an auditor's particular focus also exist in other countries, though they may not have been mentioned. This is extremely helpful for improving an enterprise's global security posture and obtaining the necessary sponsorship for change. Auditors should be used as enablers, and their advice should be taken as if they were consultants. Openness and honesty on both sides can be the key to successful certification.

Finally, be aware of any potential language barriers with local auditors. Determine beforehand whether the assigned auditor is fluent in the enterprise's formal language and which language the audit will use for every country to ensure that it runs smoothly.

Does Certification Mean Security?

Obtaining certification of a global ISMS means a lot of things, but it does not mean that the enterprise cannot be breached. It means that certain operations of the enterprise follow a consistent, standardized approach, enabling more effective and more mature preventive and detective information security measures. This, in turn, means that information security risk factors and incidents can be identified faster and handled according to global guidelines that conform to good practices. However, there is always room for improvement and this is evident by the certification audit findings.

Does certification make the enterprise more secure? Indirectly, yes. But one would have to drill into the details of a certification audit report to understand which preventive and detective measures are enabling a better security posture.

Maintaining a Global ISMS

Certifying an ISMS is not a one-time exercise. For most enterprises, maintenance of the certified ISMS and the relevant baseline is more difficult than developing them in the first place. Continuous effort is required to ensure that:

- Standard requirements are constantly met.
- Information security threats are managed.
- Information security processes are embedded, and potential exceptions are documented, monitored and periodically attested.
- Performance of the ISMS is evaluated and reported.
- All employees (internal, external) are trained.
- Documentation is reviewed and updated.
- Security posture is improved.

Conclusion

Complying with internal and external information security requirements for a global enterprise is hard work. For an information security system to operate at its best, it takes time and requires human and technology resources. To make compliance efficient and effective, all those requirements must be combined, baselines established and one global ISMS developed. The introduction of blueprints can be a huge help to ensure certification of the ISMS against globally accepted standards and frameworks, so that the enterprise shows interested parties that it takes information security seriously and conforms with their multifaceted requirements.

Endnotes

1 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001:2013 *Information Technology–Security techniques–Information Security Management Systems–Requirements, 2nd Edition*, Switzerland, 2013, *https://www.iso.org/obp/ui/iso:std:iso-icc:27001:ed-2:v1:en*

Designing Ethical Systems By Auditing Ethics

Disponible également en françaiss
www.isaca.org/currentissue

Ensuring that any emerging technology that is implemented within an organization honors inalienable human rights is nonnegotiable. The question remains, how can ethics be audited when they involve so many perspectives that can be influenced by different cultural viewpoints? Ethics are generally defined as sets of beliefs about what are considered acceptable and unacceptable behaviors within a society.[1] But the opinions of individuals from one region in the world may be vastly different from those of another region. Furthermore, asking organizations to perform audits of their technology implementations through an ethical lens seems to be contrary to what drives an organization's bottom line and stakeholder value—especially when organizations are asked to document the results. When organizations fail to embed ethics as a foundational requirement within their development processes and are found to be violating foundational ethical beliefs engrained within society, they can face reputational or financial impact, potential litigation or regulatory consequences.[2] This can lead to a direct impact on customer and employee trust in the organization and may offset any potential benefits received by circumventing processes. It is critical that organizations understand and embed ethics when developing and implementing emerging technologies, thereby validating their responsible technology processes throughout the life cycle. Furthermore, they must audit the implemented processes to ensure that ethical values are embedded throughout.

The Ethical Dilemma

Although there is generally a consensus on what norms are accepted in society, there is not one specific ethical perspective that serves as the standard for how organizations should act or define their ethical or responsible technology programs. These foundational perspectives inform and determine the ethical lens used when developing technologies. Opinions about what is ethical can shift significantly between communities within society.[3] Ethics can also evolve, making it critical that a new process be established to address evolving perspectives.

It has been noted that "Culture has a significant impact when determining the foundational values to be leveraged when technology systems are deployed."[4] In addition, business drivers impact

JOSH P. SCARPINO | D.SC., CISM

Is the vice president of information security at TrustEngine, where he leads IT operations, security and compliance programs. He is also responsible for developing and managing the organization's responsible technology program. Scarpino has more than 18 years of IT and security experience in the US Department of Defense (DoD). He has led security operations for Fortune 500 companies, enhanced critical controls at financial and manufacturing organizations, and led, scaled and audited security and compliance programs. He has spent his career bridging areas across technology and security to include operations, governance, risk and compliance (GRC), and responsible technology. Scarpino also has a passion for educating the next generation of professionals. Currently, he is partnering with ForHumanity to develop frameworks for auditing artificial intelligence (AI) systems and is continuing his research of ethical AI independently and in partnership with the University of Pittsburg CAIR Lab (Pennsylvania, USA).

When it comes to emerging technology, there is no clear alignment or standard approach to embedding ethics.

ethical decisions and require organizations to make tradeoffs between accuracy, fairness and ethics as perceived by society.[5] Unless an organization is firmly grounded in its ethics program, ethics only becomes a priority when organizations are at risk of becoming a case study or facing regulatory impacts.[6] Organizations must do better to ensure that technology honors inalienable human rights and does not cause an unnecessary disparate impact on members within society.

The Institute of Electrical and Electronics Engineers (IEEE) Global Initiative on Ethics of Autonomous and Intelligent Systems states:

> *Whether our ethical practices are Western (Aristotelian, Kantian), Eastern (Shinto, Confucian), African (Ubuntu), or from a different tradition, by creating autonomous and intelligent systems that explicitly honor inalienable human rights and the beneficial values of their users, we can prioritize the increase of human well-being as our metric for progress in the algorithmic age.*[7]

Varied Approaches to Addressing Ethical Concerns

When it comes to emerging technology, there is no clear alignment or standard approach to embedding ethics. Organizations are focused on delivering products to market and may deprioritize conversations that could delay time to value. Instead, organizations must align with social and moral norms to guide their approach to ethical technology development.[8] However, there are several approaches to managing ethics for emerging technologies. One option is to ignore ethics to avoid stifling innovation, with the ultimate goal that the outcomes outweigh any negative consequences. Another approach is to address ethical concerns as they are realized. The last approach is to attempt to predict ethical challenges and understand how they can impact emerging technology.

One author's proposed approach aimed at predicting ethical challenges is anticipatory technology ethics.[9] This approach considers three levels of ethical analysis: the technology, artifact and application. At the technology level, the ethical review focuses on the pieces of the technology and considers the ethical issues associated with the components. At the artifact level, the ethical analysis focuses on the components that result or could result from a specific technology presenting a moral issue. At that level, results are unavoidable by nature, due to potential applications or simply due to the inherent risk of the artifact or the need for ethical justification. At the application level, the focus is placed on how the artifacts are used, the procedure, or its potential configuration. Although the process of defining a shared view of ethics and how it applies to emerging technologies is difficult, it is necessary to find a path forward and embed ethics into all development processes.[10] One way to ensure that ethical values are continuously evolved and embedded is by ensuring that developed processes align with an organization's code of conduct and ethics.

Auditing the Process, Not the Application

Ethics audits ensure an organization's behaviors align with its code of conduct and ethics.[11] A code of ethics is a set of rules dictating what is considered acceptable and unacceptable behavior within an organization. The US Securities and Exchange Commission (SEC) defines a code of conduct as being leveraged to deter wrongdoing and promote, among other things, honest and ethical conduct.[12]

An ethics audit includes analyzing the organization's mission, vision, value statements, code of ethics and supporting documentation. The interview or completion of questionnaires by board members, staff and volunteers help identify any gaps. The creation of a report and follow-up activities may include the development of an educational program and monitoring to address gaps.[13, 14]

However, auditing ethics is challenging because views can change based on the individual beliefs and the societal backgrounds of those involved in the process. In addition, organizations have different moral frameworks, which are sets of reasonable and coherent moral beliefs and principles that distinguish a group of people or a culture, or common and accepted values in society.[15] Moral

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

frameworks in organizations are the result of organizations positioning themselves within the industry and defining core values and unique employee perspectives.

Although there is societal disagreement on many common ethical challenges, organizations cannot leverage just one moral framework to audit or ensure the compliance of emerging technologies. Instead, they must look to understand the process that addresses ethics and ensure that the appropriate controls have been implemented. It is critical to ensure that ethical evaluations and checkpoints are a fundamental component of the technology development process.

As a foundational requirement and to promote transparency and trust in results, organizations should have their programs assessed by an independent auditor after adoption.

Understanding and examining the impact of emerging technologies, the cultural values of who is developing the system, and for whom the system is deployed is a core component that must be considered when ensuring ethical technology deployments.[16] Taking into consideration why the system was designed and who it will impact should be at the forefront for all organizations reviewing their deployments. In addition, as these systems are deployed, ethical reviews should be performed and inalienable human rights explicitly honored.[17] Deploying technologies that have a disparate impact on individuals or portions of society should cause organizations to pause and evaluate the true purpose and need of their technology. To appropriately evaluate the technology, organizations must maintain diverse and varied viewpoints when implementing artificial intelligence (AI) and machine learning (ML) and ensure that all potential risk factors are analyzed throughout the deployment life cycle.[18] Including stakeholders from different backgrounds who offer varied cultural perspectives as part of the designing, testing and monitoring processes is critical to ensure responsible technology. Individuals must be responsible for confirming that emerging technology deployment follows an ethical development life cycle, which includes ensuring that ethical implications are assessed before implementation and validated after deployment.[19]

Ethical Audit Considerations for Emerging Technologies

As a foundational requirement and to promote transparency and trust in results, organizations should have their programs assessed by an independent auditor after adoption. This helps remove the potential for bias and increases public confidence in the process. Some items that should be included in an ethical process audit include:

- Ensuring that ethical audits are part of an organization's standard process and following a standard audit format, starting with an analysis of artifacts within the organization. Analysis of these documents facilitates an understanding of how the organization approaches ethical decisions, the practices for managing ethics and what should be the expected outcome.
- Assessing the individuals involved in the ethical review process to determine whether they come from varied backgrounds, education levels and offer unique perspectives. Does the review team consist of individuals with varied perspectives to include different ethical lenses such as the rights lens, the justice lens, the utilitarian lens, the common good lens, the virtue lens and the care ethics lens?[20] The rights lens suggests that ethical action is the best and protects the rights of those affected. The justice lens takes the perspective that each individual should be afforded fair or equal treatment. The utilitarian lens aims to understand how this will impact everyone involved and the consequences. The common good lens aims to consider that life in community is good and actions should contribute to this, highlighting concern for all members of a community. The virtue lens aims to ensure that ethical actions align with the ideal virtues for humanity. The care ethics lens aims to understand the needs of and impact on each individual and their specific circumstances.
- Ensuring that the individuals who are part of the ethical process understand the technology deployment they are analyzing, including the

When organizations leverage audit to validate processes that can impact the rapidly expanding emerging technology field, they can ensure that risk and ethical concerns are evaluated earlier in the process.

purpose and intended outcomes, and who is impacted by the system. Understanding who will be impacted by the system can change the ethical perspective. For example, deployment of a system that targets adults has a completely different set of requirements than a system that targets minors.

- Determining if the ethical process includes documented artifacts for the ethical review, decisions and outcomes. Documentation and tracking of the ethical review processes are critical to ensuring accountability and promoting transparency in the process.
- Monitoring the outcomes of the systems analyzed to ensure that they do not deviate from the anticipated outcomes. Failure to validate and monitor for compliance with expected outcomes can result in the potential for nondetected impacts.
- Ensuring that a documented feedback loop is present so that lessons learned and external feedback are reingested into the ethical process.

Conclusion

Ensuring that technologies are designed and deployed ethically can bring value to organizations, drive profit and prioritize inalienable human rights. It is critical that organizations remember that "there are trends in the industry that need to be addressed, favoring operational goals and efficiency over ethics will no longer be acceptable."[21] Although audits can only provide a snapshot of an organization's current approach to its ethics process, they can provide the external validation for a well-defined and implemented ethics or responsible technology program. Having a firm understanding of the ethical issues present can help stakeholders reflect on the potential technology outcomes and the deviation from the expected trajectory. Organizations must understand the context of a system's use and how ethical issues could evolve so that society can trust how these systems are deployed.[22] Senior leadership is responsible for setting the tone for how ethics are addressed and handled within the organization.

Promoting transparency in ethical processes, establishing standard practices, and ensuring appropriate oversight and stakeholder involvement are critical. Auditing has always been a crucial step to ensuring that organizations adhere to their core processes and regulatory requirements. When organizations leverage audit to validate processes that can impact the rapidly expanding emerging technology field, they can ensure that risk and ethical concerns are evaluated earlier in the process. These audits can reveal how well or poorly organizations are aligned to expected standards and ensure that society has confidence in the organization's solutions and ethical approach. When organizations perform audits that review their ethical processes and impacted systems, they can provide assurance that they have embedded audit findings into how they do business. Furthermore, this validates the importance that the organization has placed on the development of responsible technology. Organizations must audit their responsible technology programs to ensure consistency and alignment with their ethical values to validate that these foundational processes exist and ensure that there is not a disparate impact on individuals or society.

Endnotes

1 Scarpino, J. P.; "An Exploratory Study: Implications of Machine Learning and Artificial Intelligence in Risk Management," Marymount University, Arlington, Virginia, USA, 2022

2 Cheatham, B.; K. Javanmardian; H. Samandari; "Confronting the Risks of Artificial Intelligence," *McKinsey Quarterly*, 26 April 2019, *https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence*

3 Chaput, R.; J. Duval; O. Boissier; M. Guillermin; S. Hassas; "A Multi-Agent Approach to Combining Reasoning and Learning for an Ethical Behavior," *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society*, July 2021, *https://doi.org/10.1145/3461702.3462515*

4 *Op cit* Scarpino

5 Lo Piano, S.; "Ethical Principles in Machine Learning and Artificial Intelligence: Cases From the Field and Possible Ways Forward," *Humanities and Social Sciences Communications*, vol. 7, iss. 1, 2020, *https://doi.org/10.1057/s41599-020-0501-9*

6 *Op cit* Scarpino

7 Shahriari, K.; M. Shahriari; "Ethically Aligned Design: A Vision for Prioritizing Human Well-Being With Autonomous and Intelligent Systems (A/IS)," *2017 IEEE Canada International Humanitarian Technology Conference (IHTC)*, Canada, 2017, p. 197–201, *https://ieeexplore.ieee.org/document/8058187*

8 Trunk, A.; H. Birkel; E. Hartmann; "On the Current State of Combining Human and Artificial Intelligence for Strategic Organizational Decision Making," *Business Research*, vol. 13, iss. 3, 2020, p. 875–919, *https://doi.org/10.1007/s40685-020-00133-x*

9 Brey, P.; "Anticipatory Technology Ethics for Emerging IT," CEPE 2011: Crossing Boundaries, University of Wisconsin Milwaukee, USA, 2011, p. 13–26.

10 Manyika, J.; J. Silberg; B. Presten; "What Do We Do About the Biases in AI?" *Harvard Business Review*, 25 October 2019, *https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai*

11 Krell, E.; "How to Conduct an Ethics Audit," HR Magazine, vol. 55, iss. 4, 2010, p. 48–51, *https://www.proquest.com/trade-journals/how-conduct-ethics-audit/docview/205070994/se-2*

12 US Securities and Exchange Commission, "Code of Business Conduct and Ethics," *https://www.sec.gov/Archives/edgar/data/1094007/000119312504044901/dex14.htm*

13 Allen, M. B.; "The Ethics Audit," *Nonprofit World*, vol. 13, 1995, p. 51, *https://www.proquest.com/magazines/ethics-audit/docview/221335917/se-2*

14 Hofmann, P. B.; "Performing an Ethics Audit," *Healthcare Executive*, vol. 10, iss. 6, 1995, p. 47, *https://www.proquest.com/trade-journals/performing-ethics-audit/docview/200314221/se-2*

15 Frederick, R.; *A Companion to Business Ethics*, Wiley-Blackwell, USA, 1999

16 *Op cit* Scarpino

17 *Ibid*.

18 *Ibid*.

19 Scarpino, J.; "Evaluating Ethical Challenges in AI and ML," *ISACA® Journal*, vol. 4, 2022, p. 27–33, *https://www.isaca.org/archives*

20 Markkula Center for Applied Ethics at Sanata Clara University, "A Framework for Ethical Decision Making," USA, 2021, *https://www.scu.edu/ethics/ethics-resources/a-framework-for-ethical-decision-making/*

21 *Op cit* Scarpino, *ISACA Journal,* 2022

22 Stahl, B. C.; J. Timmermans; C. Flick; "Ethics of Emerging Information and Communication Technologies: On the Implementation of Responsible Research and Innovation," *Science and Public Policy*, vol. 44, iss. 3, June 2017, p. 369–381, *https://doi.org/10.1093/scipol/scw069*

An Evolutionary Strategy for Leveraging Data Risk-Based Software Development for Data Integrity

Organizational decision-making is largely dependent on the availability of adequate supporting data, data elements or records. These are perhaps the most important elements that can aid enterprises in making critical decisions promptly and efficiently. For example, healthcare organizations rely on electronic health and medical records to inform important decisions. However, in many organizations, when it comes to product code and software development and design models, data elements do not appear to carry equal importance compared to functionality. But there has been a gradual rise in recognition of the importance of data risk-based systems development across industries. Data risk-based systems development involves performing data element selection, analysis, cleansing and integration to highlight the critical data points and attributes to determine how to significantly limit risk. It recognizes that less data risk is linked with the objective of systems development with least possible risk.

Routine traditional software development methodology does not serve as a one-size-fits-all approach for every industry. For example, organizations specializing in life sciences and banking have certain key data elements that play critical roles in enterprise processes and are highly scrutinized via regulations and laws. Therefore, giving equal importance to identified critical data elements as functional specifications during the design and development phases results in effective systems development and helps avoid the cost of subsequent additional development activities to address data quality and regulatory findings.

Taking into consideration findings from data element risk analysis during the software development life cycle (SDLC) adds a higher level of confidentiality, integrity and protection controls to organizational data and business-critical processes. This can be implemented by proactively incorporating the results of data element risk analysis into user requirements, functional requirements, customization of coding standards, data modeling, system architecture and database design. Organizations operating in industries such as pharmaceuticals, finance and clinical research are routinely exposed to situations in which they must invent innovative products and systems while remaining compliant with regulations. Updating the traditional software development methodology to include data risk-based development enables organizations to avoid any penalties that may be imposed due to a lack of controls and noncompliance with regulations and laws, which makes data element risk-based development a highly lucrative approach for information systems development in many industries in the public and private sectors.[1,2]

Traditional vs. Data Risk-Based Software Development

Traditionally, code or feature development in software development is either functional or performance-focused, which limits the entire system to functional and nonfunctional requirements gathered and illustrated through use cases. Functional requirements are focused on the functionality of the system, and performance requirements are focused on requirements such as load speed, maximum number of transactions, and scalability. Such a traditional approach can expose product development projects to failure as it does not consider the various classes and types of data to be included in the system. Conversely, the combination of data risk-based development and traditional

SASIDHAR DUGGINENI | CISA, CISM, ITIL FOUNDATION

Is a compliance manager at PPD, part of Thermo Fisher Scientific. Duggineni's professional background is in healthcare technology compliance, data integrity research, quality assurance, information systems auditing, information security, good practice (GxP) compliance and server administration. He has worked with specialized teams to prepare for International Organization for Standardization (ISO) standard ISO 27001 certification. He is also a lead auditor for his organization's supplier audit program and internal audit program. Duggineni participates in various operational committees within his organization related to information security, internal quality compliance and supplier compliance, and he has mentored many of his team members in information security auditing and data integrity.

It is arguable that the value of an information system almost always depends on the size and type of data that are stored, managed and used to conduct business processes.

systems development methodology not only gives adequate attention to critical data elements and classes that are managed and stored, but also aligns the data elements with the functional and performance attributes to be delivered.

It is arguable that the value of an information system almost always depends on the size and type of data that are stored, managed and used to conduct business processes. Departing from the traditional belief that effective information systems are those that fulfill functional and performance requirements, modern and evolved evidence supports the belief that such systems gain significance based on the data they process as inputs to generate meaningful outputs that can be utilized to the enterprise's benefit. Thus, a hybrid systems development model that incorporates data element risk analysis and adequate checks and balances (e.g., audit trails, security logs for critical data inputs, and forensic capabilities to ensure regulatory and legal compliance along with functional compliance) is essential. Also, by appropriately classifying and identifying the types of data elements to be captured by the system, enterprises bound by government regulations and laws can better respond to investigations, conduct forensics and manage incidents.[3,4]

The Birth of DQaaS

In response to the rising demand for inclusion of data element risk-based systems development across industries, a new form of service has emerged: Data Quality as a Service (DQaaS). DQaaS involves hiring third-party independent consultants who master the art of data profiling via exploratory data analysis and mining activities tailored to the industry compliance needs in question. The main activities involved in DQaaS include profiling, validation, cleansing and data stewardship-related services. These services can immensely help in determining an organization's position and need for development of new information systems. This is especially true for industries that need to include a data element-based development approach in their systems development methodology of choice, since the focus of this approach is to comprehensively classify and analyze the most relevant and valuable data elements in a system.[5]

Regulatory and Legislative Expectations

Meeting regulatory expectations for data integrity is crucial for many local, national and global organizations. These expectations are enforced in the form of regulations, rules and laws, such as:

- The Code of Federal Regulations (CFR) 21 enforced by the US Food and Drug Administration (FDA), which ensures data integrity in the pharmaceutical industry. CFR Part 11 went into effect in 1997 to extend data integrity regulations into the modern era with electronic records and electronic signature standards.[6]
- Guidelines on data integrity compliance introduced by the World Health Organization (WHO), the European Medical Agency, and the UK Medicines and Healthcare Products Regulatory Agency.[7,8,9]
- The US Sarbanes-Oxley Act (SOX), a US federal law that sets strict standards for safeguarding the integrity of financial data.[10]
- The US Health Insurance Portability and Accountability Act (HIPAA), which provides federal protection of patients' health data against

During the stages of requirement gathering for a product, emphasis should be placed on effective translation of data integrity requirements into formal product requirement documents for simple communication of data integrity expectations

misuse or exposure and requires technical and administrative controls to ensure compliance.[11]

Noncompliance with these laws and regulations can lead to serious consequences such as heavy fines, loss of reputation, products banned from markets, financial losses and lawsuits.[12]

Implementing Data Risk-Based Development

To help reduce data integrity risk and maintain compliance, data risk-based development can be implemented by incorporating a variety of controls during various phases of systems development. There is no one-size-fits-all approach to accomplish this goal. Beginning with coding standards, developers can be proactive and incorporate data integrity and data quality as code throughout the build processes, such as compilers and binaries, and in deployment technologies and processes involved in centralized source code management. Examples include:

- Ensuring that the code does not involve integrity violations such as modules or libraries from untrusted sources.
- Performing code reviews with targeted data integrity benchmarks.
- Developing critical system functionalities with required attributes such as audit trails, traceability and authentication.
- Enforcing the integrity of values in database columns and rows.
- Implementing logs and input data validations.
- Educating the workforce about the importance of the inclusion of data quality and integrity requirements in work processes.
- Cleansing and clearly defining all data elements that are critical for data integrity, quality and accountability, and further incorporating those specifications into coding standards to eliminate the gaps in data forensic and data audit trail system capabilities.
- Identifying appropriate data elements on a comprehensive scale to fit the functional and regulatory needs of the system, which helps significantly increase efficiency and coverage for proactively integrating those identified critical data elements into code building processes. This also enhances the compatibilities with external systems integrations for data transfers. This strategy leads to a significant decrease in reactive implementation of those specifications because of a discovered data integrity violation or regulatory noncompliance after the rollout of a specific build version of a system.

During the stages of requirement gathering for a product, emphasis should be placed on effective translation of data integrity requirements into formal product requirement documents for simple communication of data integrity expectations to product designers and developers from the people who use the product to conduct daily business operations.

Industry Case Study

Clinical trials are a good example of the value of implementing data risk-based development. The data gathered, stored and processed by information systems for clinical research organizations (CROs) play an important role in determining clinical efficacy and making critical decisions that impact patient safety. In addition, these data often are reported to regulatory agencies. However, critical requirements for data elements cannot be entirely accommodated by traditional software development methodologies wherein data classification and data elements are not given adequate attention during the application development stage. The validation of whether a clinical trial's success is directly dependent on the availability of supportive and attributable data, which is why the inclusion of data element risk-based development in any software development methodology of choice is critical. Systems developed with this hybrid methodology can readily perform data capturing, analysis and reporting, which are critical processes in applications such as clinical trials, finance operations and hospital procedures. Industries also benefit from data risk-based systems development inclusion because it allows them to retrieve information with data integrity, security, data trails and forensics built into the systems. This enables

LOOKING FOR MORE?

- Read *Defending Data Smartly. www.isaca.org/defending-data-smartly*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

organizations to investigate any malpractice, privacy breaches or integrity compromises.

Figure 1 tabulates the differences between hybrid SDLC methodology with data element risk analysis and nonhybrid traditional SDLC methodology in terms of compliance requirements that both methodologies readily support.

Figure 2 is a comparative analysis of compliance defects encountered in a typical application life cycle in the span of 10 years using hybrid SDLC methodology with data element risk analysis vs. nonhybrid traditional SDLC methodology.[13]

Data Audit

When discussing data risk-based systems development, the concept of data audit cannot be ignored. Data audit is aimed at evaluating the quality and integrity of data that are available or accessible to business processes. It involves the adoption of a variety of tools and techniques to ensure that the current data sets are not only fit for purpose, but also of high quality and integrity. Here, data quality implies the authenticity and accuracy of data sets regarding organizational aims and objectives. For example, a data audit of a clinical trial enterprise would include checking the data for accuracy, integrity and reliability relevant to patient cases and the intended patient-specific outcomes. As another example, a financial sector organization may perform data audits to check the integrity and correctness of

FIGURE 1

Compliance Compatibility

Compliance Requirement	Hybrid SDLC Methodology With Data Element Risk Analysis	Nonhybrid Traditional SDLC Methodology
Privacy	Fully supports	Partially supports
Audit trails	Fully supports	Partially supports
Data storage protections	Fully supports	Partially supports
Audit readiness	Fully supports	Does not support
Regulatory compliance	Fully supports	Partially supports
Legal compliance	Fully supports	Does not support
Digital forensics suitability	Fully supports	Partially supports
Data confidentiality	Fully supports	Partially supports

FIGURE 2

Compliance Defects in the Application Life Cycle

its financial statements and performance throughout the calendar year. In this sense, systems developed with the inclusion of data element risk in their development methodology are better suited for both regulatory and functional compliance audits because they comprise the key data elements and attributes that are directly relevant to the regulatory and functional compliance needs of the industry. In other words, these systems are ready for a divide-and-conquer approach to performing data audits, wherein they specifically identify and analyze the data elements of greater significance and compliance relevance. Such an approach also saves time and effort pertaining to data risk audits.[12]

Conclusion

The role of data in organizational decision-making is critical across all industries. Data provide goods and services and meaningful insights that enable systems owners and regulatory authority to make accurate and mission-critical decisions and confirmations. Although the traditional approach to software development tends to neglect data elements due to a higher focus on the code aspect of system development, combining the traditional software methodology of choice with data element risk-based system development puts data in a meaningful position in the systems development life cycle. Data element risk-based systems development involves performing data element selection, analysis, cleansing and integration to ensure that the system at hand fulfills its intended purpose completely. Data element risk-based systems development can help enterprises across all industries remain proactive in terms of compliance and control while also fulfilling the relevant functional and performance requirements of a system.

Endnotes

1 Kogan, A.; B. W. Mayhew; M. A. Vasarhelyi; "Audit Data Analytics Research—An Application of Design Science Methodology," *Accounting Horizons*, vol. 33, iss. 3, 2019, p.69–73

2 MD Group, "Importance of Data Capture, Analysis, and Reporting for Patient-Centric Clinical Trials," 1 October 2020, *https://mdgroup.com/blog/the-importance-of-data-capture-analysis-and-reporting-for-patient-retention-in-clinical-trials/*

3 US Department of Defense, Military Standard on Software Development and Documentation (MIL-STD-498), USA, 5 December 1994, *http://everyspec.com/MIL-STD/MIL-STD-0300-0499/MIL-STD-498_25500/*

4 Grow, "Why Is Data Important for Your Business?" *https://www.grow.com/blog/data-important-business*

5 Rajan S.; S. Narayanan; "Data Quality as a Service: Practical Guide to Implementation," Data Quality Pro, 2022, *https://www.dataqualitypro.com/blog/data-quality-as-a-service-practical-guide*

6 Code of Federal Regulations, *Part 11 - Electronic Records*; *Electronic Signatures*, USA, 20 March 1997, *https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11*

7 European Medicines Agency, "Data Integrity: Key to Public Health Protection," 8 November 2016, *https://www.ema.europa.eu/en/news/data-integrity-key-public-health-protection*

8 World Health Organization, *Guideline on Data Integrity*, Switzerland, June 2020, *https://www.who.int/docs/default-source/medicines/norms-and-standards/current-projects/qas19-819-rev1-guideline-on-data-integrity.pdf*

9 Medicines and Healthcare Products Regulatory Agency, "MHRA GxP Data Integrity Definitions and Guidance for Industry," United Kingdom, 21 July 2016, *https://www.gov.uk/government/news/mhra-gxp-data-integrity-definitions-and-guidance-for-industry*

10 HR 3763 Sarbanes-Oxley Act of 2002, USA, 2002, *https://www.congress.gov/bill/107th-congress/house-bill/3763*

11 Edemekong, P. F.; P. Annamaraju; M. J. Haydel; "Health Insurance Portability and Accountability Act," National Library of Medicine, USA, 3 February 2022, *https://www.ncbi.nlm.nih.gov/books/NBK500019/*

12 D'Halluin, C.; "The Importance of Data Integrity in the Finance Industry," *Payments Journal*, 6 December 2021, *https://www.paymentsjournal.com/the-importance-of-data-integrity-in-the-finance-industry/*

13 Deloitte, *Under the Spotlight: Data Integrity in Life Sciences*, United Kingdom, 2017, *www2.deloitte.com/content/dam/Deloitte/uk/Documents/life-sciences-health-care/deloitte-uk-data-integrity-report.pdf*

Cooperating With Fear

Throughout human evolution, fear has been crucial to survival. The brain is made to fear uncertainty.[1] When experiencing fear, the amygdala in the brain actively works against the ability to rationalize. Therefore, when reacting to fear, humans think quickly instead of slowly,[2] which leads to bias in the decisions made. People may believe that they are making rational decisions, but if they are acting out of fear, they most likely are not.

By acknowledging the complexities of security and cooperating with the element of fear, enterprises are empowered to focus on their most critical sources of risk.

Humans' cognitive evolution, including the ability to imagine fiction,[3] has improved the ability to consider risk. Being risk-aware, while developing knowledge, actions and inventions that decrease risk, leads to fewer injuries and deaths. However, humans are shaped by their histories to act on risk that is simple and within sight. The human brain is wired to perceive straightforward risk, which is beneficial early in life. As humans grow, this can become a habit.

Unfortunately, for some enterprises, security becomes an out-of-sight, out-of-mind domain, which often exposes the enterprise to the effects of fear. This can result in exaggerated control of less important sources of security risk, leaving more important ones neglected. By acknowledging the complexities of security and cooperating with the element of fear, enterprises are empowered to focus on their most critical sources of risk.

Determining the Real Danger

Even though risk for humans has changed significantly over thousands of years, fear has always been present. Fear is subjective and sometimes irrational, so how does one determine what to fear?

Cardiovascular diseases were the biggest killers in the world in 2019, causing a staggering 18.56 million deaths.[4] But cardiovascular diseases generally are not a predominant fear in daily life.

This is because they are a complex and not a highly visible source of risk. Cardiovascular diseases are typically caused by unhealthy lifestyles, characterized by a nutrient-poor diet, physical inactivity, and tobacco and alcohol use.[5] In the minds of many, mitigating actions such as a healthy diet and exercise are not directly correlated to preventing disease. Because diseases may develop over a long period of time and are not immediately obvious, the risk is not as evident until it comes to fruition.

The ability to deal with complex, niche sources of risk such as cardiovascular disease requires slow thinking, which can be challenging to master. For this reason, humans often simplify complex risk to process it faster, especially if they are not trained in how to think slowly.

JACOB ZWICKI | CISM, CISSP

Is the chief information security officer for group.ONE, a multibranded web hosting company. His interest lies in the intricate relationship between technology and humanity and how they influence each other. His focus is on the psychological and social impact of technology, exploring how it shapes communication, decision-making and overall well-being.

Fear in risk management can have significant consequences, such as exaggerated security controls being imposed and more serious sources of risk being neglected if attention is not directed to the right areas.

The connections in the brain's neural network become stronger with repetition.[6] So, the training of slow-thinking capabilities is crucial because it plays a key role in the ability to piece together information and draw thoughtful conclusions.

When humans are exposed to stories about someone getting injured due to not wearing a bike helmet, they are reminded that not wearing a bike helmet leads to injuries. The neural connections in the brain supporting that narrative are strengthened, while other aspects are not. The perceived impact is dominant for human understanding of risk at this stage, and if there is an easy method of mitigation, it is preferable and less stressful. Therefore, the message is to wear a bike helmet to be safe when riding a bike.

This is one of the reasons there is a continued struggle to contend with climate change. Climate change is a complex problem with many aspects, uncertainties and ramifications. It is an out-of-sight, out-of-mind risk for most humans because they do not yet suffer from its direct impact.

The Impact of Fear on Security

So, why are these considerations important to the information security domain?

Fear in risk management can have significant consequences, such as exaggerated security controls being imposed and more serious sources of risk being neglected if attention is not directed to the right areas.

One of the most notable public catastrophes due to neglecting risk in modern times is the meltdown of the Chernobyl nuclear power plant.[7] The plant's operational procedures failed to account for the human factor,[8] having designs in place that outstripped the ability of the operators to use it safely because they did not correctly understand the risk and risk indicators.

Security professionals working with risk management should acknowledge the impact of fear and establish methods to prevent irrational thinking and decision-making. Less visible sources of risk should be made evident and understandable for all stakeholders in partnership with the enterprise. To do this, requires three important steps:

1. Choosing the right security framework
2. Aligning with the vision and mission
3. Applying slow thinking

Choosing the Right Framework

Context is essential for understanding the value of content. The right operational security framework provides value by making security transparent and accessible. By studying reputable security frameworks, enterprises can select the one that is most suitable for their needs. A framework should be selected based on several criteria:

- **Internal communication and adaptation**—It should be easy for nonsecurity employees to access, read and understand the content of the chosen framework. Relevant information must be easy to find and preferably be integrated into existing communication platforms. Stakeholders should consider how much information is made inaccessible because of additional hoops the receiver must jump through before accessing what is relevant to them. If this is not achievable, more customized communication to the most important stakeholders should be prioritized.
- **Integration of the existing governance model**—The organization's current governance methods should be reflected in the newly adopted framework. Changing culture can be difficult for employees, so finding a framework that supports the existing model makes the transition much easier.
- **External stakeholders**—Enterprises should choose a framework that meets the expectations of external stakeholders. Whether customers, supervisory authorities or others, external stakeholders have a significant impact on security. Organizations should familiarize themselves with those expectations and their possible impact and take them into consideration when selecting a framework.

LOOKING FOR MORE?

- Read *Optimizing Risk Response. www.isaca.org/optimizing-risk-response*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Choosing the right framework increases the likelihood of those involved in risk management trusting new procedures and, therefore, engaging actively with the process. When this is achieved, the output is less irrational and biased by personal opinions, ensuring that fear has less of an effect on operations.

Aligning With Vision and Mission

Context is everything. Vision and mission are rooted deep within an organization and can lend themselves to understanding the challenges an enterprise experiences.

When assessing risk, an understanding of why it is important to assess the risk is crucial. Consider this example: Parents are debating whether it is necessary for their child to wear a helmet when riding a bike. Parent A believes that the child rides the bike to go from A to B, so riding the bike is solely perceived as a means of transportation. Parent B believes that the child riding the bike is an important form of social interaction with other kids. Riding the bike is about being with others and belonging to a group.

Parent A considers the distance and route traveled, the speed of the bike and the child's riding experience compared to the risk of injury. Parent B's line of thinking consists of Parent A's considerations combined with aspects of the other kids' behavior, the child's social status in the group, whether the design of the helmet is sufficient in the eyes of the other kids, and the other kids' parents' views on wearing a helmet. Parent B compares these qualities against the risk of injuries combined with the danger of feeling like an outsider compared to the rest of the group or even losing certain aspects of identity.

Although the parents agree on the basis of loving their child and wanting to protect them from harm, their differing perspectives involve different considerations with different losses and gains.

Aligning on the why is crucial to establishing a common understanding when assessing risk. This requires an enterprise to be precise when determining the objectives of risk management initiatives, which should be linked to the organization's vision and mission.

Alignment on the why is typically driven by culture, which, for many organizations, is rarely fully controlled. Identifying and being more explicit about the why increases the likelihood of realizing the preferred outcome.

Putting the enterprise vision and mission first creates a common foundation for a more objective assessment of risk and a minimized impact of fear.

Putting the enterprise vision and mission first creates a common foundation for a more objective assessment of risk and a minimized impact of fear.

Apply Slow Thinking—Fear Thrives in the Opposite

Anyone who has ever tried to force creativity likely agrees that it is close to impossible. Many may reflect on some of the decisions they made in stressful situations and think they were not the best.

Achieving an analytic, creative state of mind requires the brain to be in a relaxed state. When stressed, the mind looks for quick and easy solutions to bring itself out of the uncomfortable state. This phenomenon has the benefit of encouraging swift reaction, but such a reaction is typically less informed than it would be under calm circumstances. When reacting swiftly, the mind's focus is on only one or two things. Having a holistic perspective slows the decision-making process, which is why being in a stressful, uncomfortable situation is not preferable when one should apply slow thinking.

Practicing procedures is the key to success for professional groups that frequently encounter stressful situations. This is also why procedures are not written in real time during stressful situations, but rather afterward with newfound knowledge, when time and slow thinking are available.

Fear is built into stressful situations, which is disturbing. So, when the mind is in a stressful state, decisions are likely to become irrational and informed by narrowed perspectives.[9] The outcome of risk management with a stressful mindset must be considered. It is shortsighted, irrational and not holistic. To avoid this dynamic, practitioners should find appropriate methods—which are impacted by variables such as mood, sleep, food, workload, culture, exercise and skill level—or establish a clear state of mind when conducting risk management

activities. This is crucial to limiting the influence of fear that is hardwired into the mind.

Conclusion

In recent years, some have argued that risk management has failed to provide proper value. Arguments such as, "There are too many uncertainties, so why bother?" have been raised. It could be surmised that such suggestions originate from the many failed implementations of risk management that do not limit the influence of fear and create unrealistic expectations.

All living beings engage in risk management. It is wired into biology. What separates humans from other animals is the ability to cooperate with fear rather than be controlled by it.

Endnotes

1 Robinson, B.; "What Brain Science Reveals About Uncertainty and Six Strategies to Cope at Work," *Forbes*, 24 August 2022, *https://www.forbes.com/sites/bryanrobinson/2022/08/24/what-brain-science-reveals-about-uncertainty-and-6-strategies-to-cope-at-work*

2 Kahneman, D.; *Thinking, Fast and Slow*, Farrar, Straus and Giroux, USA, 2013

3 Martone, R.; "Signs of Modern Human Cognition Were Found in an Indonesian Cave," *Scientific American*, 17 April 2020, *https://www.scientificamerican.com/article/signs-of-modern-human-cognition-were-found-in-an-indonesian-cave/*

4 Our World in Data, "Number of Deaths by Cause," 2019, *https://ourworldindata.org/grapher/annual-number-of-deaths-by-cause*

5 Centers for Disease Control and Prevention, "Know Your Risk for Heart Disease," USA, 21 March 2023, *https://www.cdc.gov/heartdisease/risk_factors.htm*

6 Schmelzer, G.; "Understanding Learning and Memory: The Neuroscience of Repetition," January 2015, *http://gretchenschmelzer.com/blog-1/2015/1/11/understanding-learning-and-memory-the-neuroscience-of-repetition*

7 World Nuclear Association, "Chernobyl Accident 1986," April 2022, *https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx*

8 Vicente, K.; *The Human Factor*, Routledge, USA, 2006

9 Sharot, T.; "Why Stressed Minds Are More Decisive," BBC, 15 June 2018, *https://www.bbc.com/future/article/20180613-why-stressed-minds-are-better-at-processing-things*

Bank's CyberOps Team Wins EDR Buy-In

In 2015, Israel's Supervisor of Banks issued *The Proper Conduct of Banking Business Directives*, a sprawling set of regulations that set "prudential requirements for proper conduct of banking business on various matters."[1] The directives address risk management in Regulation No. 361, Cyber Defense Management, also known as Order #361.[2]

The government's new demands on financial institutions led to an important career experience for Ofir Eitan, a cyber operations manager employed at one of the largest financial institutions in Israel at the time. In January 2016, he was tasked with establishing a new cyberoperations (cyberops) team within the information security (infosec) department to develop a plan for achieving compliance with Order #361, among other responsibilities. Eitan's first step was to conduct a review of the bank's cybersecurity posture.

The review process was intensive. Over a three-month period, Eitan conducted interviews "with a long list of core employees in the company," he recalled, including the head of infosec, the chief risk officer (CRO), the head of IT infrastructure, the head of network administration and the director of business continuity planning (BCP). The department's final product was a report showing Order #361's directives, the bank's compliance status, and a suggested road map for bridging gaps and mitigating risk.

EDR Is Critical

"Endpoints are the battlefield to protect networks against malware attacks," Eitan said. The most worrisome risk he identified was the bank's lack of an endpoint detection and response (EDR)[3] security solution. The focus of the bank's control environment was twofold: prevention and compliance, which required monitoring of critical servers to meet regulatory requirements. Its strategy was based on protecting selected systems rather than on defining a one-stop-shop solution for comprehensive security visibility and response. Endpoint visibility, forensics and malware remediation capabilities were lacking.

A core incident response (IR) tool stack, Eitan said, should consist of a security information and event management (SIEM) system integrated with EDR, intrusion prevention systems (IPSs), intrusion detection systems (IDSs), an email gateway, and a threat intelligence platform (TIP) (**figure 1**).

Compared to other incident response solutions, EDR is the primary one-stop-shop. EDR should be utilized by an organization's blue team[4] as the main battlefield defense against malware and intruders, Eitan maintained. He laid out the core capabilities that a robust EDR solution provides:

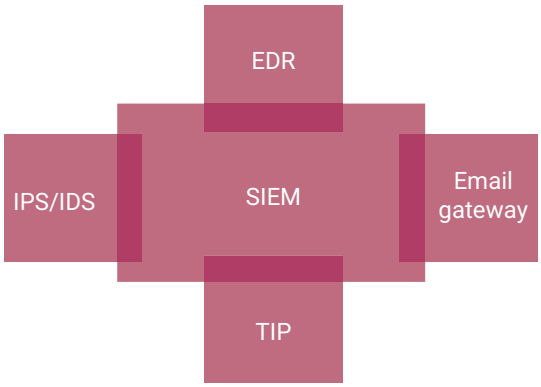
- **Visibility and control**—Different organizations may use different combinations of security tools to design their control environments. However, it is essential to equip security professionals with a single platform that can provide full visibility and control over network endpoints to detect malware threats and execute all phases of the incident response cycle in a comprehensive, timely and

MICK BRADY

Is a freelance technology communicator with more than 20 years of experience editing and writing for technology-focused publications.

FIGURE 1

Core IR Tool Stack

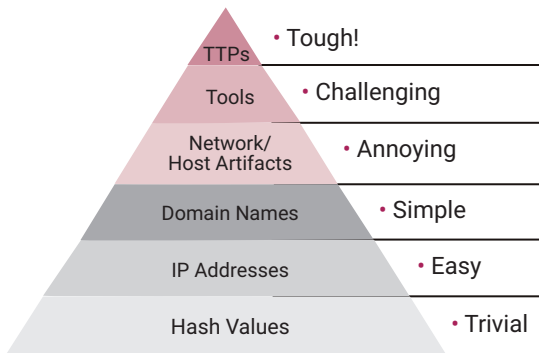


efficient manner, Eitan noted. An organization experiencing a ransomware attack on its network, for example, needs to respond quickly and, preferably, automatically. The old way—that is, physically logging in to each endpoint, copying the memory disk, indexing the data based on predefined components and then running a full forensics investigation—is no longer a scalable solution against cyberattacks. In any case, it is virtually impossible to apply it in a cloud or hybrid environment.

- **Maximum intelligence**—Because the cyberthreat landscape is constantly evolving, defenders are challenged to stay up to date with the latest threats. In addition to incorporating signature-based monitoring and prevention, Eitan said, organizations should pursue near-real-time monitoring using the latest behavioral tactics, techniques and procedures (TTPs) and indicators of compromise (IOCs) (**figure 2**). The cyberops team at his financial institution was able to upgrade its intelligence program through multiple avenues. "Our business case resonated with the bank. We upgraded the program from feed-based to threat intelligence platform-based (TIP-based), which also supported other security teams in the bank, such as the antifraud unit that gets alerts on stolen credit card numbers. Further, my team helped shore up the IT infrastructure through prioritizing and expediting patch management based on the latest exploited vulnerabilities," Eitan said.

FIGURE 2

Pyramid of Pain—IOCs That Can Be Detected and Prevented



Source: Bianco, D. J.; "The Pyramid of Pain" Enterprise Detection and Response, 1 March 2013, *https://detect-respond. blogspot.com/2013/03/the-pyramid-of-pain.html.* Reprinted with permission.

- **Immediate and comprehensive response actions**—In addition to preventive capabilities such as blocking access by Universal Serial Bus (USB) devices and banning hashes based on their reputation, EDR provides a robust first response to malware found in endpoints. Vendors sometimes configure EDR to operate automatically. With a click of a button, the EDR tool may be able to kill suspicious/malicious processes, isolate targeted endpoints, enforce existing policies (e.g., whitelisting) to prevent malicious applications from running, or activate other incident responses that would take valuable time if implemented manually.
- **Sandboxing**—Filtering of files and code strings in an isolated and cloud-based environment is key to implementing a one-stop-shop EDR solution. In addition to sanitizing files, a sandboxing feature can record the various processes and running codes in the network, constantly making comparisons with suspicious scenarios. The rules should trigger alerts based on a scoring method that is aligned with the organization's incident response plan (IRP).

Although the bank lacked sufficient capabilities to detect and eradicate malware threats in a timely manner, its security strategy did have its strengths. Its existing SIEM and other endpoint security tools were advanced solutions with comprehensive capabilities for mitigating compliance risk and insider threats.

"The head of infosec was able to implement a state-of-the-art preventive control environment, which included high-level segmentation, secured Internet access, a strict public-facing server policy and a thorough patch management process," Eitan said.

Those strengths contributed to his most complicated challenge: getting buy-in for a more robust security

program that could offer a similar level of protection against malware and advanced persistent threats (APTs). Eitan's primary objective at the time was to demonstrate to leadership that the most prominent threats would likely penetrate the bank's first line of defense, forcing response teams to contain and eradicate attacks on an already breached network.

Four-Pillar Mitigation Plan

To mount an offensive strategy in a war against determined cyberintruders, the bank needed security tools and personnel capable of identifying network compromises and malware insertions and eradicating them, Eitan said. He proposed a mitigation plan based on the MITRE ATT@CK framework's TTPs, an approach that couples extensive intelligence feeds with behavioral detection rules (**figure 3**).

The plan was designed to ensure that every associated project or initiative designated would not only address Order #361 regulatory directives, but also encourage buy-in for the purchase and implementation of a comprehensive EDR solution. It consisted of four key pillars:

1. Establish a three-tier operations model equipped with endpoint discovery and forensics investigation capabilities and based on an IRP.
2. Implement a proactive threat and vulnerability management program combining breach and attack simulation (BAS) with a TIP. Define processes to prioritize mitigation plans based on intelligence and attack simulation findings. Enrich detection and investigation based on tactical intelligence.
3. Institute a training program designed to benefit employees at all levels within the organization: tabletop exercises for C-suite executives, cyberexercises for the IT department, and hands-on training for the responders. (A new computer security incident response team [CSIRT] had recently been formed in the IT department as part of the cybersecurity program.)
4. Conduct a security control policy review and make configuration changes based on the threat landscape to secure the email gateway, vaults, IPS/IDS and web platforms (e.g., enterprise web email platforms, social media accounts).

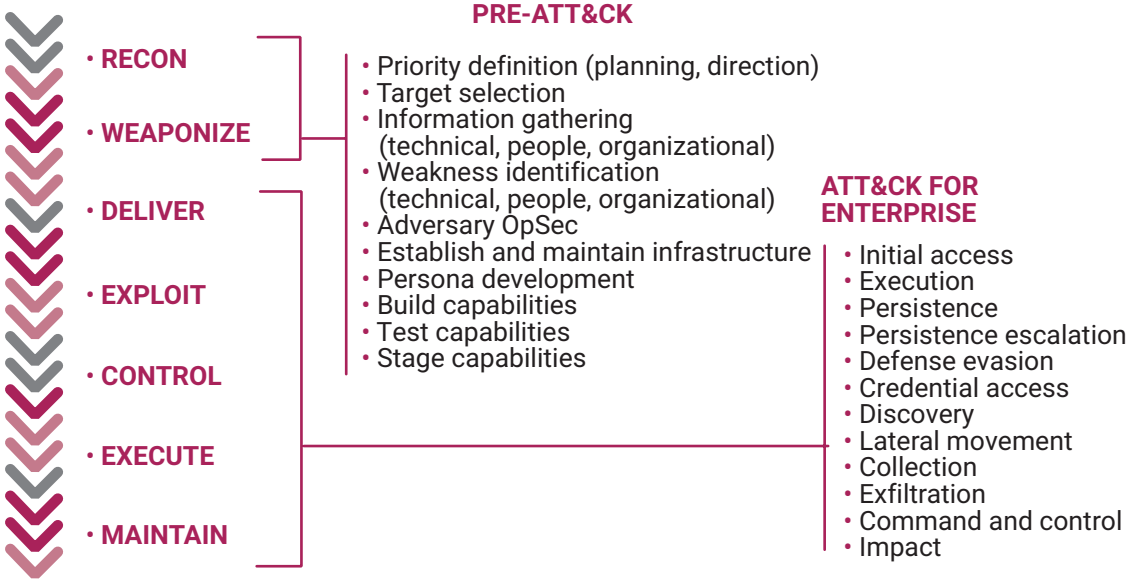
The proposal faced resistance. A new chief information officer (CIO) had been onboarded at the bank just as the cyberops team concluded its review, and he questioned the plan, mainly due to budgetary constraints and other pressing priorities.

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 3

MITRE ATT&CK Framework to Build Use Cases



Source: Burg, S.; "Introducing the MITRE ATT&CK Enterprise Framework Collection," Cyberbit, 17 August 2020, *https://www.cyberbit.com/cybersecurity-training/introducing-the-mitre-attck-enterprise-framework-collection-2/*. Reprinted with permission.

The bank's budget-constrained security plan was a bigger problem, though, because it would allow the deployment of agents only at endpoints where suspicious activity was detected by the SIEM for further forensics and endpoint discovery.

"The head of information security was the acting and primary cybersecurity leader. He reported to the CIO and I reported to the head of the information security department," Eitan explained. "It was the head of information security department's decision to establish a new team dedicated to designing and implementing a revised cybersecurity program. It was approved by the former CIO."

Problems arose when the new CIO chose to rethink the approval his predecessor had already given, Eitan noted. He had not been involved in approving formation of the team. He took note of all the security resources the bank had in place—thanks in large part to the head of information security department's efforts—and challenged the new cyberops team on the need for an EDR solution, given the multiple other agents in use to reduce risk.

To make the team's case, Eitan said he adopted a strategy "based on an intelligence analysis of global and local incidents to showcase how the bank could face similar fatal ramifications without properly defending against similar threats." He conducted a TTP[5] analysis and showed the attack kill chain, demonstrating that the bank's controls were insufficient to protect it.

At that time, ransomware attacks were just beginning to emerge, and the targets initially were home users. The CIO acknowledged that there were weaknesses in the bank's defensive system, but he believed the alarms raised in industry and media reports over advanced security threats were exaggerated. He said that further due diligence by the infosec team would be necessary to justify an EDR system. In the CIO's view, additional major investments in security tools were not immediately warranted, particularly since temporary financial constraints at the bank were resulting in delays in several initiatives for the following year.

Setting Plan B in Motion

Eitan was directed to focus on developing the incident response plan and training program first, but his team persisted in seeking buy-in for its overall recommendations. "WannaCry[6] was the beginning of the turning point," he recalled.

A ransomware worm that struck in 2017, WannaCry had a devastating global impact, encrypting files on hundreds of thousands of Windows computers and demanding ransom payments in exchange for decrypting them. However, most of those who paid ransoms did not have their access restored, so willingness to pay a ransom as a response tactic was exceedingly risky. Heavily regulated industries, such as banking institutions, were reluctant to do business with unreliable cybercriminals.

The ransomware threat soon mushroomed, demanding fast, effective action. At the bank, Eitan's team was permitted to acquire a low-budget host discovery tool, RSA-ECAT,[7] which was useful in demonstrating that the threat was real and immediate. The new tool detected attempts by prominent ransomware variants to breach the bank's unclassified WiFi network. Although bank operations were not impacted by that attempt, ransom notes and disarmed executables were found at multiple endpoints. Combined with the potential damage associated with WannaCry, that attack helped demonstrate that the threat was real and that attackers were knocking on the bank's doors.

However, there were significant downsides to relying on the RSA-ECAT system, said Eitan. It provided limited CTI feed integration and was not user-friendly. The RSA-ECAT deployment "was designed only for an aftermath threat scenario," Eitan said, "definitely not for a proper mitigation plan against ransomware, which distributes much faster than the bank's ability to reach proper agent saturation before the ransomware can impact the network."

The bank's budget-constrained security plan was a bigger problem, though, because it would allow the deployment of agents only at endpoints where suspicious activity was detected by the SIEM for further forensics and endpoint discovery.

The secondary projects and programs that were part of the original proposal were approved and funded—and

their value subsequently demonstrated—but approval for the key piece, the EDR tool, was still on hold.

"We genuinely tried to find secondary alternatives to utilize to achieve similar functionalities," Eitan said. However, as the team implemented those other projects, it used them specifically for the purpose of achieving buy-in for the EDR.

In addition to creating an incident response plan, the team wrote up EDR and SIEM use cases, developed TIP integrations, built tier 1-3 operating models and designed a training program. It reevaluated all current agents and the existing control environment based on the IRP and use cases. Although the team achieved several quick wins with the available tools, such as implementing some threat feeds and blocking malicious hashes, the improvements were far from what a comprehensive EDR solution could offer.

None of the measures were adequate EDR substitutes, but they served to prove the team's business case for stronger threat detection:

- **BAS**—Demonstrated how prominent threats (e.g., ransomware, advanced persistent threats [APTs], behavioral TTP) could potentially breach the network
- **Threat landscape analysis**—Defined the scope of the top priority threats with supporting case studies
- **Training**—Triggered discussions about the bank's ability to mitigate prominent threats

Eventually, the team managed to accomplish everything necessary to go forward with an EDR implementation, including benchmarking for desired solutions and identifying the people, processes and technologies necessary for integration with other tools, such as the SIEM, TIP and email gateway. The only thing left to do was get approval and start the EDR project.

Presenting a united front in support of the business case tipped the balance in favor of acquiring an EDR solution.

Revisiting the Case for EDR

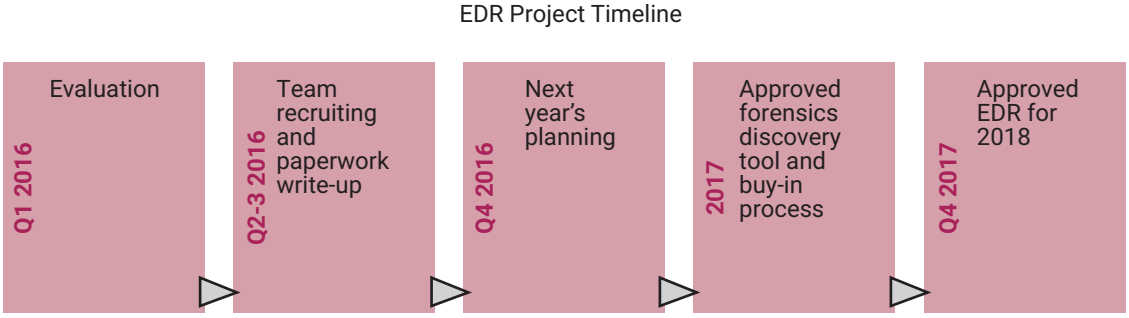
Eitan sought—and obtained—buy-in from other prominent figures at the bank, including the chief revenue officer (CRO), relevant IT directors and the head of the information security department. To underscore the importance of their goal, he and the head of the information security department adopted a motto that likened EDR to antivirus (AV) software: "EDR is the new AV—it's a must for every organization."

Presenting a united front in support of the business case tipped the balance in favor of acquiring an EDR solution. The agenda presented by some of the IT teams involved in maintaining the control environment also helped achieve buy-in. Those team members advocated for the need to acquire and implement an EDR solution and expressed support for all the efforts incorporated in the IR program (i.e., the development of an IRP and a training program, the creation of use cases, and the integration of threat intelligence feeds).

After nearly two years of working toward the implementation of an EDR, Eitan was gratified to see it finally approved (**figure 4**).

FIGURE 4

Timeline for Gaining Approval of the EDR Proposal



EDR Project Timeline

Although Eitan started working in the United States and was no longer with the bank by the time its EDR project was complete, his control mapping report demonstrated two critical findings:

1. The risk assessment was high regarding the top threats to the bank (i.e., ransomware, espionage APT, terror/destructive APT). It demonstrated high severity and probability based on intelligence analysis and security control evaluation.
2. The threat mapping demonstrated that without EDR it would not be possible to detect several key threats. Further, the bank's capabilities for responding to data breaches were not streamlined, and its capabilities for mitigating a ransomware outbreak were insufficient.

With its EDR implementation fully deployed, the bank would enjoy a much-improved security posture, with substantially reduced risk and vastly improved threat detection and response capabilities.

Endnotes

1 Bank of Israel, "Banking Supervision," *https://www.boi.org.il/en/BankingSupervision/SupervisorsDirectives/Pages/nihultakin.aspx*

2 Supervisor of Banks, "Proper Conduct of Banking Business Directive (9/21) [2] Cyber Defense Management," Israel, 30 September 2021, *https://www.boi.org.il/media/422h2aed/361_et.pdf*

3 Wright, G.; A. Gillis; "Endpoint Detection and Response (EDR)," *TechTarget*, April 2021, *https://www.techtarget.com/searchsecurity/definition/endpoint-detection-and-response-EDR*

4 National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC), "Blue Team," USA, *https://csrc.nist.gov/glossary/term/blue_team*

5 National Institute of Standards and Technology Computer Security Resource Center, "Tactics, Techniques, and Procedures (TTP)," USA, *https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures*

6 Fruhlinger, J.; "WannaCry Explained: A Perfect Ransomware Storm," *CSO*, 24 August 2022, *https://www.csoonline.com/article/3227906/wannacry-explained-a-perfect-ransomware-storm.html*

7 RSA, "New RSA ECAT Release Engineered to Extend Ability to Rapidly Detect and Block Advanced Threats on Endpoints," PR Newswire, 22 July 2015, *https://www.prnewswire.com/news-releases/new-rsa-ecat-release-engineered-to-extend-ability-to-rapidly-detect-and-block-advanced-threats-on-endpoints-300116802.html*

Using Near Miss Incidents as Risk Indicators

Disponibile anche in italiano
www.isaca.org/currentissue

Any unforeseen event that does not cause apparent damage while perhaps having the potential to do so is particularly interesting for providing an idea on how to build a risk indicator,[1] which warns of the approach of an unwanted situation and should be analyzed as such. In the field of information security, having timely alerts on the quality of the information protection system is of vital importance. Performance and risk indicators are essential sources for measuring the effectiveness of the protection measures adopted. The difficulty is finding the appropriate information to develop indicators fit for purpose.

Attention is mainly focused on the performance indicator because it provides an immediate and continuous measurement of the evolution of an action. Risk indicators, on the other hand, are linked to signaling the occurrence of a specific event and focused on the prevention or containment of potential consequences. In other words, performance indicators are a showcase of the results achieved, while risk indicators are a magnifying glass that can be used to observe what is useful for the organization to achieve its objectives.

Differentiating Between Indicators

Performance indicators are often easier to identify than risk indicators. In the project requirements, the parameters for the control have already been established (i.e., the measurements of the extent to which the functioning of the activity corresponds to what is expected). For example, consider a car; its purpose is to transport people from one place to another more rapidly and efficiently than previous forms of transportation. In this case, speed is an important parameter, and the speedometer is a typical performance indicator. The speedometer instantly indicates the speed, and it does so for the entire period of vehicle activity. Ideally, there should also be an indicator of the maximum speed limit and an audible signal should be emitted in the event of reaching the preestablished speed threshold. This is a risk indicator. It signals when the speed reaches the threshold beyond which it is no longer acceptable to accelerate because there is a potential for unintended consequences (e.g., fines, damage to people or things).

Due to the ability of the risk indicator to predict the elevating risk of a given situation, it is also called an early warning (i.e., it highlights the entry into a potentially dangerous condition). However, there is an objective difficulty in identifying risk indicators because they are not part of the original idea of what is to be achieved, and often, the elements to determine them are discovered only in the operational phase.

Performance is a required result, and the way to evaluate it is always well defined in the project requirements, while the risk event is a consequence of unexpected vulnerabilities (despite the risk analysis, the exact moment remains undetermined) that could emerge in the development, implementation or operational phases or because over time new threats can arise and change the risk scenario. The ability to signal the approaching risk

LUIGI SBRIZ | CISM, CRISC, CDPSE, ISO/IEC 27001 LA, ITIL V4, NIST CSF, UNI 11697:2017 DPO

Is a lead auditor and a senior consultant on risk management, cybersecurity and privacy issues. He has been the risk monitoring manager at a multinational automotive company for more than seven years. Previously, he was responsible for information and communication operations and resources in the Asia and Pacific Countries (APAC) region (China, Japan and Malaysia) and was the worldwide information security officer for more than seven years. He developed an original methodology for internal risk monitoring, merging an operational risk analysis with a consequent risk assessment driven by the maturity level of the controls. He also designed a cybermonitoring tool and an integrated system involving risk monitoring, maturity model and internal audit. Sbriz was a consultant for business intelligence systems for several years. He can be contacted on LinkedIn at *https://it.linkedin.com/in/luigisbriz* or at *http://sbriz.tel.*

cannot be based only on exceeding the operating limits, but it must be consistent with the risk scenario and its assessment.

Determining Risk Indicators

An empirical way to determine a risk indicator is to start from the risk scenario, considering all the vulnerabilities that have emerged in operations. Then, instead of continuing with the risk analysis, a cause-and-effect analysis should be implemented to identify the factors underlying the identified weaknesses. This step highlights the dynamics of the relationships between the operational actions, the elements of weakness, and the identified threats to establish measures to estimate the extent of the phenomenon and use them to determine an alarm activation threshold in the event of a risk level variation. Within the set of identified causes, the organizations must choose the one that will produce the most serious impact, and this will be the basis of the key risk indicator (KRI).

The path to establishing the risk indicator is quite easy, but only if the analysis has suitable sources of data on vulnerabilities. In addition, it can be helpful to focus on a category of situations that are potentially harmful but without obvious consequences—near miss incidents. Not all of them are significant, but they are a source of potential vulnerabilities that cannot be overlooked in the risk scenario.

Understanding Near Miss Incidents

A near miss incident is an unplanned event that has the potential to cause an impact but does not actually cause significant consequences. Although it may not produce obvious effects on the protection system, it is, in any case, an alert to the presence of a real vulnerability, and, as such, it must be addressed through a preliminary analysis that determines its severity. Due to the similarity of this concept with that of the risk indicator, near miss incidents can be considered ideal candidates for creating risk indicators.

The first consideration is the type of risk indicator that can be built. It is lagging because it is based on events that have already occurred. Furthermore, it has the possibility of satisfying the most significant characteristics that make the indicator effective:

- **Impact**—The analysis carried out within the risk scenario ensures that only reports relevant to the organization are considered.
- **Effort**—The indicator is a warning already present in the control environment and only needs to be evaluated in terms of severity.
- **Reliability**—The indicator is a real occurrence of an unexpected event where the vulnerability that facilitated it must be assessed.
- **Sensitivity**—The evidence gathered guarantees the accuracy of the risk analysis because it is derived from concrete facts.
- **Repeatability**—Phenomena are constantly monitored, and the analysis can take advantage of past events stored in the risk register.

Due to the similarity of this concept with that of the risk indicator, near miss incidents can be considered ideal candidates for creating risk indicators.

Further consideration has a beneficial impact on the organization's risk culture. Having a mature risk culture means also analyzing events that have not caused damage. Formalizing the systematic analysis of near miss incidents is a way to give attention to apparently insignificant events and is an indication of maturity in risk management. In an immature risk culture, these incidents would be considered lucky events that did not require specific actions. Instead, completing this analysis would create time to understand the event and take action.

A near miss incident is a risk indicator that could activate an appropriate event management procedure if it should occur in a foreseen situation or could lead to the intervention of a risk practitioner to determine the cause and assess the severity of the risk. There are two types of near miss incidents that can be used to clarify how to generate risk indicators: the results of an internal audit and the detection of computer viruses.

Near Miss Incidents and Internal Audit

The concept of a near miss incident has various meanings, including the unexpected violation of policies, guidelines, standards, regulations or procedures or even deficiencies in the definition of rules. The internal audit process ensures alignment between the correct functioning of the organization's processes described in its organizational documents and the business objectives. Near miss incidents can function in similar ways to internal audit findings in that they alert to potential violations or vulnerabilities that need to be addressed. When the auditor detects deficiencies in the organization's control environment, the findings should not only be filed in the audit opinion or remediation plan, but also should be communicated to the risk manager to analyze the implications for the objectives. The results of the audit recall the way risk indicators act (i.e., they warn of anomalous situations). Investigation is always needed.

Internal audit, by definition, must demonstrate the effectiveness of the internal control system. Detected weaknesses such as deficiencies in the assignment of roles or responsibilities, deadlines not met in updating documents or operational processes, or controls not performed provide an indication of organizational risk. Prior to the audit, these situations may be deemed fully functional, but any noncompliance is a potential cause of an incident (i.e., a near miss incident). Therefore, the finding is a risk indicator and its causes must be analyzed, the severity of its consequences with respect to the business objectives must be determined, and effective treatment must be undertaken.

Near Miss Incidents and Viruses

In addition to organizational weaknesses, risk indicators can be identified in the technological field. For example, antivirus reports allow the creation of interesting indicators despite the fact that antivirus systems have lost much of their effectiveness over time. The antivirus system needs to be reevaluated. It is perceived as a normal basic function to protect against attempts to compromise personal computers, while the protection of critical systems—rightly considered of greater value—is entrusted to sophisticated anti-intrusion tools capable of interpolating information from various network and system sources. The attention paid to the reports of these tools is very high. On the other hand, the notification of a virus detected on a personal computer almost never receives the classification of an incident if it does not affect critical systems, despite the fact that it has overcome some sort of defensive barrier and, therefore, has the potential to do damage. Generally, only the automatic remediation of the infected computer is foreseen, and it is recorded as a statistically irrelevant event certifying the success of the antivirus system.

Near miss incidents can function in similar ways to internal audit findings in that they alert to potential violations or vulnerabilities that need to be addressed.

Instead, from a risk point of view, warning of the presence of a virus has a different meaning. It is an opportunity to analyze the intrusion ability demonstrated by the virus and, consequently, the effectiveness of the in-depth defense system. This is why it is important to analyze two aspects of the infection. The first point is the intrusion technique used by the virus to evade defenses. It is helpful to understand what went wrong and which layers of protection were found to be vulnerable. In addition, the technique used by the virus could bring out a new threat. The second point is to understand the value of the potentially compromised resources at the depth of the defense system where the infection took place, and possibly reevaluate the level of risk.

If a virus has no significant consequences, it is often classified as having no impact, or being a near miss incident. Its relevance lies in the opportunity

LOOKING FOR MORE?

- Explore the *Risk Scenarios Tool Kit. www.isaca.org/risk-scenarios*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

to investigate causes and to collect information to understand where there is a flaw in the protection system, and to prevent major incidents. It should be noted that not all viruses can be used as lessons learned. Only those related to particular attack methods that bring out vulnerabilities are helpful, for example, the intruding, moving or masking properties of the virus. For the analysis, it is necessary to separate the infection techniques from the effect of the infection itself. The first are risk indicators, as they identify the activity carried out to cause the incident, while the second are performance indicators (of the virus), as they show the extent of the consequences. All reports of viruses that, due to their particular typology or specific characteristics, bring out some vulnerability in the organization's protection system should be included as risk indicators.

Conclusion

A near miss incident is an unplanned event that can potentially develop unintended consequences but does not actually develop them. From a risk perspective, it is an indicator of an anomalous situation and, as such, must be investigated to understand the potential impact on an organization's objectives. It provides an opportunity to analyze causes, identify solutions, and strengthen the protection system.

A near miss incident signals the presence of some type of vulnerability that must be addressed within an adequate time to resolve it. It is certainly not a zero-day vulnerability that would require an immediate remedy to mitigate the risk of unintended consequences. Being a potential incident means there is time to act, and the risk analysis tells how much time. Regardless, that amount of time is short because there is evidence of a real defect. The vulnerabilities associated with the near miss incident risk indicator could be called one-day vulnerabilities. The risk indicator signals the need to place the light of the analysis before the possible darkness of the risk.

The vulnerabilities associated with the near miss incident risk indicator could be called one-day vulnerabilities.

Endnotes

1 ISACA®, Glossary, *https://www.isaca.org/resources/glossary*

The Digital Twin Advantage in Automotive Manufacturing Systems

Digital twin technology has gained significant traction with the emergence of big data and the Internet of Things (IoT) and is now being utilized in many industries worldwide. A digital twin is a virtual model of a physical object designed to accurately reflect the object.

In digital twin technology, a physical object is outfitted with many sensors across different areas of functionality so that the sensors can effectively measure attributes of the physical object (e.g., temperature).[1] The sensors collect and relay data to the processing system, which applies the data to the digital copy, updating it in real time. With these data, simulations using artificial intelligence (AI) wand machine learning (ML) can be run on the virtual model to further study performance and help make decisions.[2]

The data allow for valuable insights that can be applied to the original physical object, improving its overall condition and performance.[3]

Virtual models are used by industries such as construction and automotive manufacturing to help identify which areas of performance manufacturers should focus on and what possible improvements can be made. For example, the construction industry effectively uses digital models of buildings and bridges to understand their structural integrity better and to pinpoint any issues. In addition, digital twin technology is used in complex projects such as the production of jet engines, aircraft and automobiles to improve the overall efficiency of the products.[4]

Digital twin technology using AI and ML in the automotive industry can enhance the overall design and efficiency of automotives products; however, these technologies pose cybersecurity risk. Therefore, it is essential to understand the mitigation measures organizations can take to protect themselves and their products.[5]

ML Algorithms in Digital Twin Technology

Digital twin technology uses AI, or more specifically, ML algorithms, to effectively analyze and assess the large amounts of data the sensors provide.[6] The aim of both AI and ML is development of intelligent programs that can handle complex tasks. ML algorithms are built on three major components: representation, evaluation and optimization. These components have requirements that must be fulfilled to generate an ML model and algorithm effectively. An ML-based twin of a production root cause analysis (RCA) process is intended to diagnose the root cause

KARTHIK TRICHUR SUNDARAM

Is director of IT solutions management at Applied Materials. He has more than two decades of experience in supply chain and asset management business processes, working with organizations such as SAP. Sundaram has served on the judging committees for many technical awards and published many articles in the media and in the review panel of a leading journal. He has lead projects for global customers in asset intelligence networks, digital twins with the Internet of Things and Industry 4.0. He also recently implemented one of the first digital vehicle hub solutions in North America for a large agricultural automotive leader.

DIVYA KARTHIK

Is a DevOps automation and site reliability engineer at Poshmark. She has experience in working with a variety of new technologies and taking them from proof of concept to production. She has a background in debugging critical site reliability issues, software system design and DevSecOps. She enjoys learning about new products and technologies by participating in judging panels for the Stevie and Globee Awards. She has also been involved in leading a chapter of Women in Computer Science at the University of California, Davis (California, USA) and volunteering with the National Center for Women and Information Technology Aspirations in Computing Scholarship Committee.

of a deficiency or anomaly found in the finished product or during the manufacturing process. It enables line managers to troubleshoot the most likely root causes based on the tool's predictions, identify the problem definitively, and implement corrective and preventative actions (CAPA) without spending too much time and effort searching through machine maintenance records, operator history, processes and IoT sensor inputs.[7] The goal is to minimize machine downtime and loss of production and enhance resource utilization.

Most of the uses of digital twin technology in the automotive industry involve testing the products (namely cars) through simulations.

The Digital Twin Advantage in Automotive Manufacturing

The global digital twin technology market currently stands at US$9.5 billion and is expected to reach US$72.65 billion by the year 2032, at a robust compound annual growth rate (CAGR) of 22.6 percent from 2022 to 2032.[8] North America has the largest digital twin technology market share, with 40 percent.

The transportation and automotive sectors hold more than 15 percent of the market share due to growing demand for automotives. This could be explained by the growing adoption of electric vehicles (EVs) around the world.[9]

The advantages of digital twin technology are numerous, and its application can result in various advantages across industries. Most of the uses of digital twin technology in the automotive industry involve testing the products (namely cars) through simulations. This testing revolves around the manufacturing of automotive vehicles and how their performance can be enhanced.[10] Digital twin technology can provide several benefits for automotive manufacturers including:

- Executing tests using the digital copy of the product or vehicle and simulating crash tests, autonomous driving and other scenarios to enable a better understanding of the various aspects of the vehicle that could be improved.[11]
- Testing with digital twin technology to confirm compliance with standards and automotive industry certifications such as International Automotive Task Force (IATF) 16949[12] and International Organization for Standardization (ISO) standards ISO 9001:2015 *Quality management systems—Requirements*,[13] ISO 14001:2015 *Environmental management systems—Requirements with guidance for use*,[14] and ISO 45001:2018 *Occupational health and safety management systems—Requirements with guidance for use*.[15]
- Improving overall customer satisfaction through the use of digital twin technology by using the sensors and the data digital twin technology provides, for example, to improve the performance, lifespan, safety levels and fuel efficiency of vehicles.[16]
- Enhancing the overall agility and resilience of the supply chain through digital twin technology. To form an understanding of what materials model home manufacturers can use for construction, for example, and what would benefit the product.[17]
- Understanding the overall energy consumption of a product and how it behaves—an electric vehicle for example, by developing a digital copy or model of the product and running the necessary simulations and design changes on the digital model to ensure that there are no issues. Test results and ML algorithms can aid in achieving a superior design with less energy consumption. Manufacturers can also gain an understanding of how they can improve the overall aerodynamics of a car and reduce the vehicle's weight.

- Assessing the effect on a vehicle of environmental factors such as temperature and humidity using predictive ML algorithms. Based on the data, different models can be tailored to the needs of every region and their geographies. Modifications or revisions to an important component or part can be published on the digital twin platform, allowing seamless collaboration by original equipment manufacturers (OEMs), automotive manufacturers, customers and service providers.

These benefits are the primary drivers of digital twin technology implementation in many manufacturing facilities across industries. The US-based automotive manufacturer Tesla uses digital twin technology in every vehicle it produces.[18] Thinkwik, the partner that developed Tesla's digital twin application, states that real-time mechanical issues at Tesla Motors, regardless of their magnitude, are fixed by simply downloading over-the-air (OTA) software updates.[19] It is important for manufacturers to continuously exchange relevant data with the vehicles they produce to improve the quality of their products. The use of digital twins, along with pioneering technologies such as IoT, AI and ML, has made it feasible to perform processes that were once thought to be impossible.

Potential Risk of Digital Twin Technology

The adoption of evolving and emerging technologies to accelerate business growth inevitably creates an additional avenue of cyberrisk. Digital twins represent critical manufacturing assets that can directly affect an organization's bottom line. Though challenging, protecting digital assets is a key requirement organizations must meet when using digital twin technology. Although digital twin simulations can be used to monitor and track performance, they can also be configured to run real-life simulations to ensure that cybersecurity risk is mitigated.[20] However, securing digital twin operations, which are often hosted in the cloud, is another key challenge.

Digital twins represent physical systems, using additional inputs from sensors and controllers to provide a comprehensive summary for analysis. Although the physical assets may have protections such as microcontrollers or firewalls, digital twin representations can be vulnerable to security threats. Hackers can use cybersecurity threat techniques such as malware or spyware to control physical objects through digital twins, which could result in outages or major disasters. Digital twins may also represent objects that require intellectual property protection, such as semiconductors. If the digital twin is a blueprint of a piece of intellectual property, then hackers may be able to reverse-engineer and reproduce that property, bypassing the need for research and development of their own.

The use of digital twins, along with pioneering technologies such as IoT, AI and ML, has made it feasible to perform processes that were once thought to be impossible.

The security of any organization is only as strong as its weakest link. If digital twin credentials are exposed, the organization may be compromised. This is because most digital twins are connected through application programming interfaces (APIs) to IoT and other systems. Hackers can use a weak digital twin to disrupt or bring down an entire organization in a short amount of time.

Recommended Risk Mitigation Techniques

IoT devices are generally less secure than traditional devices such as processors, so using them as sensors in a twin setup creates concerns. Because most organizations already have a cybersecurity framework that does not cater to digital twins or other emerging technologies, new generation digital projects often involve internal cybersecurity experts only on a need-to-know basis. However, cybersecurity experts within and outside the organization can be engaged on a dedicated basis with a proper budget at each stage of a digital twin project to mitigate security risk areas. Security leaders and chief information security officers can teach their employees about authentication, authorization, data integrity, data confidentiality and nonrepudiation using their standard cybersecurity framework. Every apparent and perceived threat should be documented.

An organization's cyberframework should have policies that help its security infrastructure to be scalable and cyberresilient to meet growing security needs. Static security solutions cannot provide adequate security.

The key to scalable security is constant adaptation and redesign—not just expensive security products and specialized security experts. The cyberframework

LOOKING FOR MORE?

- Read *Audit Practitioner's Guide to Machine Learning, Part 1: Technology. www.isaca.org/audit-practitioner-guide-to-ML-part-1*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Many tend to overlook the longevity of digital twin technology; however, it can be used over the entire life cycle of the product, from the time of inception until its disposal.

should contain a planning strategy, streamlining, logic, up-to-date organizational policies, and security directives implemented by informed employees.

At both the interface level and the object level, digital twins should be protected with a zero-trust architecture. Multifactor authentication (MFA), microsegmentation and biometrics are additional layers of security that can help mitigate risk and provide returns on investment for secured organizational assets.

The use of ML algorithms for intrusion detection can help organizations identify and mitigate cybersecurity threats in a timely manner. However, it is imperative to train models using high-quality data sets to achieve successful intrusion detection. To build an attack model with high accuracy and low false positives, meaningful data collection and feature extraction are required. A digital twin-based security architecture can be effective for protecting industrial automation and control systems.[21] There are distinct security requirements for different components of the proposed architecture. It is advisable to synchronize clocks between the physical and digital twins at regular intervals to achieve active-state replication. Implementation of intrusion detection is critical to the entire architecture.

Conclusion

Digital twin simulation technologies are used by automotive manufacturers to gain an understanding of different aspects of the vehicle being designed. When applied to vehicle manufacturing systems, this technology can help reduce the cost of the vehicle, the level of carbon dioxide emissions, and fuel and maintenance costs, providing the manufacturer with a competitive advantage. Digital twins also allow manufacturers to improve the comfort, safety and efficiency of vehicles. ML algorithms can be used to develop digital models of a vehicle to test certain scenarios (e.g., vehicle crash, mechanical breakdown) and simulations to understand the various complexities and problems the product may encounter. They may also be able to improve the overall energy consumption of the vehicle, decrease air resistance, and make the vehicle more aerodynamic.

However, any organization that has digital twin capabilities is also at risk of cybersecurity threats. Digital twin projects should include cybersecurity experts at all stages. There should be enhanced security measures in place for all hybrid platforms and the network. Digital twins and their APIs should be tested for security vulnerabilities. Critical digital assets should be tested against hackers and disaster recovery mechanisms. A change agent can enforce security hygiene by implementing security measures such as zero trust architecture with MFA and additional security protection layers.

Digital twin assets security can be enhanced with ML. ML can analyze patterns in cybersecurity systems and learn from them to help prevent similar attacks and respond to changes in behavior. Real-time responses to active attacks can help cybersecurity teams be more proactive in preventing threats. Using ML-based cybersecurity systems to protect digital twin assets can reduce the time spent on routine tasks and enable organizations to utilize their resources more effectively.

Having an effective cybersecurity framework formalizes the subject matter expert's knowledge on anomaly detection. "If the framework has not seen a certain anomaly before, such as digital twin technology, a subject matter expert should analyze the collected data to provide further insights to be integrated into and improve the system," said Efe Balta, a postdoctoral researcher at ETH Zurich.[22]

The expert can either confirm the cybersecurity system's suspicions or teach it a new anomaly to store in the database. And as time goes on, the models in the system would theoretically learn more and more, and the human expert would need to teach them less and less.

Many tend to overlook the longevity of digital twin technology; however, it can be used over the entire life cycle of the product, from the time of inception until its disposal. The technologies composing digital twinning such as IoT, industrial IoT, AI, ML, big data, simulation and cloud computing have been on a path of constant evolution; thus, it can be assumed that digital twin technology will continue to evolve in parallel to these technologies.

Endnotes

1 Batty, M.; "Digital Twins," *Environment and Planning B: Urban Analytics and City Science*, vol. 45, iss. 5, 2018, p. 817–820, *https://journals.sagepub.com/doi/full/10.1177/2399808318796416*

2 Tao, F.; Q. Qi; L. Wang; A. Y. C. Nee; "Digital Twins and Cyber–Physical Systems Toward Smart Manufacturing and Industry 4.0: Correlation and Comparison," *Engineering*, vol. 5, iss. 4, 2019, p. 653–661, *https://www.sciencedirect.com/science/article/pii/S209580991830612X*

3 Tao, F.; Q. Qi; "Make More Digital Twins," *Nature*, 25 September 2019, *https://www.nature.com/articles/d41586-019-02849-1*

4 Rosen, R.; G. Von Wichert; G. Lo; K. D. Bettenhausen; "About the Importance of Autonomy and Digital Twins for the Future of Manufacturing," *IFAC-PapersOnLine*, vol. 48, iss. 3, 2015, p. 567–572, *https://www.sciencedirect.com/science/article/pii/S2405896315003808*

5 Singh, M.; E. Fuenmayor; E. P. Hinchy; Y. Qiao; N. Murray; D. Devine; "Digital Twin: Origin to Future," *Applied System Innovation*, vol. 4, iss. 2, 2021, p. 36, *https://www.mdpi.com/article/10.3390/asi4020036*

6 Zhou, G.; C. Zhang; Z. Li; K. Ding; C. Wang; "Knowledge-Driven Digital Twin Manufacturing Cell Towards Intelligent Manufacturing," *International Journal of Production Research*, vol. 58, iss. 4, 2020, p. 1034-1051, *https://www.tandfonline.com/doi/abs/10.1080/00207543.2019.1607978*

7 Kritzinger, W.; M. Karner; G. Traar; J. Henjes; W. Sihn; "Digital Twin in Manufacturing: A Categorical Literature Review and Classification," *IFAC-PapersOnLine*, vol. 51, iss. 11, 2018, p. 1016–1022, *https://www.sciencedirect.com/science/article/pii/S2405896318316021*

8 Dyson, L.; "Digital Twin Market to Grow 22.6 Percent Annually in Next Decade," Traffic Technology Today, 3 November 2022, *https://www.traffictechnologytoday.com/news/data/new-report-suggests-transportation-and-automotive-sector-will-sway-the-digital-twin-market.html*

9 Future Market Insights, Inc., "Transportation and Automotive Sector to Sway the Digital Twin Technology Market, Reaching US$ 72.65 Bn by the Year 2032," *GlobalNewswire*, 11 October 2022, *https://www.globenewswire.com/en/news-release/2022/10/11/2531840/0/en/Transportation-Automotive-Sector-to-sway-the-Digital-Twin-Technology-Market-reaching-US-72-65-Bn-by-the-year-2032-Future-Market-Insights-Inc.html*

10 Jiang, Y.; S. Yin; K. Li; H. Luo; O. Kaynak; "Industrial Applications of Digital Twins," *Philosophical Transactions of the Royal Society A*, vol. 379, iss. 2207, 2021, *https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2020.0360*

11 Damjanovic-Behrendt, V.; "A Digital Twin-Based Privacy Enhancement Mechanism for the Automotive Industry," Institute of Electrical and Electronics Engineers, *2018 International Conference on Intelligent Systems (IS)*, September 2018, p. 272–279, *https://ieeexplore.ieee.org/abstract/document/8710526/*

12 Automotive Industry Action Group, "IATF 16949:2016," *https://www.aiag.org/quality/iatf-16949-2016*

13 International Organization for Standardization (ISO), *ISO 9001:2015 Quality management systems—Requirements*, Switzerland, 2015, *https://www.iso.org/standard/62085.html*

14 International Organization for Standardization (ISO), *ISO 14001:2015 Environmental management systems—Requirements with guidance for use*, Switzerland, 2015, *https://www.iso.org/standard/60857.html*

15 International Organization for Standardization (ISO), *ISO 45000:2018 Occupational health and safety management systems—Requirements with guidance for use*, Switzerland, 2018, *https://www.iso.org/standard/63787.html*

16 Piromalis, D.; A. Kantaros; "Digital Twins in the Automotive Industry: The Road Toward Physical-Digital Convergence," *Applied System Innovation*, vol. 5, iss. 4, 2022, p. 65, *https://www.mdpi.com/2571-5577/5/4/65*

17 Fleisher, G.; "Four Technology Shaping the Future of Modular Construction," Modular Home Coach, 11 March 2022, *https://modularhomesource.com/four-technologies-shaping-the-future-of-modular-construction/*

18 Rais, A.; "Digital Twin in the Automobile Industry," Maschine Markt International, 8 January 2019, *https://www.maschinenmarkt.international/digital-twin-in-the-automobile-industry-a-851549/*

19 Tesla, "Software Updates," *https://www.tesla.com/support/software-updates*

20 Glocker, G.; "A Primer on Digital Twins in the IoT," Bosch Digital Blog, October 2018, *https://blog.bosch-si.com/bosch-iotsuite/a-primer-on-digital-twins-in-the-iot/*

21 Gehrmann, C.; M. Gunnarsson; "A Digital Twin Based Industrial Automation and Control System Security Architecture," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, 2020, p. 669–680, *https://ieeexplore.ieee.org/document/8822494*

22 Staff, "How Digital Twins Could Protect Manufacturers From Cyberattacks," *Homeland Security Today*, 3 March 2023, *https://www.hstoday.us/subject-matter-areas/cybersecurity/how-digital-twins-could-protect-manufacturers-from-cyberattacks/*

CROSSWORD PUZZLE

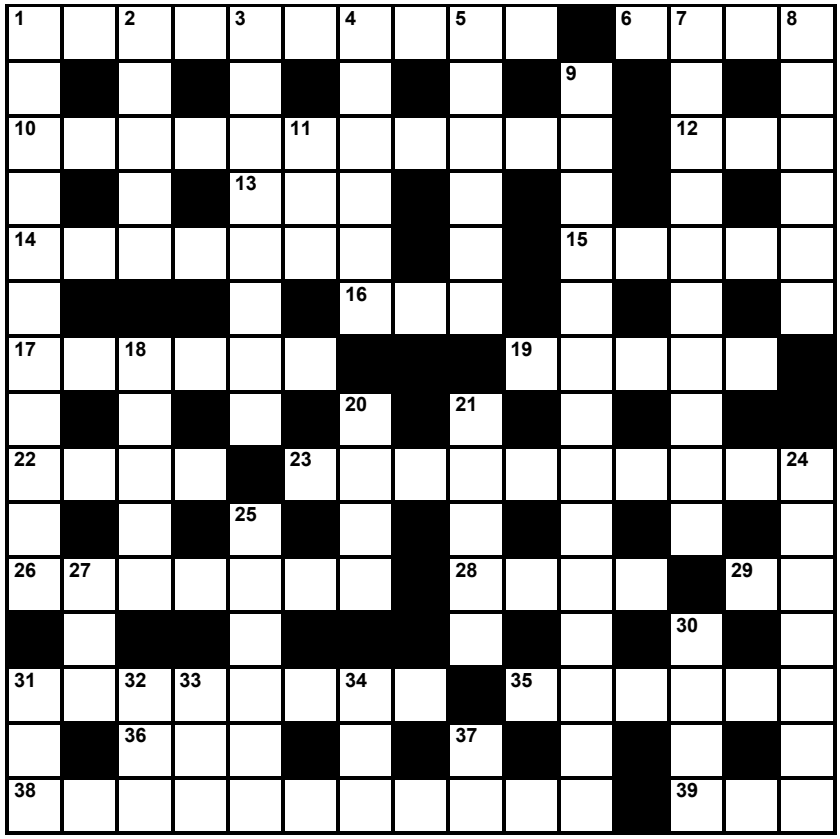
By Myles Mellor
www.themecrosswords.com

ACROSS

1. Responsible management
6. Work detail
10. One of the values of effective cybersecurity
12. Survey closely
13. Malign, slangily
14. Perform repeatedly
15. Incident, in technical language
16. Cry for help, abbr.
17. Agile
19. Not chronic
22. Benchmark
23. Devices used to store electrical energy
26. Added up
28. Popular EHR software-as-a-service provider
29. Prefix for sponsor and operate
31. Mechanisms used to manage a system and its security
35. Protect by creating a new iteration of data, 2 words
36. Life story, in brief
38. Vital to establish these for cybersecurity protection, 2 words
39. Agree silently

DOWN

1. Extremely difficult or involved problem, 2 words
2. Worth
3. Easy to understand
4. Turns up
5. Serious emergency
7. Action of keeping from happening
8. Make
9. They engage in hacking, phishing, etc.
11. Information unit
18. Relating to concepts of right and wrong
20. Receipt word



21. Expert
24. Prevented
25. Chips
27. A while ago
30. Biggest human organ
31. Accountant, abbr.
32. News channel, abbr.
33. Secure
34. Corporation type
37. Promotional material

Answers on page 59

Take the quiz online.

http://bit.ly/3qq0JjR

Based on Volume 2, 2023—Interruptions, Disruptions and Impact of Emergence
Value—1 Hour of CISA/CRISC/CISM/CGEIT/CDPSE Continuing Professional Education (CPE) Credit

TRUE/FALSE

Ross Article

1. Because the information security function is responsible for preventing cyberattacks, it follows that it has the necessary expertise to lead an organization's efforts to repair damage to systems and make the business cyberresilient after an attack has occurred.
2. In modern businesses and government agencies, information systems and telecommunications activities affect all other enterprise functions, and program management is necessary to achieve cyberresilience across the enterprise.

Pearce Article

3. Strong emergence anticipates expected emergence and is the only type of emergence that can predict total emergence in complex real-world systems.
4. At 127 terawatt hours annually, the energy consumption of the Bitcoin blockchain is an example of detrimental unexpected IT emergence.

Trautmann Article

5. Because the European Banking Authority requires that audit and access rights for competent authorities be included in outsourcing agreements for the purpose of supervising financial services institutions, cloud service providers must permit all requesting clients to conduct on-site audits or inspections.
6. In the financial sector, audit reports ensure the integrity, availability and confidentiality of data shared with outsourced service providers, simplifying the regulation of cryptoassets and negating the requirement for corresponding institutional controls.

Gassauer and Burch Article

7. If enacted, the European Commission's proposed regulations on the use of artificial intelligence (AI) technologies would prohibit machine learning algorithms deemed unacceptable risk, monitor and impose restrictions on those considered high risk, and set relatively few requirements for those classified as low risk.
8. Real-time biometric identification systems in public spaces constitute an unacceptable risk, according to the EU's classification system for AI, and would be prohibited under its proposed AI Act.

Sayana Article

9. The role of the IT auditor is evolving due to remote work and other disruptive technologies, and it is likely to be phased out over the next decade as pervasive new forces, unpredictable and abrupt changes, and lack of disaster preparation become dominant trends.
10. Recent research has demonstrated that quantum computing will be viable and feasible in the near future, significantly increasing the problem-solving capabilities of computers and boosting the power of existing encryption and cryptography tools.

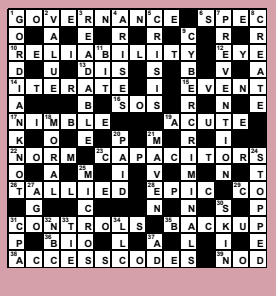
Butaka Article

11. The need for trust is a constant in real-world organizations, but trust is changeable, comprehensive and multidirectional in the digital realm, with applications to users' digital experiences and behaviors, as well as the overall digital environment and end-user attitudes.
12. Auditors can help strengthen an organization's digital trust through heavy reliance on new technologies such as robotic process automation, which increase an audit's efficiency and accuracy while preventing flawed human judgments from influencing the decision-making process.

Scott Article

13. Errors or omissions may occur in the design stage of the security development life cycle, but developers can typically resolve them at a minimal cost in later stages using robust threat modeling and risk analysis techniques.
14. Defensive programming techniques include testing field equipment input signals for out-of-range values, comparing control output signals for randomness and predictability, checking values for rounding errors, and identifying uncharacteristic messages from programmable logic controllers.

Answers: Crossword by Myles Mellor. See page 58 for the puzzle.



ADVERTISERS/WEBSITES

AuditBoard	*https://www.auditboard.com/product/compliance-control*	Back Cover

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 professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

ISSN 1944-1967

SUBSCRIPTION RATES

US: one year (6 issues) $85

All international orders: one year (6 issues) $100

Remittance must be made in US funds.

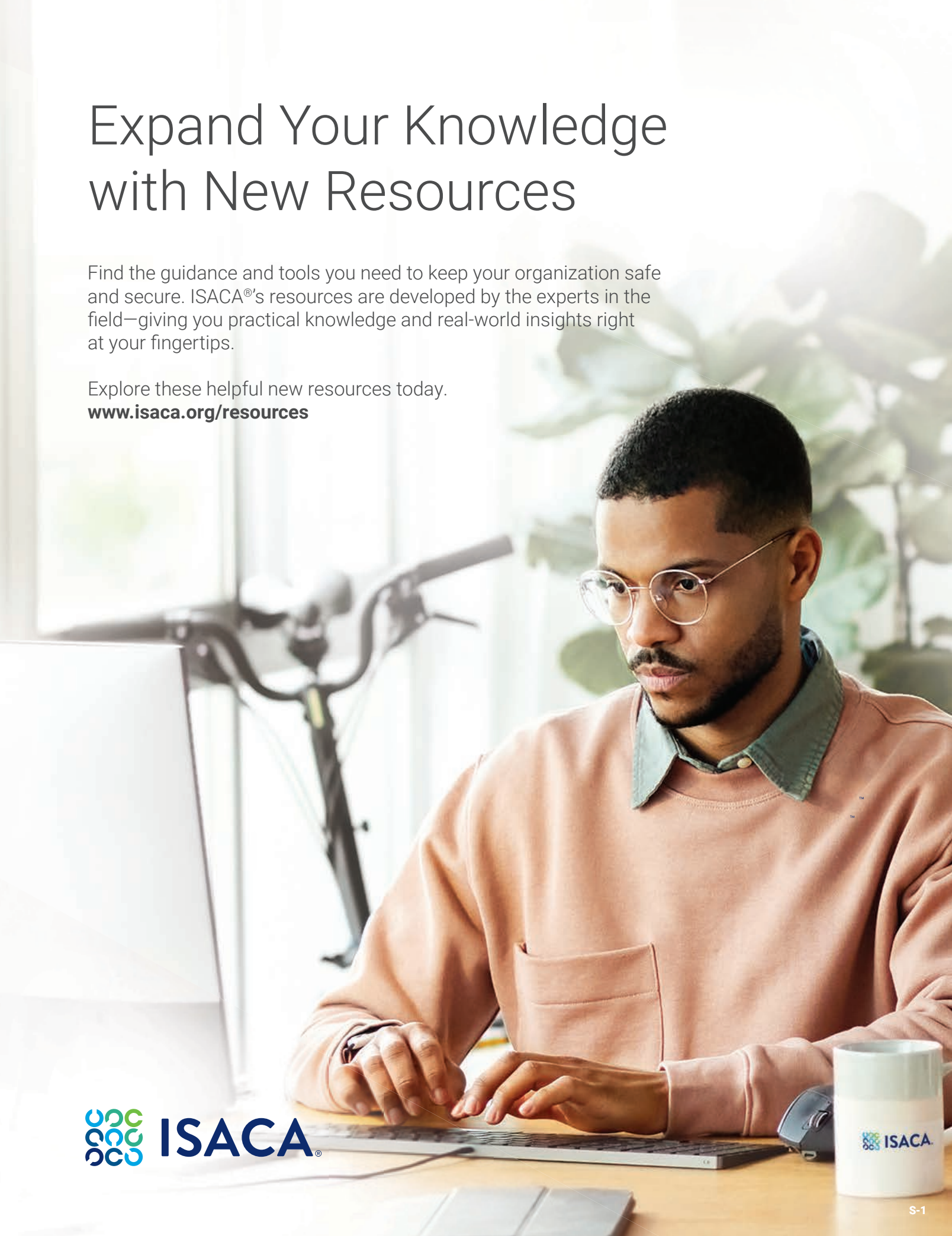
https://bit.ly/3w1MTnd

Leaders and Supporters

Expand Your Knowledge with New Resources

Find the guidance and tools you need to keep your organization safe and secure. ISACA®'s resources are developed by the experts in the field—giving you practical knowledge and real-world insights right at your fingertips.

Explore these helpful new resources today.
www.isaca.org/resources



ISACA®

FEATURED RESOUCES

Blueprint for Ransomware Defense

Free Digital Resource

As ransomware attacks continue to increase in frequency, complexity and damaging effects worldwide, cybercriminals have operationalized ransomware into a multibillion-dollar illegal enterprise with the capability to exploit and disrupt even the largest and most sophisticated companies. However, both the probability and severity of an attack can be mitigated when companies develop and maintain strategies for both prevention and mitigation. This white paper offers insight into the current ransomware landscape and outlines steps an organization can take to prepare for and respond to ransomware attacks.

Google Cloud Audit Program

Digital Resource – Member Free/Non-member $49

As many companies continue to undergo digital innovation and transformation, optimize global workforce access to productivity products, and shift business operation to hybrid, single cloud, or multi-cloud environments, it's important that auditors be prepared with a framework to understand and assess risk across various enterprise cloud technologies. ISACA has been an early leader in developing auditing templates for a number of widely used enterprise cloud services providers. With the continued growth and adoption of Google® Cloud Platform (GCP®), now representing the third largest provider of cloud services, ISACA has developed an audit program that helps auditors assess and test control coverage adequacy and effectiveness of GCP® services, adding to the library of frameworks that exist for the two other major cloud providers. ISACA created the Google® GCP® Audit Program to assist auditors in developing an audit plan that caters to the uniqueness GCP® while effectively assessing an enterprise cloud environment for adherence to organizational risk and compliance objectives.

Privacy Regulatory Lookup Tool

Free Digital Resource

Given the myriad privacy laws and regulations with which organizations must comply, many privacy professionals struggle to understand their compliance obligations. Comparing laws and regulations can enable an enterprise to more rapidly identify how to achieve compliance. To that end, ISACA's Privacy Regulatory Lookup Tool provides technical privacy practitioners with an easy way to compare privacy laws and regulations. This Microsoft Excel tool has mapped the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), Personal Information Protection and Electronic Documents Act (PIPEDA), Lei Geral de Proteção de Dados Pessoais (LGPD), Australian Privacy Principles (APPs), the Personal Data Protection Act (PDPA) and Personal Information Protection Law (PIPL) with a core set of principles developed by ISACA.

Order online at www.isaca.org/resources

CDPSE Official Review Manual, 2nd Edition

Available in Print and eBook – Member $109/Non-member $139

The CDPSE Review Manual 2nd Edition is a comprehensive reference guide designed to help individuals prepare for the CDPSE exam and understand technical privacy implementation and privacy principles. The manual represents the most current, comprehensive, peer-reviewed IT-related privacy review resource available.

The manual is organized to assist candidates in understanding essential concepts that can facilitate a common understanding of privacy best practices and ensure the proper integration of IT privacy solutions that mitigate risk while ensuring an optimal end-user experience. The exam and the manual are organized within three high-level domains:

- Privacy Governance
- Privacy Architecture
- Data Life Cycle

These domains are the result of extensive research and feedback from IT privacy subject matter experts from around the world. This manual, along with other training and review options, will help candidates prepare to take the CDPSE exam and provides a practical privacy desk reference for future use.

CDPSE Official Questions, Answers and Explanations Manual, 2nd Edition

Available in Print and eBook – Member $129/Non-member $159

The *CDPSE Official Questions, Answers & Explanations Manual, 2nd Edition* is designed to familiarize candidates with the question types and topics featured in the CDPSE exam.

The manual consists of 350 practice items covering the three domains (Privacy Governance, Privacy Architecture and Data Life Cycle) that are tested on the CDPSE exam.
These questions are not actual exam items but are intended to provide CDPSE candidates with an understanding of the type and structure of questions and content that has previously appeared on the exam.

This publication is ideal to use in conjunction with the *CDPSE Review Manual, 2nd Edition.*

CRISC Official Review Manual, 7th Edition Revised

Available in Print and eBook – Member $109/Non-member $139

Risk and compliance and how new technologies impact overall enterprise risk remains top of mind for boards and upper management. The IT community looks continually for training, credentials and resources in IT risk and compliance to keep themselves up to date and their organizations and/or clients compliant.

CRISC is the **only credential focused on enterprise IT risk management** and designed for IT and business professionals who have hands-on experience with risk identification, risk assessment, risk response and risk and IS control monitoring and reporting.

The *CRISC Review Manual 7th Edition Revised* is a comprehensive reference guide designed to help individuals prepare for the CRISC exam and understand IT-related business risk management roles and responsibilities. The 7th Edition Revised manual is organized to assist candidates in understanding essential concepts and studying the following job practice areas:

- Governance
- IT Risk Assessment
- Risk Response and Reporting
- Information Technology and Security

The *CRISC Review Manual 7th Edition Revised* offers an easy-to-navigate format. Each of the book's chapters has been divided into two sections for focused study. Section one of each chapter contains:

- Definitions and objectives for the four areas
- Task and knowledge statements
- Self-assessment questions, answers, and explanations
- Suggested resources for further study
- Section two of each chapter consists of reference material and content that support the knowledge statements. The material enhances CRISC candidates' knowledge and/or understanding when preparing for the CRISC certification exam. Also included are definitions of terms most found on the exam.

While this manual is an excellent stand-alone document for individual study and can be used as a guide or reference for study groups and chapters conducting local review courses. It can also be used in conjunction with the:

- CRISC Questions, Answers and Explanations Database
- CRISC Online Review Course

ISACA

EMPOWER YOUR TEAM. **POWER** YOUR BUSINESS.

If you want to be ready to take on the business challenges of tomorrow, you need to start with IT team training today. ISACA offers globally recognized programs that are personalized to fit your company's goals and needs. Not some one-size-fits-all, cookie-cutter training. But team training that lets them learn in person, online or by a virtually led instructor. The result? A stronger, satisfied team that will work more efficiently and effectively for you. Your future success begins now with ISACA.

To learn how ISACA can empower your team, visit us at www.isaca.org/enterprise.

Compliance Management, Unified.

Build trust and scale your compliance program with a connected risk platform that unifies SOC 2, ISO 2700x, NIST, CMMC, PCI DSS, and more across your organization.

Centralize Management

Seamlessly navigate today's complex risk environment with one integrated platform.

Increase Efficiency

Automate manual tasks, avoid duplicative assessments, and streamline reporting.

Empower Collaboration

Eliminate manual follow-ups with automated notifications and reminders.

AUDITBOARD

Learn more at **auditboard.com/product/compliance-control**

Top-Rated by Customers

Gartner peerinsights. ★★★★★

g2.com ★★★★½

Capterra ★★★★½