ISACA

Journal

VOLUME 5, 2023

THE OPERATIONS IMPERATIVE

FUTURE FITTING OPERATIONAL COMPLIANCE

IT RISK AND IT AUDIT WORKING TOGETHER: REDUCING THE BURDEN ON THE BUSINESS

A RISK-FIRST APPROACH TO SETTING AN INFORMATION SECURITY BUDGET

ISACA.ORG

Help a Colleague LEVEL UP Their Career

Technology professionals know an ISACA® certification can open doors, increase pay and help drive their careers to the next level. ISACA's Certification Referral Program rewards ISACA-certified professionals for referring colleagues to register for an ISACA certification exam. If you have an ISACA certification, you can earn up to US$500 in digital* rewards as a referrer, while the referee receives 10% off their exam.

Start earning today by visiting ISACA's Certification Referral Program at **www.isaca.org/cert-referral-jv5**

ISACA

*Digital payouts will be made by way of Tremendous.com

ISACA

COMMUNITY DAY

PEOPLE | SERVICE | PURPOSE

Join ISACA members and staff as we work to perform volunteer services to improve our communities. By giving back locally, we can have a huge impact globally!

The CommunITy Day 2023 details:

WHEN: 7 October 2023

WHERE: Your local community or ISACA Global

WHO: All ISACA members either through their local chapter or individually

HOW: Go to https://www.isaca.org/CommunITyDay-jv5 to sign up for virtual and in-person opportunities and to track your CommunITy Day activities and hours.

Plus, you can use **#ISACACommunITyDay** to follow, share and celebrate the real-time impact ISACA members are having around the world.

SIGN UP TODAY! Scan the QR code or go to https://www.isaca.org/CommunITyDay-jv5

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 September and October:

Forensic Investigations and Computer Forensics in the Age of Blockchain
ANUJ CHOUDHARY, CISA, CA, CFE

Improving Information Security Through Organizational Change
SCOTT ROSENMEIER, CISA, CRISC, CISM, CGEIT, CDPSE, CCSP, CIPP/E, CISSP-ISSAP, CISSP-ISSSMP

Reducing Barriers to Adoption of CCM Through Alarm Management
PETER BEST, KISHORE SINGH, PH.D., AND JOHN HALLIDAY

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/

Dear Readers

I joined ISACA® as chief executive officer (CEO) approximately four months ago. There has been much to absorb in that time, but what has stood out the most is this: The ISACA community is truly special. It is rare to find a group of people as connected, involved, passionate and dedicated as this one.

It has also been gratifying to see how much value our members find in ISACA. From a member who has found all of her jobs through her ISACA network to members whose credentials have helped them transform their careers, I have seen countless examples of how ISACA has been a valued career partner—and I am committed to continuing that important partnership.

ISACA was established in 1969, and the *ISACA® Journal* celebrated its 50th anniversary in 2022. There is much rich history in this organization—and there is also much to look forward to. This is a uniquely interesting time for ISACA professionals. Following the COVID-19 pandemic, organizations are grappling with remote, hybrid or in-person work and events, and the related technological challenges and solutions those decisions present. Artificial intelligence (AI), long talked about, has taken the world by storm this year with the rapid evolution of generative AI tools. Additionally, the tech workforce continues to be in high demand, even as the job market cools for many other professions.

Our job at ISACA, and in this *Journal*, is to prepare you for these challenges and opportunities, to help both you and your organization thrive, and to be a valuable learning and career resource for you, regardless of how regulations, technologies or workforce needs change.

These pages of the *ISACA Journal* will help you stay abreast of operational imperatives. You will learn about resilience, key collaborations and accountability—things that are important for all organizations, in every industry around the world.

These first months have been a truly rewarding experience as I get to know ISACA members and the headquarters team, and as I better understand the future operational imperatives for our organization. I look forward to getting to know all of you better and to delivering the information, resources and tools you need to help you succeed today and in the future.

Erik Prusch

Erik Prusch
ISACA CEO

ERIK PRUSCH

Is chief executive officer (CEO) of ISACA®. Prior to joining ISACA, he was CEO of Harland Clarke Holdings Corp., a provider of integrated payment solutions and integrated marketing services. He has also served as CEO of Outerwall, Lumension, NetMotion Wireless, Clearwire and Borland Software Corporation. Additionally, Prusch has served as a board member for RealNetworks, WASH, Calero Software and Keynote Systems. Previously in his career, he served as chief financial officer (CFO) for a number of public companies, including Identix and Borland, and for divisions of public companies, including Gateway Computers and PepsiCo. He began his career at Deloitte & Touche (then Touche Ross).

Organizing for Cyberresilience

A few issues back, I raised this question: Which function within a typical enterprise should be leading the development of resilience in the face of cyberattacks?[1] After some hemming and hawing about the definition of cyberresilience,[2] I suggested that functions including information security, business continuity management and business leadership might be candidates, each with potential advantages and drawbacks. I then wimped out and said that all these functions and more needed to be involved and that a program management office should take the lead.

All of which raises another question: How should businesses in both the private and public sectors organize to create resilience in the face of potentially successful cyberattacks? The key to answering this question is that cyberresilience is not anyone's job. It requires the involvement of nearly every function in the enterprise. The difficulty with this statement is that if everyone is involved, then a fairly rigorous organization of roles is necessary to keep everyone from tripping over everyone else.

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.

Managing Conflicting Interests

As a starting point, there is a need for a process for adjudicating conflicting interests in keeping an organization cyberresilient. For instance, the sales department might want systems to be brought back into use even if it is not proven that malware has been excised from them, while the information security function would be firmly opposed to such a move. Or human resources (HR) might emphasize retention of employees even if normal operations were impossible, but the chief financial officer (CFO) would prioritize cost reduction in a time of constrained cash flow. These are just examples of disputes I am aware of—there must be many others.

These clashing perspectives are not unique to the responses to cyberattacks. In these examples, sales did not understand operations, which could not figure out what finance was up to. And nobody understood what IT was doing. In many enterprises, the organizational response is to erect silos of data, systems, funding and personnel, regardless of senior management's expressed desire to break down the divisions between the divisions.

Collaboration in Crises

However, it has long been observed that in periods of crisis the barriers between functions disappear when they are facing common, potentially existential problems. Simply put, collaboration leads to sustainably higher performance in times of distress.[3] Teamwork, often honored more in the breach than the observance when things are going well, may become a reality when times are tough. And cyberattacks with widespread impact (i.e., destructive attacks) are extraordinarily tough for any enterprise to withstand. Sales cannot sell; operations cannot operate; accounting cannot account. The public sector is no different: The public interest cannot be served. The challenge is to create a structure for collaboration in advance of an attack so that if one should occur, the broadest overall interests will be supported.

Cyberattack Crisis Management Team

Unless decisions on responding to a cyberattack are to be referred to the chief executive officer (CEO), there must be some forum to deal with them. In

fact, there is a need for a committee to oversee both the development and execution of plans to keep an organization going should it be attacked. Many enterprises have such a committee in place to deal with crises in general,[4] which certainly would include the disruption caused by a cyberattack that downed IT systems. However, the nature of the disruption caused by a cyberattack calls for different skills and possibly for different participants in decision-making.

Because not all cyberattacks are the same, the cyberattack crisis management team (CCMT) must be flexible enough to plan for the right managers to deal with each eventuality. Disclosure of employees' personal information, for example, requires involvement by HR, privacy, legal and labor relations. Sales and operations might not have much to say. An attack on a key IT servicer—say, payroll processing—would affect everyone, though HR would necessarily take the lead with nearly all other functions responsible for managing the impact on their own personnel. A ransomware attack that incapacitated multiple functions would require all executives to determine how to weather the outage until systems and data could be restored. And, of course, whatever sort of cyberattack can be envisioned, the IT function will have a major role to play.

If an enterprise intends to make itself as cyberresilient as possible, it must confront potential attack scenarios before they occur. The CCMT might conduct formal exercises such as simulations or table-top tests. Or it might simply meet periodically to talk through the identified threats and the actions it would take if the organization were to experience a cyberattack. Of course, these preparatory measures have been—or should have been—undertaken for many years as a part of a business continuity management program and, indeed, a disruption or system outage caused by a malicious actor should be no different.

Cyberattacks and "Routine" IT Disasters

Except it is different. Many enterprises have long been prepared for outages due to weather-related events, the interruption of key utilities, fires, earthquakes and other disasters beyond management's control. The COVID-19 pandemic showed that many were able to withstand absenteeism and the inability to use business premises. But none of these negative events entailed planned, organized, targeted and malicious attacks by outside human forces on the nerve center of an enterprise. Complicating matters, an antagonist might well be a government—or a criminal gang supported (or intentionally overlooked) by a government. Most of today's managers were educated in an earlier era. Dealing with criminal attacks was not a subject when they went to business school.[5]

The nature of the disruption caused by a cyberattack calls for different skills and possibly for different participants in decision-making.

Management has had to deal with crises caused by information system outages for quite some time. But those events, as painful as they have been, were generally shorter, more easily solved and less pervasive. Plans for recovery from "routine" disasters have evolved to the point that in many organizations that I am aware of, all systems can be recovered well within the organization's tolerance for downtime. Not so with recovery from cyberattacks.[6] They take longer, call for more resources, and are more difficult to bring to a conclusive finish.

Organizing for Prior Planning

Convening the CCMT prior to an actual attack forces conflicting concerns into the open and may lead to resolution prior to the timing of need. Moreover, working through cyber-related problems in advance can identify areas of common rather than conflicting interests (some of which may be taken advantage of right away). And it helps to identify the specific responsibilities that each function must address in an attack to minimize unnecessarily overlapping efforts.

Apart from preventing cyberattacks in the first place, IT must prepare to recover systems and data from backups as rapidly as possible. Finance must plan for continued availability of cash. HR must determine how and whether to pay idled workers. Operations needs to work with vendors to ensure delivery of supplies and raw materials. Sales needs to work with customers to determine ways to keep products flowing. And some functions may just have to plan to work as best they can with whatever support they can get.

As long as all these functions organize themselves to prepare together, they are far more likely to work together should their systems be taken from them.

LOOKING FOR MORE?

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

Convening the CCMT prior to an actual attack forces conflicting concerns into the open and may lead to resolution prior to the timing of need.

Even more so, they are likely to manage the enterprise in a collaborative manner if they implement the organizational structures needed to survive an attack before one occurs.

Endnotes

1 Ross, S.; "Who Leads Cyberresilience?" *ISACA® Journal*, vol. 2, 2023, *https://www.isaca.org/archives*

2 *Ibid*. For reference purposes, I said that "Cyberresilience is the demonstrated ability to continue operations at an acceptable level despite any type of potential business disruption due to a cyberattack."

3 Gardner, H. K.; I. Matviak; "Seven Strategies for Promoting Collaboration in a Crisis," *Harvard Business Review*, 8 July 2020, *https://hbr.org/2020/07/7-strategies-for-promoting-collaboration-in-a-crisis*

4 This committee is often referred to as a crisis management team (CMT). There are many sources concerning the roles and responsibilities of a CMT. See, for example, Posey, B.; "Roles and Responsibilities of a Crisis Management Team," *TechTarget Disaster Recovery*, 7 April 2020, *https://www.techtarget.com/searchdisasterrecovery/tip/Roles-and-responsibilities-of-a-crisis-management-team*. This committee might also take responsibility for cyberresilience, although its membership might need to be different from one that deals with physical disasters or financial crises. For ease of discussion, let us call it the cyberattack crisis management team (CCMT) to keep the focus on this particular form of crisis.

5 But it is today. A recent survey found 23 business schools offering Master of Business Administration (MBA) or other degrees in cybersecurity in the United States alone. *Cybersecurity Guide*, "Guide to an MBA in Cybersecurity," 7 June 2023, *https://cybersecurityguide.org/programs/cybersecurity-mba/*

6 IBM, Ponemon Institute, *Cost of a Data Breach Report 2022*, USA, 2022, *www.ibm.com/downloads/cas/3R8N1DZJ*. The most recent IBM/Ponemon Institute annual study of data breach costs states that the average time to contain the impact of a cyberattack, *once the attack has been discovered*, is 74 days.

Outsourcing vs. In-House: Getting the Most Out of the Business Case and RFP

Short on staff, in need of an objective opinion, lacking subject matter expertise—there are myriad reasons to consider outsourcing. It is a critical decision that impacts small and large enterprises, and there is always a mix of opinions on whether the right decision was made. So, when do you buy? When do you build the product or provide your own services? If you buy, can you validate the work with the same degree of scrutiny you would apply to your own resource and your own intellectual capital? Ultimately, how do you find a trusted vendor and build the monitoring steps that will ensure a successful project?

It is often said that building the business case is the first step to evaluating a project and answering the buy vs. build question. One must determine the project objective and provide enough detail on the expected outcome to ensure that business partners will be satisfied with the end product and accepting of the final cost. Building a skeleton of features and functionality with concrete vendor project team deliverables is typically done after approval of a standard business case, but doing so as the business case is created gives stakeholders and the potential internal project team a chance to determine whether there is enough bandwidth to get the work done in the time frame required. Fleshing out the outsourcing engagement at this stage also allows internal research to be done. Is this scope of work potentially applicable to other departments? If so, do they have work underway or under consideration for a similar project? Is it possible that there is something already created internally and available for immediate use or retrofitting? Consider this scenario:

Dan was relatively new to the CommBank data analytics team. He had been hired as the new director. He had several ideas in mind for CommBank and had made the rounds asking his fellow managers about their areas and building rapport with them. Dan was on the brink of finalizing a business case for development funding when he ran into a friend in the company cafeteria. He casually mentioned his new department's work and was surprised to discover that his friend's new work group was undertaking a very similar initiative. Instead of finishing the business case, Dan decided a few meetings with his friend's department, which turned out to be in the same division, was the best next step.

Vetting the Decision to Go Outside or Stay In-House

Once a review of the project is completed and translated into a business case that has enough detail to rule out duplicate efforts and provide reasonable assurance of user satisfaction, the buy vs. build in-house decision needs consideration. Several questions should be kept in mind:

- If you decide to buy due to aggressive time frames that cannot be accommodated internally, is the contracting and ramp-up learning time for a vendor taken into account in meeting the time frame expectations?
- If you seek subject matter expertise that is outside your organization's core competency, are you prepared to familiarize the outsourced party with internal requirements, cultural norms and user expectations? Have you considered the time and resources that vendor orientation will take?

CINDY BAXTER | CISA, ITIL FOUNDATION

Is executive assistant to the Massport Community Advisory Committee (MCAC). Baxter is pleased that technology has allowed her to reinvent her career and continue learning through all of it. She had the privilege of learning technology and managing Fortune 100 client relationships at AT&T. Baxter then applied her expertise as an IT operations director at Johnson & Johnson before moving to compliance and risk management roles at AIG and State Street Corporation. After a brief period of running her own consulting business, Baxter joined MCAC, which advocates on behalf of communities impacted by the US State of Massachusetts Port Authority aviation and port operations. She applies her expertise to website redesign, drafting vendor requests for proposals (RFPs), updating bylaws and providing regulatory support to the MCAC board. In her spare time, Baxter serves as compliance and operations officer for the ISACA® New England Chapter (Maine, Massachusetts, New Hampshire and Vermont, USA) and volunteers on the Nantucket Lightship.

- If your staff is already overwhelmed with work, are there resources available to coach and monitor the vendor's work, including management of any enterprise compliance requirements that supplement industry standard requirements?
- Has a financial analysis been conducted that includes not only the expected cost elements that will be provided by the vendor, but the internal project costs associated with managing the vendor?
- Have risk considerations been considered, specifically the risk to reputation if the outcome does not meet expectations, the financial risk for potential cost overruns, the operational risk of continued manual operations due to project delays, and the potential security risk of having an outsider either host a project or provide an externally accessible service?

There are several factors to consider when contemplating a vendor engagement, but there are just as many factors to consider with in-house project development and management. Comparisons between vendor attributes and in-house expertise need to include these elements:

- Determination of whether there is sufficient staff for completing the project compared to managing a vendor
- Investigation of how in-house expertise can be supplemented with resources such as interns and creative ways to temporarily supplement the work
- Consideration of potentially lower risk of using outside resources compared to employees

Writing the RFP

There are numerous tales to tell regarding vendor projects that have gone wrong. Buying services, similar to hiring new employees, is a commitment to having clear work objectives and a clear job description focused on the expected scope. Up front evaluation of needs and a thorough business case are an important foundation for building a solid request for proposal (RFP). Large organizations may have a dedicated department that handles RFP creation, while small organizations may distribute a basic quote request or hire a vendor solely based on feedback received from other organizations without using an RFP. All scopes of work, however, benefit from a formal request to vendors, which serves both candidates for the statement of work (SOW) and the organization requesting the work by providing specificity regarding the project and clarity regarding how performance will be judged. A team or person writing the RFP needs to consider not only the business case that has been prepared beforehand, but also legal and business operations criteria. The RFP starts with a solid understanding of the expected outcome from the stakeholders' and users' perspectives. Although the outcome must be clear, how the vendor gets to the end result should be left open to allow for creative solutions by vendor candidates.

Buying services, similar to hiring new employees, is a commitment to having clear work objectives and a clear job description focused on the expected scope.

The RFP is also an appropriate vehicle for outlining service level agreements (SLAs) that will form part of the contract once a final candidate is selected. The SLAs need to offer a guarantee of outcome or ongoing service commitment. They also need to be measurable and add value to the users' experience. It is worth examining each of the three elements:

1. **Guaranteed outcome.** Both the vendor candidate pool and the buying organization must be clear on the expected outcome. There are two points where one must level set. First, the service/product provided needs to have realistic parameters. There are times when buyers push potential suppliers into accepting criteria that cannot be met. Second, if there are doubts when vendor-experts indicate limitations, it behooves the buyer to do additional research and compare

LOOKING FOR MORE?

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

responses for similar criteria abilities. An RFP and contract should not be an opportunity to push a vendor toward the unachievable.

2. **Added value.** SLAs need to be determined based on the functional specifications (specs) that add value for the users. Functional specs translated into SLAs may fall into categories of improved productivity or increased market share or a broader product set. Meaningful SLAs are those that resonate with those buying and using the services. Meaningful SLAs must also be straightforward enough for those monitoring the vendor's performance to make accurate assessments of status.
3. **Key metrics.** SLAs are the control points of a vendor agreement and, as such, must be measurable. It is not enough to establish the metrics without communicating the steps to be tested or the formulas for evaluation. Like any control point, SLA metrics must be understood and agreed upon between the parties. They must not only be clear, but also be legally binding with consequences that will promote remediation. Setting expectations is important and stating them in writing is essential, including these important elements:
   - SLAs must be outlined in the RFP. It is the place to ensure that the best vendor is selected and that there are no major issues when it is time to contract services.
   - SLAs in the contract must specify the outcome, the expected value to users, and the metrics/performance testing that will be used. Negotiation regarding SLAs during the contract phase is common, but changes should be minor if the RFP is sufficiently detailed to set criteria and expectations for monitoring performance.
   - Metrics should be clearly established and flexible enough to modify upon mutual agreement as the product/service matures. There should be agreement regarding which party will supply the metrics and agreement on any cross-verification. Metrics are most effective when both parties participate in collecting them and when results are shared on a timely basis.

The RFP is also an appropriate vehicle for outlining service level agreements (SLAs) that will form part of the contract once a final candidate is selected.

Conclusion

Success is good for everyone and is a joint effort that starts with understanding the need, doing sufficient research, and participating in a transparent way with stakeholders and vendor candidates alike. Once a vendor is selected, the vendor/buyer relationship is an important one to work on together for mutual growth and benefit. When viewed as a lasting relationship that will have bumps along the way, it results in the best work from all involved.

Digital Trust and an Eye on Reliable Operations

Operations are a core part of the Digital Trust Ecosystem Framework (DTEF).[1] The *Enabling and Support* domain has elements around process and technology. The *Direct and Monitor* domain includes governance, sustainability and resilience. Part of any organization's reputation, which effects others' trust in said organization, is the ability to deliver services consistently at an acceptable performance level.

The reality is that customers and partners care when operations are down. Organizations do not get a pass because an outage happens digitally instead of in the physical world. It is useful to look at several examples of how operational failures impact trust from the physical world, then delve into the digital world with several more examples.

The Telephone: Landline vs. Cellular

I grew up in the era before the cellphone and our expectation was when we picked up the handset on a physical landline, it just worked. Outside of a disaster or some unexpected incident such as a truck knocking down a telephone pole, we were caught by surprise when we picked up the phone and did not get a dial tone.

Outside of an unexpected event, when we received a fast busy signal because either the local exchange or the one where we were calling (e.g., for a long distance call) was overloaded, most telephone corporations (telcos) knew that as customers, we would not tolerate that situation for very long and capacity was something that was quickly addressed.

That same expectation initially carried over to cellular phones. However, users learned quickly that coverage was not equal across providers or consistent across locations in a particular metropolitan area. For instance, on a recent forum, I saw a post from a military member who was moving to a new location and asked what provider was best there.

With that said, if we start to experience operational issues outside of coverage and dead zones, as with the physical landline, we start to lose trust in the cellular carrier. A consumer who has a bad experience in a cellular providers brick-and-mortar store may be inclined to change providers, no longer trusting the carrier to deliver a reasonable experience. This is why both cellular service and purchase experience are considered.[2] This certainly happens in the corporate world. If a cellular provider does not measure up, when the contract comes due, the organization will likely make a change.

A Hard Freeze and the Loss in Confidence

The US State of Texas, and especially the city of Houston, has had its fair share of hardships during the last decade, but the most surprising was the deep freeze Texas experienced in February 2021. The power grid for most of the state was ill-prepared to handle extreme cold temperatures, and for that, the Electric Reliability Council of Texas (ERCOT) took the brunt of the blame. Many Texas residents were left without power with temperatures below freezing. A large percentage were also without running water. And, in some of the most vulnerable areas of Houston, food was scarce as well since those communities are considered food deserts. Without operating infrastructure, it was nearly impossible to get needed food supplies.[3] After such a catastrophic event, it was unsurprising that many

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.

Texas residents lost confidence in the ERCOT and the state as a whole to provide proper utilities in the event of another deep freeze. However, the power company has an edge in these situations because of its monopoly status. Consider if consumers had another reasonable option. Would they have stayed with ERCOT? Likely not.

On the other hand, this crisis did boost the profile and trust of a particular product, the Ford F-150 hybrid truck with electrical generator. Some truck owners were using the vehicle to provide electricity to their homes. When the reports went viral, Ford asked its dealers in the affected areas to loan the trucks with onboard generators where needed.[4] Ford, and the F-150 Hybrid with generator, in particular, received a great deal of positive media attention as the reports went viral.

Distrust with one area of a government can lead to distrust with every area of that government.

From Physical to Digital

It is often easier to better understand trust when considering physical world situations, because it is more tangible and is often what we first experience. However, there are operational concerns in the digital realm that greatly affect trust as well. One common example is the biggest shopping day of the year in the United States: Black Friday.

Black Friday Issues

"Black Friday" is the common term for the Friday after the US Thanksgiving holiday. Traditionally, it is the start of the holiday shopping season in the United States. Many brick-and-mortar retailers offer highly publicized sales with deeply discounted prices and open early, sometimes as early as midnight, to generate shopping excitement. Black Friday 2022 saw a data quality issue arise with Amazon ad reporting, meaning advertisers were getting bad data from Black Friday afternoon to sometime on Sunday.[5] The ad expenditures were significantly less than what advertisers expected, yet the ads were still successfully running. This meant that advertisers had no accurate information on how much money

they were spending. Their only means of gathering data was the system Amazon provided, and it was providing data that could not be trusted. It is not difficult to understand why advertisers lost some trust in Amazon's ability to deliver.

Of course, operational issues on the biggest US shopping day of the year can have a significant financial impact on the organization due to creating a trust issue. Costco opened sales on Thanksgiving Day but had a lengthy site outage, which was estimated to have cost the company nearly US$11 million.[6] While Costco extended its promotional sales into Friday due to the outage, there were likely some consumers who did not give the retailer a second chance, meaning lost sales. While others may have stepped in to seize the opportunity, a dissatisfied customer can have a significant impact on an organization's perception, hurting its relationships all around. *Inc*. compiled statistics from various studies that indicate a dissatisfied customer is 91 percent likely to be a permanently lost customer and will also tell nine–15 people about the poor experience leading up to it.[7]

Ransomware and Government

While I have focused primarily on retail, the DTEF is applicable to any organization that is active in the digital world. This includes governments. A government entity has similar relationships with customers and partners as with retail organizations, but the nature of those relationships is different. There are different trust factors involved when it comes to government organizations. A consumer can choose to go to another retailer, but unless one moves, one must interact with the government where one lives. So, if a city government's services and capabilities suddenly go down due to a ransomware attack, where do you go to pay your water bill?[8]

As with the Texas deep freeze, the uncertainty of when services will be restored can lead to a growing distrust in the government entity, be it municipal, regional or national. Distrust with one area of a government can lead to distrust with every area of that government. While a government is not going to have statistics such as lost revenue, this lack of trust can manifest as lack of engagement and lack of cooperation or in people leaving the area altogether. Ransomware is possibly the worst digital issue that a government may have to deal with—for example, when the US city of Dallas, Texas, was hit with a ransomware attack and many municipal services experienced serious disruptions or went down altogether.[9]

The worst thing the city could have done was to implement what was effectively a black out policy, which was what the city chose to do. By providing estimates, even if those estimates had to be updated to reflect new information, the city could have done a better job of maintaining its public trust with constituents. That lack of transparency exacerbated the trust issues cause by the operational outage with residents stating that they did not know "what's going on with the city."[10]

Neglect Operations at Your Own Peril

A failure in operations can lead to a loss of trust in relationships for any enterprise. This is true both with physical and digital interactions. Part of what determines an organization's digital trust in a digital world is its reliability. Issues with reliability will cause customers who have relationships with the organization to look elsewhere. This is why the DTEF has trust factors focused on operational capacity, monitoring, reliability and sustainability. Keep in mind that when we talk about an operational failure, a physical failure can impact an enterprise digitally, especially in the retail sector. For instance, if an organization cannot ship the orders it has accepted, that is going to affect customer confidence in the organization. The reality is that any operational issue can affect an organization's digital trustworthiness. Therefore, the warnings in the physical world apply to the digital one as well: neglect operations at your own peril.

LOOKING FOR MORE?

- Read *Digital Trust: A Modern Day Imperative. www.isaca.org/digital-trust-modern-day-imperative*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

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 Cox, D.; "Report: The Best Cellphone Providers in America," Clark.com. 15 June 2023, *https://clark.com/cell-phones/best-cell-phone-providers/*

3 Stewart, S.; "Remembering Houston's Deep Freeze of 2021," *Houstonia*, 21 December 2022. *https://www.houstoniamag.com/news-and-city-life/houston-storm-uri-deep-freeze-february-2021*

4 Gorgan, E.; "2021 Ford F-150 PowerBoost Is a Life Saver in Texas Freeze, Powers Up Appliances," AutoEvolution, 19 February 2021. *https://www.autoevolution.com/news/2021-ford-f-150-powerboost-is-a-life-saver-in-texas-freeze-powers-up-appliances-156390.html*

5 Goldman, J.; "Amazon Ads' Reporting Mishap on Black Friday Gives Retail Media a (Temporary) Black Eye," Insider Intelligence, 29 November 2022, *https://www.insiderintelligence.com/content/amazon-ads-reporting-mishap-on-black-friday-gives-retail-media-temporary-black-eye*

6 Goldman, M. C.; "Costco's Thanksgiving Day Website Crash Cost It Nearly $11M," TheStreet, 30 November 2019, *https://www.thestreet.com/technology/costco-thanksgiving-day-website-crash-cost-it-nearly-11million-15185344*

7 Thomas, A.; "The Secret Ratio That Proves Why Customer Reviews Are So Important," *Inc.*, 26 February 2018, *https://www.inc.com/andrew-thomas/the-hidden-ratio-that-could-make-or-break-your-company.html*

8 Brumfield, C.; "Ransomware Attacks Pose Communications Dilemmas for Local Governments," *CSO*, 21 June 2023, *https://www.csoonline.com/article/3700488/ransomware-attacks-pose-communications-dilemmas-for-local-governments.html*

9 *Ibid.*

10 *Ibid.*

Digital Trust and Adopting Generative AI

As a reader of the *ISACA® Journal*, you might have naturally noticed some cognitive dissonance happening—at least in one very specific area. What I mean is, on one hand, generative artificial intelligence (AI) is everywhere in the mainstream media and seemingly on everyone's lips. Tools such as OpenAI's ChatGPT, Google's Bard, GitHub's Copilot and others are everywhere. They have been covered extensively in the news and media, they have had a tremendous impact on sectors such as education (e.g., as students find new use cases for how AI can help them with their work), publication (e.g., as publications and authors use them to generate content), marketing and numerous other areas. Yet, professional guidance for practitioners—particularly trust practitioners—has not been abundant in the trade media.

It seems as though there is a veritable seismic shift happening on the technology landscape, yet many of us in the trenches are left wondering how to address it—and there seems to be relatively little guidance available to help us. Why is that?

There are two things happening, I think. One is that questions about risk often take more work to answer than questions about usage—in other words, it is easier to understand how to use something than it is to evaluate how risky it is to use. For example, compare what you need to know to answer the question, "How do I drive this car?" vs. what you need to know to answer the question, "Is this car safe to operate?" For usage, there is a set of critical information items: the rules of the road, how to operate the specific vehicle's controls, etc. For risk, however, you need to know the answers to most (if not all) of the usage-related questions plus many other things, such as road conditions (and by extension the planned driving route); the vehicle maintenance history; the weather forecast; and the condition of the vehicle's safety features, such as brakes, seatbelts and airbags. This is to name just a few.

Given this, I think it is natural that we would see usage emerge before any detailed analysis of risk—and ways to address those risk areas—becomes well known. Anyone who remembers the rise of virtualization, mobile, cloud or even (to go very far back in history) desktop computing can recognize the pattern where usage is already well under way before the full risk picture is known.

The second thing happening is that generally accepted safe practices for usage of these tools is taking time to emerge. If you are in the business of *building* these tools, there is some very exciting work happening. For example, the Open Worldwide Application Security Project (OWASP) is working on a Large Language Model (LLM) Top 10,[1] the US National Institute of Standards and Technology (NIST) has draft guidance out (NIST AI 100-2e2023),[2]

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.

In just the past year or so, we have seen integration of AI functionality into search engines; business applications such as sales tools, collaboration, and messaging platforms; and numerous other places.

and the UK National Cyber Security Centre (NCSC) has authored a set of principles about securing AI.[3] The point is, if you are a developer or integrator of AI (particularly LLMs) there are multiple sets of robust (though nascent) standards and guidance out there. But what if you are not? What if you are just someone who wants to make sure their organization is protected when business units, individual teams, or users themselves use these tools in novel and unexpected ways? There is quite a bit less to go on here—less advice from peers, less guidance from authorities, and so forth.

It is worth exploring some things that practitioners might keep in mind as they evaluate where they adopt, how they might already be using these tools without the knowledge of trust practitioners, and what options they might consider in response. This discussion does not go into the nitty gritty of how AI generally and LLMs specifically are developed or how they operate. Interesting though these details are, they can be a bit of a distraction from the impacts to an organization's digital trust. Instead, this discussion focuses on the emerging areas where the presence of these tools impacts an organization's digital trust posture and offers some suggestions for what might be done in response.

Risk Considerations

A few quick caveats:

- The focus here is on LLM generative chatbot-style applications (compared to, for example, image generation).
- What is covered is not intended to be exhaustive. This is not intended to be a full and complete list of every possible thing that you would need to consider in your organization or every potential risk area.
- Although there are organization-specific factors such as business context, regulatory considerations, risk tolerance and numerous other factors that play a role in what does or does not pose risk to an organization, as with any set of potential risk areas, only some are probable. There are any number of less probable situations that could arise in a particular situation.
- Addressed here are only those areas that are likely to occur, that impact a large segment of organizations (i.e., that are close to being universally applicable), and that impact digital trust.
- Discretion and good sense must be used in evaluating what may or may not apply to an organization and which areas of risk apply to that organization based on context and unique organizational factors.
- Remember that this discussion is only looking at the usage side of the equation (i.e., by end users). If an organization is a developer of an AI-based tool, an integrator of those tools, or otherwise making use of AI, there are, of course, numerous factors to consider beyond what is provided here.

Caveats out of the way, there are several potential risk areas that are worthy of consideration.

Exposure of Intellectual Property

Perhaps the biggest elephant in the room and the issue that many are most concerned about is exposure of sensitive data. This can and does happen. Samsung, for example, recently banned the use of AI chatbots due to the exposure of proprietary intellectual property by engineers and staff using these tools.[4] On multiple occasions, employees shared source code for error checking or code optimization purposes, and in another instance, an employee shared the details of a meeting to help with creation of a presentation.[5] Because the tool in question uses submissions from users to help train the model further, this means that intellectual property becomes available beyond the business need to know. It is unknown how extensive this problem is; however, some data, such as research from the vendor community, suggest that the sharing of confidential intellectual property might have already been done by more than 4 percent of the workforce.[6]

Shadow Adoption

On the surface, a complete ban might seem like a viable option given the size of this trend (imagine, for example, the chaos that would ensue if more than 4 percent of users put sensitive information at risk

via some other method, such as installing malware). It is made more challenging in practice, though, as a result of the second consideration: the adoption dynamics—specifically, the potential for shadow adoption. Not only are there multiple services and tools that users might wish to utilize in support of their daily work (a situation that always tends to compound shadow usage), but there is also a rapid-fire series of integrations underway. In just the past year or so, we have seen integration of AI functionality into search engines; business applications such as sales tools, collaboration, and messaging platforms; and numerous other places. This means that trying to technically enforce usage restrictions can be hard to do (especially when a service you already use opens up chatbot access via an integration on its side). And reliably detecting when and if data or information is exposed is likewise difficult for the same reasons.

Because LLMs provide the text that is statistically most likely to occur in any given circumstance with no awareness of how valid that text might be, it is sometimes blatantly erroneous with very little to indicate that this is the case.

Reliability and Provenance

The last consideration to be cited here relates to the reliability and provenance of the information obtained. It is concerning that users often place higher confidence in the reliability of the responses they get from these tools. Called "hallucinations," LLMs often provide inaccurate information or completely nonexistent "facts." Because LLMs provide the text that is statistically most likely to occur in any given circumstance with no awareness of how valid that text might be, it is sometimes blatantly erroneous with very little to indicate that this is the case. Many might be familiar with the reporting around attorney Steven A. Schwartz, who used ChatGPT to help prepare an official legal document. The LLM cited precedents that were entirely fabricated as "hallucinated" by the model. The judge in the case said, "six of the submitted cases appear to be bogus judicial decisions with bogus quotes and bogus internal citations."

Putting accuracy aside, though, provenance is also potentially at issue. Because the model consumes human-produced content exemplars and uses that as the basis for its responses, the ideas and concepts it relays (definitionally) were originated by others. Those ideas and concepts are then provided to users without attribution. If that sounds close to the plagiarism line to you, you are not alone in thinking so. OpenAI, the maker of ChatGPT, is already being sued[7] related to its use of data (per the lawsuit, using "stolen private information") in the training of the model.

Addressing these Concerns

All of these areas are certainly ones about which practitioners tasked with ensuring digital trust in our organizations might be concerned. However, controls in this arena are still emerging, and generally accepted standards around how to minimize risk while still ensuring that users get value from these tools (and remain competitive) are also not yet fully baked. So what then can we do?

One option is, like Samsung, to limit usage until the impacts can be better and more thoroughly understood. However, for reasons described herein, this can be technically challenging to enact given the rush to integrate LLM functionality into existing tools (even search engines and the like), the hype in the marketplace about their utility (and, thereby, the increased desire on the part of users to make use of them), and the number of different choices and offerings that users can select from (with new ones being introduced every day).

Because it can be challenging to directly restrict access for users (not to mention that these tools can be valuable in the workplace when used with discretion), one might consider alternative approaches. For example, one might consider awareness training designed to highlight to users the potential privacy, security, assurance and other digital trust impacts associated with these tools along with guidance about how they can be safely used. For example, one might consider training users on not sending sensitive, regulated or other critical information to these services. Users might be instructed on the limitations of these tools, such as AI "hallucinations" (misinformation) and other limitations

LOOKING FOR MORE?

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

on what the tools can deliver. Users might be counseled on the need to verify LLM output to ensure that output from these tools is not someone else's work being repurposed in a nonattributed way.

It also goes without saying that it can be advantageous to know where these tools are being used and for what use cases to understand the surface area of potential exposure. Organizations might, for example, maintain a record of usage when conducting activities such as business impact analysis (BIA), when performing assessments and/or audits of specific business areas and so on. Technical monitoring tools might be leveraged if organizations have them (e.g., HTTP forward proxy logs, network traffic logs, shadow IT monitoring tools) to look for areas of usage and enable follow-up.

LLMs and other AI tools have tremendous promise and potential. But like any new thing, care and forethought are required to ensure that organizations optimize risk while maximizing value.

Endnotes

1 The Open Worldwide Application Security Project (OWASP), OWASP Top 10 for Large Language Model Applications, USA, *https://owasp.org/www-project-top-10-for-large-language-model-applications/*

2 Oprea, A.; A. Vassilev; *Adversarial Machine Learning*, National Institute of Standards and Technology, USA, 2023, *https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.ipd.pdf*

3 National Cyber Security Centre, *Principles for the Security of Machine Learning*, United Kingdom, 2022, *https://www.ncsc.gov.uk/collection/machine-learning*

4 Mauran, C.; "Whoops, Samsung Workers Accidentally Leaked Trade Secrets Via ChatGPT," Mashable, 6 April 2023, *https://mashable.com/article/samsung-chatgpt-leak-details*

5 Staff, "Concerns Turned Into Reality... As Soon as Samsung Electronics Unlocks ChatGPT, 'Misuse' Continues," *The Economist* (Korea), 30 March 2023, *https://economist.co.kr/article/view/ecn202303300057?s=31*

6 Lemos, R.; "Employees Are Feeding Sensitive Biz Data to ChatGPT, Raising Security Fears," *Dark Reading*, 7 March 2023, *https://www.darkreading.com/risk/employees-feeding-sensitive-business-data-chatgpt-raising-security-fears*

7 Cerullo, M.; "ChatGPT Maker OpenAI Sued for Allegedly Using 'Stolen Private Information,'" CBS News, 30 June 2023, *https://www.cbsnews.com/news/chatgpt-open-ai-lawuit-stolen-private-information/*

Future Fitting Operational Compliance

日本語版も入手可能
www.isaca.org/currentissue

At its most basic level, the role of the operational compliance function is to ensure that laws, regulations, policies and industry best practices are followed, thereby safeguarding an enterprise from the adverse consequences of noncompliance (e.g., legal, financial and reputational injury). However, the true role of operational compliance encompasses much more. Compliance permits an enterprise to carry out its mission by ensuring that it is running smoothly, as intended and on a firm foundation. By embracing technology, fostering a positive, forward-looking compliance culture and building a diverse, multiskilled team, leaders in operational compliance can ensure that they are well positioned to handle emerging regulations, work collaboratively with operations teams, and maintain their standing in the enterprise as critical contributors to its success.

Embrace Technology

Technology will continue to be a key enabler of success in operational compliance. Enterprises are faced with both expanding regulations and a growing dependence on digital technology.[1] Compliance functions simply cannot keep pace unless they use technology to their advantage. This means developing advanced capabilities in risk analytics and predictive risk intelligence.[2]

For instance, "embedded predictive analytics enable[s] organizations to predict system health and trigger alerts or to recommend corrective actions, which can help ensure systems are performing as intended."[3] It can also help enterprises identify anomalies further upstream and assess their potential impact before they result in a material issue. Working with an in-house IT team, employing a third-party provider, and utilizing prepackaged no-code software tools are all options for compliance functions, depending on the employee skill sets, budgets and access to organizational IT resources. However, it is not simply the power of the tools themselves that results in enhanced value. "Highly paid compliance experts are working on repetitive, manual tasks, lowering the overall team efficiency and morale," notes a 2022 report.[4] Offloading such tasks to automated systems enables skilled compliance personnel to focus on more strategic work.

Compliance's relationship with predictive analytics will not be isolated to its own assurance-related projects. "As more producers recognize the benefits of predictive analytics, this method of improving production processes will no longer be cutting edge," a 3M executive wrote.[5] Instead, it will be a basic requirement to keep up with the competition. This suggests a future in which compliance becomes an increasingly collaborative two-way effort, placing more need on compliance personnel to increase their skills and level of comfort with advanced technologies. Meanwhile, it is also important to understand that machine learning (ML) and artificial intelligence (AI) applications are only as effective as the data supporting them. Therefore, it would be wise for compliance leaders to take a critical look at organizational controls related to data quality, security and integrity. These controls are crucial to compliance leaders' own efforts as well as those of the larger enterprise.

Do Not Wait to Regulate

In December 2022, Sam Bankman-Fried, founder of the multibillion-dollar cryptocurrency exchange FTX, was arrested as he was preparing to testify before the US House of Representatives Committee on Financial Services about why FTX had collapsed and filed for bankruptcy in November 2022. The charges "pulled back the veil on the cryptocurrency exchange's complete lack of internal controls and toothless risk management procedures."[6]

KEVIN M. ALVERO | CISA, CDPSE, CFE

Is chief compliance officer at Integral Ad Science. He leads the enterprise's global compliance program, including regulatory and industry standards compliance.

The FTX cryptocurrency scandal is a cautionary tale for enterprises operating in emerging fields that lack well-established regulations, even if there is no evidence of deliberate fraud or misconduct. A nascent regulatory environment may indeed represent opportunity, but the operational compliance function must approach this situation with caution because history shows that the regulatory picture will eventually become clearer. The compliance function should help the enterprise understand how well it can (or cannot) tolerate scrutiny under emerging regulations, rather than taking a wait-and-see approach and having to play catch-up later.

As the cofounder and president of MetricStream wrote in 2022:

> *Beware of the dangers of taking big risks in markets where regulation is still in the early stages. It will be years before regulators can catch up to the disruption happening in rapidly evolving digital spaces like cryptos, gaming and the metaverse. In the meantime, the task of governance falls on the individual, as well as on provider communities that have to come together to grow responsibly.*[7]

For compliance personnel in loosely regulated areas, this means looking beyond existing regulations. In general, regulation increases over time as industries and governments seek new ways to reduce the risk of harm to consumers and the public. Compliance teams must operate under the assumption that new regulations are on the way, work proactively to learn what they might look like and collaborate with operations teams to plot a path toward compliance.

Champion Compliance Culture

Understandably, many operational compliance functions devote a large portion of their time and resources to assessing the enterprise's current state of compliance with regulations related to its various business processes and utilizing detective controls to identify instances of noncompliance. However, this often overlooks the value of preventive control in the form of compliance culture. Operational compliance teams should be champions of compliance culture, ensuring that compliance is embedded in everyday workflows and supported with regular communication and education.[8] In doing so, they must find strategies to deal with the reality that compliance is not an inherently exciting topic. In short, this means making sure that communications related to compliance are positive, forward-looking and focused on the business.

Compliance functions can greatly improve stakeholders' engagement by focusing communications on future risk rather than on what went right or wrong in the past.

Enterprises often underestimate the need to explain the "whys" behind regulatory compliance, other than warning of the negative outcomes associated with breaking a rule or violating a policy. This can contribute to the perception of compliance personnel as watchdogs who get in the way of production and innovation. Compliance personnel must counteract this attitude by communicating regularly and effectively about the positive benefits of being a compliance-minded enterprise. These benefits include:

- Enhanced reputation in the marketplace and community (pride)
- Greater likelihood of fulfilling the organizational mission and achieving goals
- Ethical, transparent conduct that enhances the workplace for everyone
- Competitive advantage (Some forms of compliance, such as certification or accreditation, can be differentiators in the marketplace.)

Evaluating historical data and past outcomes will always be part of operational risk management, but compliance functions can greatly improve stakeholders' engagement by focusing communications on future risk rather than on what went right or wrong in the past. "Globally, a greater

LOOKING FOR MORE?

- Read *Achieving Data Governance and Compliance: Protecting Information. www.isaca.org/data-security-and-compliance-2020*
- Learn more about, discuss and collaborate on COBIT® and frameworks in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

number of organizations are trying to make their oprisk management programs more forward-looking."[9]

Finally, in their reports to and conversations with coworkers on the operations side, compliance personnel should never assume that their colleagues will draw the connection between an identified issue or variance and the potential business impact. Compliance personnel should always relate compliance risk to business risk and should never imply that achieving compliance is an end unto itself. By the same token, the frequency of communication and interaction between operations and compliance personnel is a key indicator of the health of that relationship. When operations personnel perceive that compliance personnel are always trying to understand the business, anticipate problems and collaborate on solutions, they are much more likely to regard the compliance function as an ally as opposed to a necessary evil.

Diversify the Team

The right mix of personnel is essential to an effective operational compliance team. Ideally, this means having people with backgrounds in auditing, accounting, law and compliance frameworks, and those who are experts in the operations side of the enterprise. In addition, employing someone who has worked at a relevant regulatory agency can give the compliance function an insider's perspective on what regulatory agencies are looking for and how their processes work. One of the key factors regulators take into consideration is whether there is a strong, functional compliance department.[10] The compliance function stands a much better chance of interacting effectively with both operations and regulators if it has people who can speak knowledgeably from varying perspectives. Compliance leaders should invest in training and development to continually grow the skill set and raise the profile of compliance personnel, reinforcing their vital position in the enterprise.

Conclusion

One article noted, "Organizations, regulatory bodies, industry watchdogs and consumers have to ensure that they work collaboratively to balance growth and responsibility."[11] Indeed, operational compliance teams cannot possibly meet the demands imposed by rapid changes—in their own enterprises and in the regulatory environment—without diverse teams that can work in an integrated and cooperative way. Utilizing technology to increase efficiency can help ensure that critical conversations take place and that compliance teams look beyond the issues of the moment and consider future risk. In doing so, they will solidify their standing as partners in and invaluable contributors to the enterprise's success.

Compliance personnel should always relate compliance risk to business risk and should never imply that achieving compliance is an end unto itself.

Endnotes

1 Bryter, *How Compliance Can Prevent Risk and Rapidly Respond to Change*, USA, 2022, *https://d6jxgaftxvagq.cloudfront.net/Uploads/g/p/y/howcompliancecanpreventriskrapidlyrespondtochangebryter_499035.pdf*
2 Idnani, N.; "The Future of Operational Risk Management," Deloitte, May 2019, *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/future-of-operational-risk-management.pdf*
3 *Ibid*.
4 *Op cit* Bryter
5 Harper, T.; "Predictive Analytics in Manufacturing," MachineDesign, 9 January 2022, *https://www.machinedesign.com/sponsored/article/21212399/3m-company-predictive-analytics-in-manufacturing*
6 Nicodemus, A.; "Bankman-Fried Fraud Charges Detail FTX's Lack of Internal Controls, Risk Management Protocols," *Compliance Week*, 13 December 2022, *https://www.complianceweek.com/regulatory-enforcement/bankman-fried-fraud-charges-detail-ftxs-lack-of-internal-controls-risk-management-protocols/32462.article*
7 Kapoor, G.; "Three Predictions for the Future of Compliance in a Super-Digital World," *Forbes*, 21 April 2022, *https://www.forbes.com/sites/forbestechcouncil/2022/04/21/three-predictions-for-the-future-of-compliance-in-a-super-digital-world/*
8 Thomson Reuters, "A Culture of Compliance," 2016, *https://legal.thomsonreuters.com/en/insights/infographics/a-culture-of-compliance*
9 *Op cit* Idnani
10 Thomson Reuters, "Building a Compliance Department," 26 July 2021, *https://legal.thomsonreuters.com/en/insights/articles/building-a-compliance-department*
11 *Op cit* Kapoor

IT Risk and IT Audit Working Together to Reduce the Burden on the Business

日本語版も入手可能
www.isaca.org/currentissue

Consider a likely scenario: A team is in the middle of working frantically, trying to meet a deadline, and they learn that their team is being audited by their organization's external auditors. The team lead is asked to provide a list of artifacts. Some of them are easy to gather, but the majority of the items listed will take a few hours to compile. So the options before the team are working late or missing the sprint commitment. What is even more frustrating is that the team was audited several weeks earlier by the organization's internal audit department. And several weeks before that, the IT risk team performed a controls assessment and asked for the same list of artifacts. The team just wants to get its work done, but it gets sidetracked with these requests.

BENJAMIN BARTZ | CRISC, AWS CERTIFIED SOLUTIONS ARCHITECT—ASSOCIATE, CCSK, CISSP

Is a governance, risk and compliance (GRC) analyst at John Deere. He is responsible for performing risk and controls assessments of third parties, internal applications and processes. He has seven years of experience in information security, with the majority of his career being in IT internal audit, first as a systems auditor and then as a supervisor and Scrum master. He also teaches network defense topics part-time at Eastern Iowa Community Colleges (Davenport, Iowa, USA).

To effectively assess an organization's control environment, IT audit and risk rely heavily on artifacts. These artifacts might come in the form of a screenshot of a configuration or an exported list of users from a system. Many times, though, these requests overlap, and asking for the same thing multiple times throughout the year creates an unnecessary burden on the business. To decrease duplication of efforts and let the business do what it does best, the third line of defense (internal audit) and the second line (risk) must work together.

To make this partnership a reality, there are four foundational principles:

1. Culture is supportive.
2. IT audit is t-shaped.
3. IT risk properly tests control effectiveness.
4. Common tools are used.

Culture Is Supportive

There are books, courses and even degrees dedicated to organizational culture, but the importance of culture cannot be emphasized enough. Security should never be seen as checking a box, and audit should not be something people fear. Employees across the enterprise must understand the importance of the security and audit teams as they start their careers at the organization, as opposed to learning about them a week before a risk assessment or an audit.[1] Risk helps the business make informed decisions. Audit uncovers gaps with organizational processes and standards that hinder the business. And a supportive organizational structure helps influence acceptance of a collaborative culture.

There are myriad organizational structures that effectively support risk and audit. Choosing a structure is a decision based on factors such as organization size and maturity. Larger, more mature organizations have dedicated risk and audit functions. Smaller organizations might instead place IT risk under another functional area, such as IT or security, to avoid duplication of efforts and streamline secure practices.[2] Regardless of where risk lands,

however, audit must remain independent and should not report under an area that would influence audit outcomes (e.g., IT in the case of IT audit). Therefore, in organizations where risk and audit are within the same functional area, such as in smaller organizations, there should be reporting in place to prevent any conflicts of interest or biases that could influence audit results.

To further enhance the partnership between risk and audit, job shadowing and swapping should be used as much as possible. Risk analysts should perform guest audits. Auditors should assist in assessments of risk and controls. These are excellent opportunities for auditors to upskill their technical knowledge and for analysts to learn more about control evaluation. These are also opportunities for each department to uncover any gaps and overlaps between the two areas.

Audit and risk must regularly market their services to the rest of the organization. If audit and risk have a seat at the table when major decisions are made, the organization will find it easier to implement solutions with a security mindset from the beginning. This could prevent the need for putting a security band-aid on existing solutions, which usually results in the adoption of very inefficient manual processes solely to meet legal and regulatory requirements. Marketing does not have to be a massive effort; it just has to be intentional. Small, frequent interactions, such as lunch-and-learns, or regular touch-bases can keep risk and audit topics top of mind and less intimidating.

IT Audit Is T-Shaped

Audit has a reputation for following checklists and running scripts, and this is understandable considering the breadth of technologies auditors must review. However, although checklists and scripts are important tools, an auditor's overreliance on them, combined with a lack of knowledge on the controls being audited, is a recipe for unnecessary or even hindered audit findings. Therefore, a t-shaped team is essential for successful and impactful audits.

T-shaped audit teams have a wide breadth of foundational auditing and technical knowledge and are made up of auditors who each have their own areas of expertise. Some will know the ins and outs of distributed operating systems and database platforms. Others will have a strong grasp of cloud controls. The amount of deep knowledge expected from each auditor depends on team size. Larger teams give auditors the opportunity to have deeper knowledge in a handful of specific technologies. They might have an Amazon Web Services (AWS) auditor and another auditor who has deep knowledge about Azure. Knowledge on smaller teams tends to be distributed more broadly. For example, one auditor may be familiar with legacy technology while another is comfortable reviewing cloud controls.

T-shaped audit teams have a wide breadth of foundational auditing and technical knowledge and are made up of auditors who each have their own areas of expertise.

In support of a t-shaped audit team, audit management must keep an inventory of the skills, certifications and degrees of each member of the team; review this inventory periodically; and encourage continuous education via conferences, webinars and certification exam reimbursement. This also helps when external auditors and regulators ask for the credentials of the auditors.

In addition to formal education, auditors need hands-on technical experience to apply the concepts they learned in the certification programs. This can be accomplished by having auditors participate in building the tools and scripts they use for performing audits. This can also be an opportunity for building relationships across the enterprise as these tools might require the help of a subject matter expert. These opportunities will not only help build an auditor's skills and relationships, but also increase the quality of the tests performed and prevent false audit findings from causing incorrect script output.

IT Risk Properly Tests Control Effectiveness

IT risk and IT audit have a number of similarities. However, one key distinction is that IT audit must always remain independent. Its tools and scripts should not be used as a first or second line of control as that could lead to hiding the root causes and to audit being responsible for auditing its own processes. Because of this, audit should rely on risk's testing when possible. For this approach to succeed, though, risk must know how to properly test a control's effectiveness and document it in a reliable way.

LOOKING FOR MORE?

- Read *Incorporating Risk Management into Agile Projects. www.isaca.org/incorporating-risk-management-into-agile-projects*
- Learn more about, discuss and collaborate on audit and assurance in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Using one shared platform for audits and risk assessments enables both teams to leverage each other's work and gives risk and audit leadership combined metrics to illustrate the entire picture.

The risk team must be familiar with information provided by the entity (IPE) and information used by the company (IUC) concepts to ensure the reliability of its work. IPE gives an auditor assurance on how an artifact was generated. IUC, on the other hand, gives the control owner assurance on how an artifact was generated. For example, a data owner performs a monthly review of all access to a system in which the data they are responsible for resides. The system administrator provides the data owner with an export of all user access logs for review. Before performing the review, the data owner must know exactly how the list was extracted. Otherwise, there could be a gap that goes unnoticed—for example, if the system administrator filtered out all system IDs thinking the data owner did not care about those IDs. Without the provision of this IUC, the data owner would never catch this large gap in the control.

In the same scenario, IT audit asks the system administrator for the same thing—a list of all users generated from the system. If the system administrator does not provide IPE, the auditor cannot be confident in the completeness and accuracy of the report. Regardless of who is to receive the report, the system administrator must include source, data, report logic and report parameters to ensure its reliability:

- **Source data**—Refers to the origin of the extracted data, that is, the system of record. In the example, this would be the server that housed the list. Or, if it came from a database, it would be the name of the database.
- **Report logic**—Refers to how the data were extracted and transposed into the artifact provided. In the example, this might be "export to Excel from active directory." In essence, the report shows how the data got from format A to format B.
- **Report parameters**—Refers to any filters applied. Again, based on the example, this might be "filtered on user type 'USER.'" This ensures the data's completeness.

For the audit team to rely on the artifacts the risk team used for testing, IPE/IUC must be provided. Otherwise, audit will have to retest everything to ensure the accuracy and completeness of the data.

Common Tools Are Used

To promote cross-team collaboration, the risk and audit teams must align their tools. Using one shared platform for audits and risk assessments enables both teams to leverage each other's work and gives risk and audit leadership combined metrics to illustrate the entire picture. For example, "Application A showed strong controls in a recent controls assessment but failed an audit." These findings can point to a needed review of risk and audit programs, scoring methodologies and processes.

Shared tools also allow the storing of artifacts in a shared record. To see if a system and organization controls (SOC) report was issued in a recent third-party review of application B, for example, the IT audit team can simply check the application record's document repository and pull any artifacts that are needed for review. Access must be configured appropriately when sharing artifacts. Artifacts such as system configurations can be shared between both groups. However, items such as audit interview notes must be kept confidential. Account management must be considered when choosing a platform.

Although using the same platform to store risk assessments, controls assessments and audit workpapers would be ideal, it is not a requirement. For situations in which a shared platform is not utilized, there are other ways to collaborate between teams. An application programming interface (API) can be used between systems, which can help from a reporting perspective. Audit can leverage the data output from risk assessments to determine the highest-risk applications across the enterprise. This can help with audit scope planning. IT risk, on the other hand, can determine which control families have been audited and note their corresponding effectiveness levels. This points to a security gap in the enterprise that could require a risk assessment.

When separate tools are being used, cross-training and access must be considered. Auditors could be trained on and given access to IT risk's system to pull artifacts that were already requested and stored as part of a controls assessment. Doing so would prevent audit from asking the business for an artifact that was already provided during a controls assessment. Again,

access management must be securely configured. For example, audit might be given access to risk's governance, risk and compliance (GRC) platform for the length of the audit period and only for specific records (or possibly even fields).

Partnership in Action

An example of this partnership in action might look like this: Audit is in the middle of scoping an IT audit of the human resources (HR) function. To help determine the scope of the audit, the team uses a dashboard directly connected to the data source where risk assessments are being stored and sorts the systems and vendors by highest criticality. These data provide audit with an objective way to prioritize the scope of the audit by the third parties and systems most critical to the organization.[3] Moreover, the audit team can verify this list with the business to see if anything is missing, as opposed to asking the business to start a list from scratch.

After the audit has been planned and communicated appropriately, the team is ready to perform the audit. Part of this audit includes reviewing third parties that are hosting any of the applications in scope. Rather than the auditors asking the business to reach out to their third-party contacts for proof of an SOC or similar report, IT risk has already performed third-party risk and controls assessments on each supplier. All artifacts are stored within the GRC platform being used. Audit is given temporary access (or a permanent auditor role) to view the results of the third-party reviews. The auditors simply review the assessments that the risk team already performed and document their findings.

Another section being audited within each application is user account management. The auditor who is assigned to application A logs into the GRC tool where the risk team is storing its assessments and pulls up the recent controls assessment performed on application A. One of the controls reviewed addresses user access. After performing this review, the risk analyst thoroughly documents analysis of this control and includes IPE for each artifact provided by the business user. Again, the auditor performs and documents a review of the assessment performed earlier and does not have to interrupt the business user for an artifact request. Of course, timeliness is important here. The original review should have been performed within the same fiscal year as the audit. And if this work will be leveraged by external auditors, it is important for internal audit to work with external auditors to understand reliance expectations and requirements.

When the audit and risk teams are in sync, they can more effectively evaluate the organization's security posture without constantly interrupting the business.

The HR audit is eventually completed. Later in the year, IT risk performs a risk assessment of the marketing function. One of the applications under review had already been reviewed by internal audit, so the risk team asks for the audit report associated with the audit of the application in scope. The risk team notices three of the controls typically evaluated already were assessed by internal audit according to the audit report and no issues were found. Risk can now mark these controls as effective and avoid sending the owner of the application a duplicate request for the same artifacts.

These examples illustrate the ideal concept of sharing input, output and processing.[4] The audit team is using risk's outputs (risk assessments) as inputs for scoping activities. Similarly, the risk team is using the audit report (output) for control assurance (processing).

Conclusion

When the audit and risk teams are in sync, they can more effectively evaluate the organization's security posture without constantly interrupting the business. Staying in sync requires more than monthly meetings with the teams. It takes persistence and intention. At the end of the day, IT audit and IT risk have different responsibilities in defending the organization, but their overall purpose is to keep the organization secure.

Endnotes

1 Tarallo, M; "Understanding, Assessing, Aligning and Transforming Organizational Culture," *ISACA® Journal*, vol. 1, 2023, *https://www.isaca.org/archives*

2 Ho, A; "Roles of Three Lines Defense for Information Security and Governance," *ISACA Journal*, vol. 4, 2018, *https://www.isaca.org/archives*

3 Schmittling, R.; A. Munns; "Performing a Security Risk Assessment," *ISACA Journal*, vol. 1, 2010, *https://www.isaca.org/archives*

4 *Op cit* Ho

A Risk-First Approach to Setting an Information Security Budget

日本語版も入手可能
www.isaca.org/currentissue

Information security is one of the most important and most popular topics in IT today. Due to the recent shift in work habits and desires, organizations need to improve their IT systems and integrate new solutions that enable safe remote work for employees. At the same time, the costs associated with preparing defenses against cybercrimes are rapidly increasing, from US$1 trillion in 2013[1] to an estimated US$6 trillion in 2023.[2] The challenge for managers is to determine how much to invest in information security.

For those setting an information security budget, determining the amount of money to spend is often a conundrum. It is hard to justify paying for a service that does not generate any revenue and tends to restrict many organization and employee actions. There are three common approaches: the compliance-first approach, the industry-average approach and the naïve approach.

Some organizations take a compliance-first approach because it is much easier to defend a budget that includes requirements for regulatory compliance. Some organizations prefer to look at what other organizations are doing and follow their lead. This can result in recommendations to spend the amount considered average for their industry, or to match the spending of their closest competitors. A third approach is to use the previous year's budget as the basis for crafting the next year's budget, but for many reasons, that approach can be naïve.

> The best and the worst scenarios for information security both arise when nothing happens.

The problem underlying the decision of which approach to take is that it is difficult for security experts to prove the efficacy of their approach. The best and the worst scenarios for information security both arise when nothing happens. It is a foregone conclusion that an organization's IT systems will be tested. If there are no detected events, that means either the organization has an exceptionally good security system and all attacks were defended, or that an attack occurred but no one noticed. In today's IT environment, any device connected to the Internet will, at least, be tested for known vulnerabilities.

It is for this reason that organizations already make investments in cybersecurity defense controls that are either preventive, detective or corrective while simultaneously maintaining administrative, technical or procedural controls that focus on risk mitigation in case a threat makes it through the defense. For example, an organization may invest in a firewall as a preventive technical measures and conduct backups as a necessary corrective technical measure in case the firewall fails. This approach helps maximize the investment return by providing both defensive and corrective actions that mitigate the overall cost of a cybersecurity attack.

PETER GROSSER

Is an undergraduate student at Ludwigshafen University of Business and Society (Ludwigshafen, Germany), participating in a cooperative study program with SAP SE, a leading enterprise software company. He has gained practical experience through internships across multiple security departments, including security operation centers. His research interests include the realm of enterprise security strategies and operations.

GERALD F. BURCH | PH.D.

Is an assistant professor at the University of West Florida (Pensacola, Florida, USA). He teaches courses in information systems and business analytics at both the graduate and undergraduate levels. His research has been published in the *ISACA® Journal* and several other peer-reviewed journals. He can be reached at gburch@uwf.edu.

Therefore, the current budgeting approaches often focus on investing in a multitude of cybersecurity measures that are difficult to defend during budget discussions. Instead, a risk-first approach to developing and defending an information security budget by evaluating the risk associated with each information security threat is proposed. Information security managers can use this risk-first approach to make informed decisions based on where the organization's greatest risk lies.

Issues With Current Information Security Budgeting Techniques

As noted, there are challenges and concerns with the current three commonly used approaches to making difficult budget decisions.

Compliance-Based Approach

The privilege of holding customer information comes with the responsibility to protect it. Many countries and jurisdictions have implemented rules about the safe handling of customer data. One method of determining how much to spend on information security is to meet the required standards of relevant governing bodies. This approach is easily defensible in most boardrooms, but it only addresses the organizational costs based on the loss of customer information. Adopting a compliance-first budget often ignores the costs associated with disrupted organizational business processes. This approach focuses on defending against cybercrimes but does not address the administrative actions that can be taken to recover from such an attack. A compliance-based approach does not include an evaluation of all cyberrisk and recovery measures and, therefore, can expose organizations to many future costs.

Industry-Average Approach

The concept of being average makes sense for an organization that is willing to accept the same level of risk that others in the same industry encounter. This approach is reasonably defensible at budget meetings since the critical decision often turns on whether to base spending on a percentage of the IT budget, an average percentage of revenue, or an amount per full-time-equivalent employee. In a study by Deloitte, enterprises spent an average of 10.9 percent of their IT budget on information security in 2020.[3] Industry details for percentage of IT budget, percentage of revenue and per full-time employee are provided in **figure 1**.[4]

Budgeting aligned with the industry average has three potential flaws. First, spending what others in the industry are spending means the organization will encounter the average number of information security issues as well. Fifty percent will have fewer information security issues and 50 percent will encounter more. This approach, in essence, outsources the decision of how much risk the organization is willing to accept. By default, the organization is accepting the risk associated with the industry. This approach removes the option for an organization to choose to make information security a competitive advantage.

The second flaw is connected to the rising increase in information security spending. Global spending on information security has grown from US$34 billion in 2017 to approximately US$60 billion in 2021.[5] This is an increase of 76 percent in four years. Being average means continually trying to spend what others are spending—an approach that may

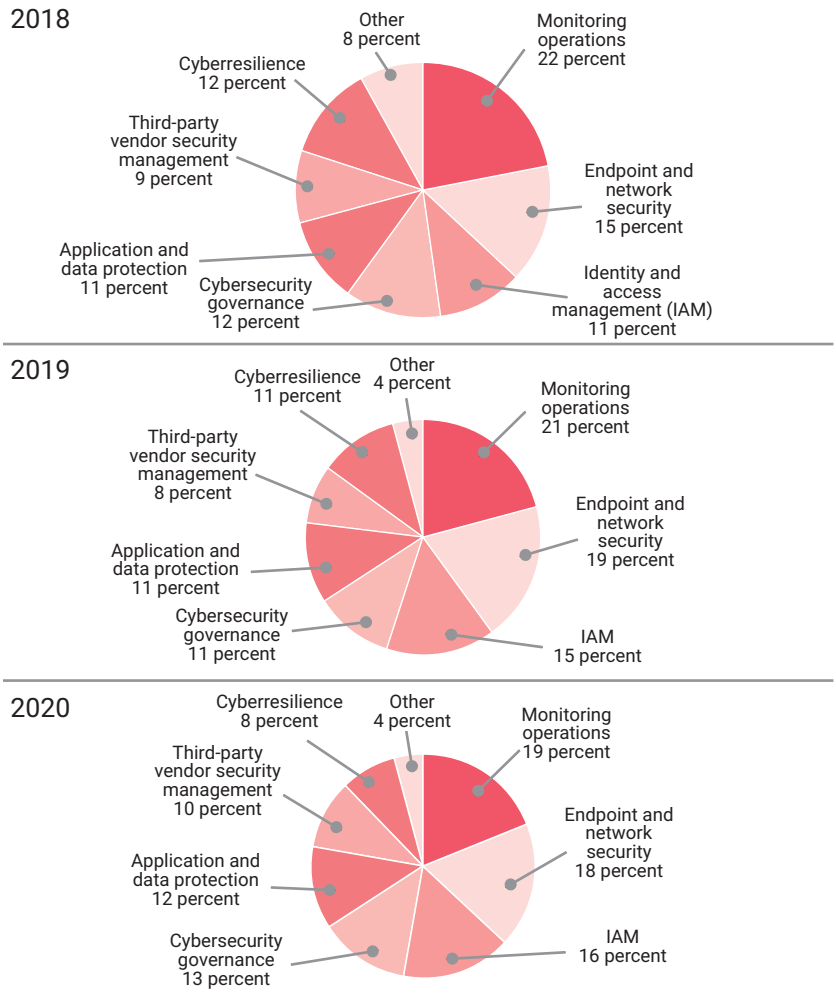
FIGURE 1

Information Security Spending Based on Industry

Industry	Percentage of Revenue	Percentage of IT Spending	Per Full-Time Employee
Consumer/financial services (nonbanking)	0.4 percent	10.5 percent	US$2,348
Financial utility	0.8 percent	8.2 percent	US$4,375
Insurance	0.4 percent	11.9 percent	US$1,984
Retail/corporate banking	0.6 percent	9.4 percent	US$2,688
Service provider	0.6 percent	7.2 percent	US$3,226
Aggregated total	**0.5 percent**	**10.9 percent**	**US$2,691**

FIGURE 2

Budget Allocation by Spending Area



not be sustainable. Organizations must find ways to manage information security costs while minimizing organizational risk.

The final flaw with this approach is associated with how the organization will spend the allocated budget. **Figure 2** shows that organizations have not significantly altered the areas associated with spending over the past several years.[6] However, this may be due to the third common approach to setting information security budgets, which is the naïve approach.

Naïve Approach

The naïve approach to forecasting is to assume that the future will look like the past—that is, deciding that next year's information security budget should be the same as the previous year's budget and the money should be allocated in the same way as in the past. **Figure 2** illustrates this approach. The percentages of the IT budget spent in each category remained relatively the same from 2018 to 2020, although information security threats certainly changed. This approach to budgeting may be the easiest to defend, but it is potentially the most flawed since it does not focus on the current risk to the organization.

Implementing a Risk-First Approach

The central focus of information security is to maintain the confidentiality, integrity and availability of an organization's information. However, there are many actors who seek to change, destroy or steal this information for profit or notoriety, which presents a risk. Taking a risk-first approach to information security starts with the assumption that risk abounds in the information sector, and organizations must find ways to manage this risk.

The insurance industry has taken this approach for decades. Insurance premiums are determined based on the probability of an event occurring and the anticipated financial loss. From an insurance perspective, the expected annual cost of an information security system could be determined by multiplying the projected maximum loss (PML) that would occur if an information attack were successful, multiplied by the probability of the event occurring over the next 12 months:

Expected annual cost = PML × Probability of occurrence

The PML, in insurance terms, is the largest loss the insurance company would expect to pay if the event were to happen.

Using this approach, information security becomes a function of minimizing the financial risk for an organization. This is accomplished by minimizing the likelihood an event will happen while simultaneously trying to find ways to reduce the loss if the event should occur.

Step 1: Estimating the Potential Loss for the Organization

The first task for information security managers is to determine the current expected annual cost of an information security failure. Successful information security attacks often result in both liability and operational costs. Liability costs are associated with

data exfiltration (the release of customer data to those who should not have it), and data exfiltration costs include the loss of goodwill, loss of future business and customer data repair costs. On the other hand, operational costs come from disruptions to IT and business processes. Organizations should determine each of these costs for their specific circumstances. To help with this task, **figure 3** provides estimates based on professionals surveyed by Ponemon Institute in 2021.[7]

One observation from this survey is that there is considerable variability in the estimates. The maximum loss estimates for both data exfiltration and business disruption costs range from less than US$10 million to more than US$500 million. Variations could be due to organization size, industry or respondents' personality attributes. Regardless, the estimates show that significant costs are associated with a loss of information security. To complete this first step, each organization needs to identify the cost that is most appropriate for both data exfiltration and business disruption.

Step 2: Estimating the Probability of a Successful Information Security Attack

This step is likely to depend on the organization's industry. To help organizations get started, **figure 4** shows the percent likelihood of a data exfiltration and business disruption due to a malware attack.[8]

Figure 4 shows that 38 percent of the organizations surveyed estimated the likelihood of an information

LOOKING FOR MORE?

- Read *Cyberrisk Quantification. www.isaca.org/cyberrisk-quantification*
- Learn more about, discuss and collaborate on risk management in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 3

Data Exfiltration and Business Disruption Probable Maximum Loss Estimate

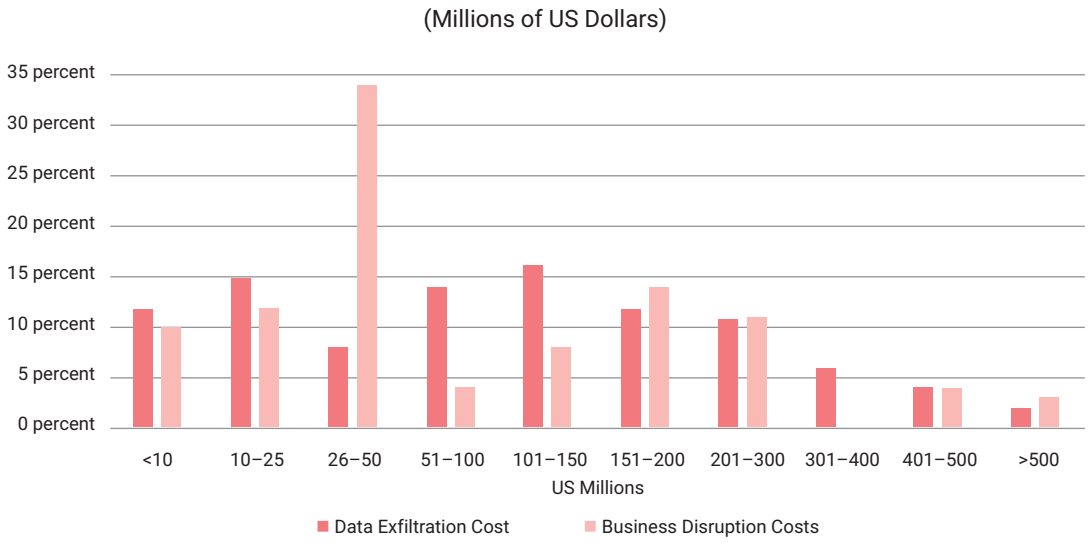
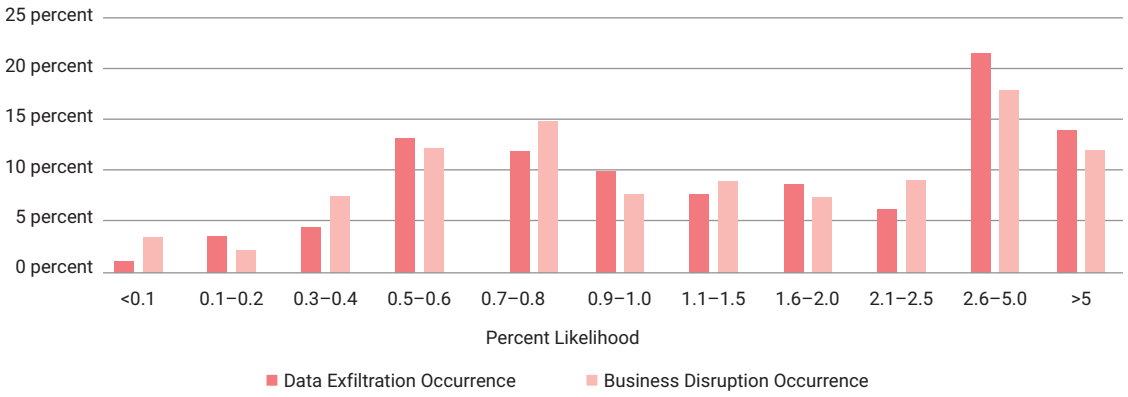


FIGURE 4

Percent Likelihood of a Disruption Due to a Malware Attack



security attack causing a business disruption to be greater than 2 percent. Similarly, 41 percent estimated the likelihood of a data exfiltration occurrence to be greater than 2 percent. Each organization should use these and other relevant data to help determine the likelihood (by percent) of a disruption due to a successful information security attack. Again, **figure 3** is only for a malware attack, so the likelihood of any successful information security attack will be greater than reported in this study.

Step 3: Estimating the Annual Cost of Information Security Attacks

Taking a risk-first approach includes estimating the annual costs associated with information security attacks. This is accomplished by multiplying the PML (step 1) by the estimated likelihood of an occurrence (step 2) for both data exfiltration and business disruption. The following equation can be used to calculate the annual total estimated cost (TEC) of information security attacks:

$$TEC = (PML_{DE} \times EL_{DE}) + (PML_{BD} \times EL_{BD})$$

(Note: $_{DE}$ = data exfiltration; BD = business disruption; EL = Estimated likelihood of an occurrence)

Figure 5 contains the average data in the survey by Ponemon Institute[9] and serves as an example of the total estimated cost due to malware.

$$TEC = (PML_{DE} \times EL_{DE}) + (PML_{BD} \times EL_{BD}) = (US\$137.2M \times .023) + (US\$117.3 \times .021) = US\$5.6M$$

The US$5.6 million estimate can serve as a reasonable starting point for many organizations. It does not suggest this is the amount any one organization paid last year. Instead, it represents the current risk for organizations. This is what an insurance company might charge to cover the average risk of covering each of the surveyed 591 clients. Organizations should develop their own PML and estimated likelihoods for business disruptions and data exfiltration and then use these three steps to determine their current 12-month risk.

Step 4: Determining the Estimated Likelihood of an Attack

The projected annual cost of US$5.6 million may come as quite a shock for many IS managers. The natural response might be to either lower the estimated probability of an attack or to reduce the

FIGURE 5

Probable Maximum Loss and Estimated Likelihood of Occurrence

	Probable Maximum Loss	Estimated Likelihood of Occurrence
Data exfiltration	US$137.2M	0.023 (2.3 percent)
Business disruption	US$117.3M	0.021 (2.1 percent)

PML. As one article stated, the "problem is that humans are poor at predicting the consequences of their actions or the risk those actions entail due to certain cognitive biases."[10] In addition, using a second method can help validate the forecasted costs.

A more scientific approach to estimating the likelihood of an event is to look at the event as a combination of probabilities. For instance, the likelihood of a successful information security attack is influenced by a combination of many failures along the way. A simplified information security system will likely have a firewall that prevents many phishing attacks from getting through. For those attacks that make it through the firewall, many more will be stopped by the antimalware software in place. A small percentage will reach the inbox of an employee who should be trained to not open suspicious emails or provide information.

The estimated likelihood of an attack is the conditional probability of each of the three events, as shown by the Bayes Theorem.[11] **Figure 6** illustrates this simplified system. Based on a study conducted by Barkly Research, the probabilities used in **figure 6** represent the risk in a real system.[12]

Figure 6 shows that the estimated likelihood of a ransomware phishing attack being successful is 0.38 percent for each attack launched on the system. This is determined by estimating the probability of each event that happens along the path. **Figure 7** shows the probabilities to further illustrate the concept.[13]

If the effectiveness of the firewall is 95 percent, then that means it blocks 95 percent of the attacks, but 5 percent of threats make it to the next step. The malware removal software is estimated to be 77 percent effective; however, only 5 percent of the threats will be evaluated by the antimalware

software because 95 percent of the threats were already removed by the firewall. The result is 3.85 percent (5 percent of 77 percent) of the threats will be removed and 1.15 percent (5 percent of 23 percent) will not be removed. Combined, the firewall and the antimalware software allow only 1.15 percent of the threats to get to an employee. This analysis assumes that the employee identifies such attacks and takes appropriate action 67 percent of the time. The outcome is that 0.77 percent of the threats are removed (1.15 percent of 0.67 percent) and 0.38 percent (1.15 percent of 0.33 percent) are not removed. The overall probability of the system failing is the product of all three individual components failing.

A risk-first approach allows IT managers to focus specifically on each type of attack and the possible associated attributes.

The Bayes Theorem provides a systematic approach for developing a more realistic estimate of the current risk of a system. This example shows the result of estimating the probability that one ransomware attack will be successful based on the current system components. Each organization should develop a Bayes model of its system and determine the probability of each type of attack.

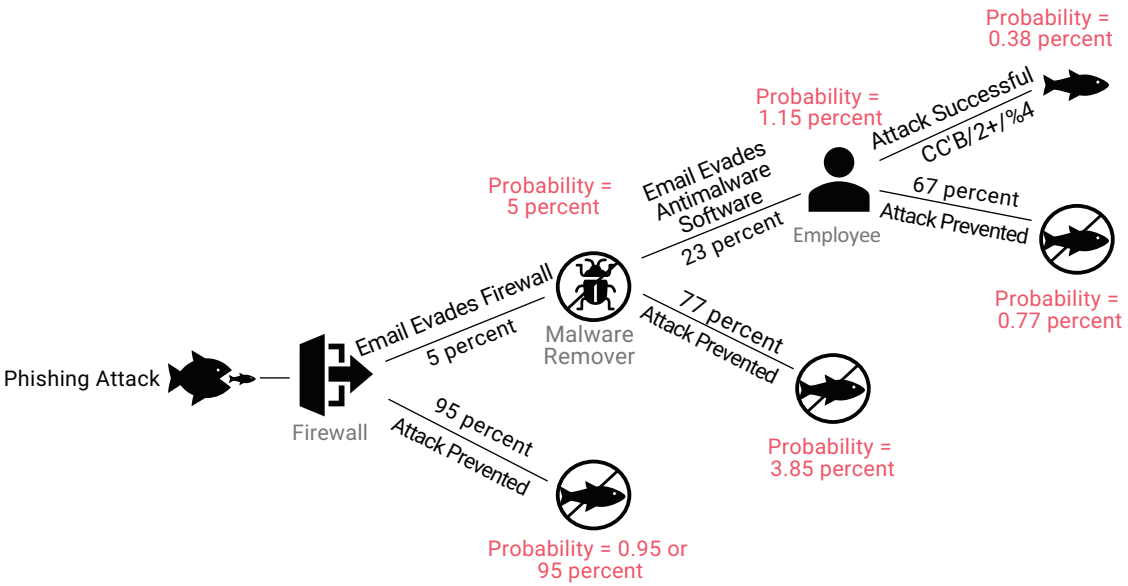
Step 5: Estimating an Organization's Annual Total Expected Cost

The annual total expected cost of information security attacks is the combined cost of occurrences, the probability of these occurrences and the types of attacks that are most likely for the organization. A risk-first approach allows IT managers to focus specifically on each type of attack and the possible associated attributes. **Figure 8** shows the average reported data for four major types of information security attacks for organizations.[14]

The data in **figure 8** show a more complete picture of the risk associated with information security attacks. Two categories that have become more important in recent years are business email compromises (BEC) and credential compromises. These attacks are focused on members of the organization who have increased access to data or the ability to transfer funds. Credential compromises often affect the same business components as malware, so the probable maximum loss for these attacks is usually the same as for malware attacks. However, business email compromises have much greater costs associated with business disruptions than with data exfiltration. By taking the time to create a similar table, IT managers can create a baseline of the risk the organization is accepting with the current budget.

FIGURE 6

Estimated Likelihood of Ransomware Occurrence Using Bayes Theorem



Creating a Risk-First Information Security Budget

These steps to implementing a risk-first approach help the IT manager gain a greater understanding of the financial risk associated with the current budget. There may be no need to change the budget if the risk is acceptable. However, that is unlikely, and a revised budget is usually needed to manage organizational risk.

For the current scenario, **figure 8** shows that the organization could incur the greatest loss from data exfiltration due to a malware attack (US$3.16 million). The IT manager could reduce this risk by making changes to the information security system that would reduce either the current probability of an attack (2.3 percent) or the possible maximum loss (PML) (US $137.1 million).

The Bayes Theorem can be used to identify ways to reduce the overall probability of an occurrence. Since the overall probability results from the combination of all events, the likelihood of an attack can be decreased by increasing the effectiveness of current components, by replacing components with more effective components, or by adding components.

Adding a more effective firewall could reduce the probability of a malware attack, given that the probability of the system failing is the product of each system failing. Replacing a firewall with one that is more effective could create a positive return on investment if the new firewall costs less than the risk associated with the current firewall. In the current example, what happens when an organization replaces the existing firewall (95 percent effective) with a firewall that is 97.5 percent effective?

- A firewall that is 95 percent effective has a 5 percent failure rate.
- A firewall that is 97.5 percent effective has a 2.5 percent failure rate.

The original firewall allows twice as many threats to get past than the more effective one. This doubles the overall probability of an information security attack being successful. Replacing the firewall could reduce the costs associated with a malware attack by US$2.81 million (US$5.62 ÷ 2).

FIGURE 7

Probability Associated With Each Step of a Ransomware Attack

Step	Probability at the Start of the Step	Probability of Removal in Each Step	Probability of Threat Removed Cumulatively	Probability Threat Is Not Removed
Firewall	100 percent	95 percent	95 percent	5 percent
Antimalware software	5 percent	77 percent	3.85 percent	1.15 percent
Employee	1.15 percent	67 percent	0.77 percent	0.38 percent

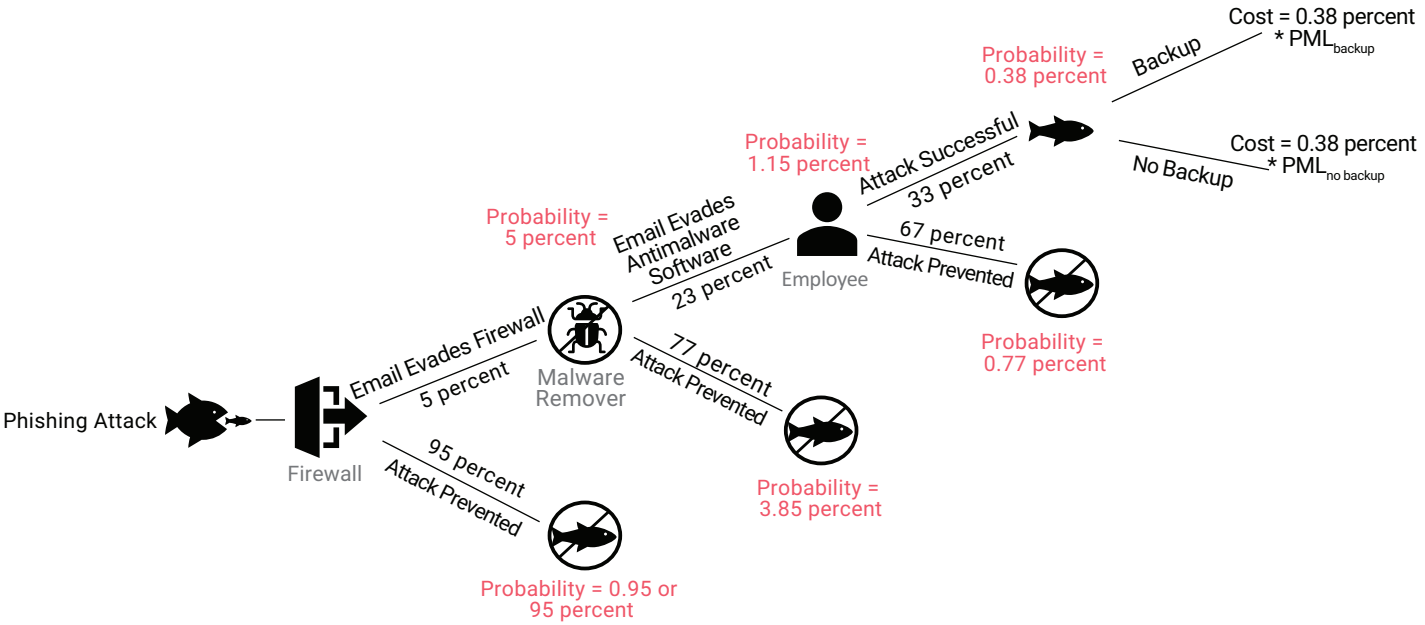
FIGURE 8

Estimated Annual Cost of Information Security Attacks (US Millions)

	Data Exfiltration			Business Disruption			
	Probability	PML	Total Cost	Probability	PML	Total Cost	Total
Malware	2.30 percent	$137.10	$3.15	2.1 percent	$117.30	$2.46	$5.61
Ransomware	3 percent	$15.60	$0.47	3.2 percent	$67.50	$2.16	$2.63
Business email compromise	1.10 percent	$8.10	$0.09	1.5 percent	$157.00	$2.28	$2.37
Credential	0.80 percent	$137.10	$1.11	1.4 percent	$117.30	$1.67	$2.78
						Grand Total	$13.39

FIGURE 9

Cost Comparison Associated With System Backups



Similar arguments can be made for increasing awareness training for employees, especially for those employees who are more likely to be targeted for business email and credential compromises. Security awareness is the knowledge and attitude instilled in employees regarding the protection of the physical and, especially, the information assets of the organization.[15] The risk-first approach allows IT managers to calculate a potential organizational loss based on employee activities and could increase security awareness and decrease successful attacks.

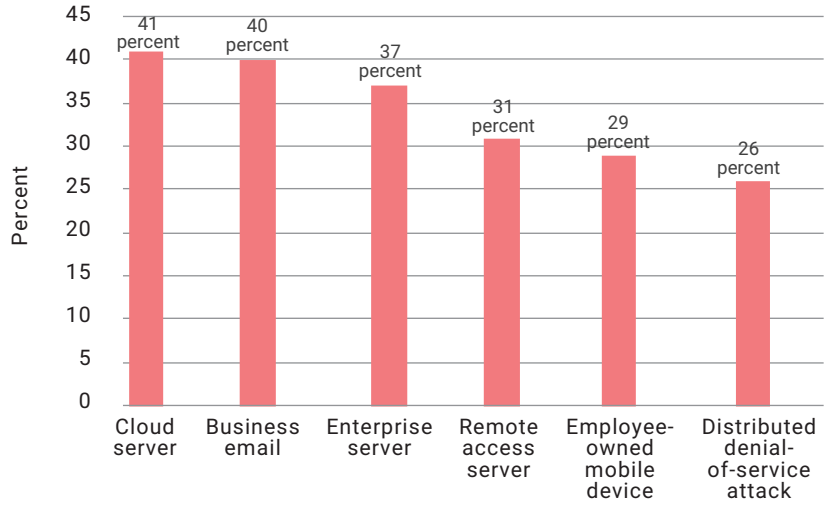
A second way for IT managers to reduce the overall risk to their organizations is to find ways to reduce the cost of a security attack. One option is to mitigate the overall cost in the event an attack is successful. The Bayes Theorem can once again be applied since each situation can be defined in mutually exclusive terms. For example, having an effective system backup plan can reduce business disruption costs. **Figure 9** illustrates both having a backup and not having a backup.[16]

The cost associated with the risk of not having a backup now becomes more concrete since the biggest aim after an attack is to restore the system.[17] A similar situation occurs when discussing whether an attack can be contained. Finding ways to lower the PML results in lowering the overall financial risk for the organization.

A final area of consideration is the use of policies that could reduce organizational risk. Attacks on private devices affect employees—and sometimes their organizations—because these attacks can result in compromised organizational data. Employees were the initial entry point for more than half of cyberattacks on European and US enterprises in 2022 (**figure 10**), with 29 percent coming from employee-owned mobile devices.[18] Policies that restrict the use of private devices to access organizational data might decrease the number of successful attacks.

FIGURE 10

Most Common Methods of Entry for Cyberattacks



Conclusion

There will always be risk associated with information security because it is impossible to have completely flawless security.[19] Organizations could spend all their revenue building fortresses around servers, restricting the use of every device, and stopping all email traffic to employees, yet attacks would still occur. The goal must be to determine the current risk to the organization and find ways to reduce that risk. Understanding the most likely events and their associated costs allows IT managers to focus on the largest financial risk to the organization. This allows for systematic development of priorities while developing a budget that is directed at reducing the overall risk. Taking a risk-first approach to information security therefore becomes defensible during budget discussions and can lead to competitive advantages for the organization.

Understanding the most likely events and their associated costs allows IT managers to focus on the largest financial risk to the organization.

Endnotes

1 Kshetri, N.; *Cybercrime and Cybersecurity in the Global South*, Palgrave Macmillan, United Kingdom, 2013

2 Purplesec, "Cyber Security Statistics: The Ultimate List of Stats, Data, and Trends for 2023," *https://purplesec.us/resources/cyber-security-statistics/*

3 Bernard, J.; D. Golden; M. Nicholson; "Reshaping the Cybersecurity Landscape: How Digitalization and the COVID-19 Pandemic Are Accelerating Cybersecurity at Many Large Financial Institutions," Deloitte, 24 July 2020, *https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html*

4 *Ibid*.

5 Sava, J.; "Spending on Cybersecurity Worldwide From 2017-2022," Statista, 28 November 2022, *https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/*

6 Ponemon Institute, *The 2021 Cost of Phishing Study*, USA, June 2021, *https://www.proofpoint.com/us/resources/analyst-reports/ponemon-cost-of-phishing-study*

7 *Ibid*.

8 *Ibid*.

9 *Ibid*.

10 Catán, I.; "The First Steps of Quantitative Risk Management," *ISACA® Journal*, vol. 3, 2019, *https://www.isaca.org/archives*

11 Bayes, T.; "An Essay Towards Solving a Problem in the Doctrine of Chances," *Philosophical Transactions of the Royal Society of London*, vol. 53, 1763

12 Kern, C.; "Ninety-Five Percent of Ransomware Attacks Bypass Firewalls; 77 Percent Permeate Email Filtering," VarInsights, 22 November 2016, *https://www.varinsights.com/doc/of-ransomware-bypass-firewalls-email-filtering-0001*

13 *Ibid*.

14 *Op cit* Ponemon Institute

15 Kakareka, A.; "Detecting System Intrusions," *Network and System Security*, Elsevier, Netherlands, 2013

16 *Op cit* Kern

17 Axelrod, C.; "Cybersecurity and Critical Infrastructure: Looking Beyond the Perimeter," *Information Systems Control Journal*, vol. 3, 2006

18 Hiscox, *The Hiscox Cyber Readiness Report 2022*, Bermuda, *https://www.hiscox.com/cybersecurity*

19 Ghosemajumder, S.; "You Can't Secure 100 Percent of Your Data 100 Percent of the Time," *Harvard Business Review*, 2017, *https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time*

Extended Accountability of the CIO

Disponibile anche in italiano
www.isaca.org/currentissue

The role of the chief information officer (CIO) is no longer that of a simple IT manager. The CIO is now responsible for the sustainable management of all enterprise-related information and must, therefore, provide the means to process information, guarantee the continuity of related services, ensure the protection of information, comply with applicable laws and regulations, and supervise all these activities to ensure that they align with enterprise objectives. In effect, the role of the CIO has evolved. The CIO is now the main person accountable for the fair treatment of all business-related information, rather than merely the person responsible for containing the costs of technology.

If the CIO's role is limited to compliance with technology objectives and cost containment, not all current business expectations will be appropriately or sufficiently addressed. Governance, risk and compliance (GRC) practices require the CIO to have the skills to link information processing technology with the value of that information for the enterprise. A governance role that is active and integrated into internal processes allows the creation of value for the enterprise by effectively and efficiently linking organizational needs to operational aspects of the business. A CIO focused only on economic savings or technology objectives does not have the skills needed to correctly interpret the evolution of business needs.

In corporate governance, the classic organizational structure considers the CIO to be a C-level position oriented toward the governance of information technologies, with the ability to analyze costs and benefits and the authority to dispose of operational resources. However, the CIO also has the privilege of interacting directly with other senior managers and taking an active part in the broader process of governing organizational risk. This is an undoubted advantage because it allows the CIO to govern information and technology (I&T) with a perfect understanding of the value and role of information while acting in full compliance with the objectives of the enterprise.

To add new and recognized value to this role, CIOs must evolve from being simply observers of business strategy to being aware of the consequences of their decisions on organizational performance as a whole. They must balance technological knowledge of operational processes with organizational skills that allow them to understand and preserve the value of the enterprise's assets. They must be able to guarantee the ability to preserve the value of information by ensuring its appropriate treatment, guarantee the availability of information in

LUIGI SBRIZ | CISM, CRISC, CDPSE, ISO/IEC 27001:2013 LA, ITIL V4, NIST CSF, UNI 11697:2017 DPO

Is a lead auditor and 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 headed information and communications technology operations and resources in the Asia and Pacific Countries (APAC) region (China, Japan and Malaysia) and was the worldwide information security officer. 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 controls. He also designed a cybermonitoring tool based on open-source intelligence (OSINT) and an integrated system involving risk monitoring, maturity model and internal audit. In addition, Sbriz was a consultant for business intelligence systems for several years. He can be contacted at *https://www.linkedin.com/in/luigisbriz* or *http://sbriz.tel.*

accordance with business needs and guarantee the continuous protection of information.

Guaranteeing the Appropriate Treatment of Information

The CIO must be able to meet business expectations in terms of providing adequate technological infrastructure, applications and services as well as proposing and providing suitable solutions to support the enterprise's objectives. The IT function must be based on a holistic vision of business processes, which includes designing, releasing and governing operational processes; allocating the necessary resources at acceptable costs; and monitoring operations. Using business objectives as a guide, it is first necessary to understand the enterprise's information processing needs—that is, the critical requirements—to develop the proper implementation, delivery and control of the requested services.

For CIOs to propose and ensure the delivery of technological solutions that align with business objectives, they must have adequate knowledge of planning and control methodologies, available technologies, the management of operational processes, and the services offered by the market. This knowledge need not be at the expert level, but it must be sufficient to allow CIOs to consider and consciously decide on appropriate solutions. They must be able to grasp the elements that create value for the enterprise and recognize those that lead to unacceptable risk scenarios. CIOs should be supported by technology officers in planning and operational matters.

Guaranteeing the Availability of Information

Information must be available based on the service requirements defined by the enterprise, such as when and for how long information is needed, in compliance with a preestablished quality level ascertained by continuous monitoring. Business needs must not be a mere imposition on IT services; they should result from a combination of business processes, internal controls and technological services.

A risk analysis evaluates decisions, and it requires the participation of the CIO as an enabler of actions that create value, such as holistically assessing the critical need for technological change and engaging the appropriate resources.

An interesting aspect of information availability is the outsourcing of processes. Outsourcing the management of IT services is sometimes justified as a simple means of saving money; however, this paradigm needs to be reversed. The consequences of violating the confidentiality, integrity or availability of data must be evaluated by a risk analysis before making any decision about outsourcing. In this, the CIO should be supported by specific IT managers dedicated to business process needs and other operational specialists.

[The CIO] must be able to grasp the elements that create value for the enterprise and recognize those that lead to unacceptable risk scenarios.

Guaranteeing the Continuous Protection of Information

Access to information must be controlled in a manner consistent with the corresponding data security classification. Information protection is largely a function of the IT department, even though it may not own the data. In such cases, depending on their organizational position, CIOs should possess the necessary knowledge related to the information's value and should take action to evaluate the effectiveness of the security strategy, verify the operational plans and promote improvement.

This perspective of the CIO's role, which encompasses some of the typical attributes of the chief information security officer (CISO), is justified by the CIO's position in the organization. The CIO is responsible for achieving I&T process objectives, has the authority to allocate the necessary resources, and is a member of top management. This position, centralizing all decision-making and verification flows, offers the best overall business vision and ensures the person has the opportunity to understand and respond to problems. In contrast, the CISO is vertically focused on security issues and does not have the same big-picture perspective as the CIO. The CIO must continuously balance I&T objectives with organizational, operational and control issues, which allows the CIO to face risk scenarios with a

LOOKING FOR MORE?

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

greater critical sense. The CIO should be supported by the CISO in operational matters.

Aligning With Business Goals

The activities constituting the I&T process should be evaluated on a regular basis to ensure that they align with business objectives. To verify the results of I&T process management from a global business perspective, the mastery of GRC-related skills is required. The issues CIOs must deal with are distinct from each other but necessary for the governance of I&T. Information represents the value to be protected, while technology is the means of doing so.

Risk

To manage information-related risk, it is essential to have the active participation of those with global accountability for infrastructures, systems, services and information technologies, not just security. The CIO's role should allow for an understanding of the value of the information processed, the critical nature of the technologies that manage it, and the consequences of the decisions made. In this way, the management of the I&T process will be guided by a systematic approach based on risk awareness.

Technology

CIOs do not carry out any operational tasks related to I&T processes but function only at a management and control level. Even so, they must maintain and update their technological skills so that they can evaluate and explain, in an understandable way, the relative advantages and disadvantages to top management and thus direct the decision-making process. Specialist knowledge can be entrusted to the operational roles in the enterprise.

Continuity

Processes that are critical to the business must meet the operational parameters set by the enterprise. Consequently, continuity plans, the business impact analysis (BIA) and incident management procedures must be verified in terms of the concreteness of the scenarios, consistency in control design, and the adequacy of allocated resources. The CIO should assume a supervisory role to improve the continuity process and make it more resilient—that is, all actions are planned and carried out with respect to business objectives and without distorting the budget.

The CIO must continuously balance I&T objectives with organizational, operational and control issues, which allows the CIO to face risk scenarios with a greater critical sense.

Security

Protecting the use of and access to classified information is not the direct responsibility of the CIO. However, based on knowledge of such information's critical nature, the CIO can act as a supervisor and provide the appropriate level of attention needed to correct existing measures and for resource finding. The CIO can also act as an enabler of the segregation of duties (SoD) and user revalidation processes.

Privacy

Any processing of personal data carried out by the enterprise falls largely in the realm of information security, even if these responsibilities are assigned to others. Although this topic is not directly pertinent to CIOs, they should have broad knowledge of critical processes and legal compliance requirements and, therefore, have great potential to act as data protection officers or similar figures if the law allows. In this sense, because CIOs are not data owners but have a complete view of the data treatment process, they can effectively support the data controller in protection and awareness actions and implement the necessary controls so that the process complies with legal requirements.

Compliance

Verifying compliance with internal and external rules is generally the responsibility of the internal audit function. Though not directly involved in the verification process, CIOs retain accountability to see that all IT actions are implemented in accordance with operational plans, and that controls are regularly carried out. CIOs should participate in the drafting of both the risk treatment plan and the audit remediation plan. Although these two plans have different origins, both are aimed at improving business processes, including in the IT area.

Evaluating the CIO's Performance

The CIO's performance should be evaluated based on four main objectives:

1. **Security**—This assessment considers the number and severity of incidents resulting in compromised information and the results of audits and all reports relating to security.
2. **Continuity**—This metric considers the number of incidents, near-miss incidents and anomalies found. Severity is used as a weight for a normalized mean.
3. **Quality**—This is the ability to meet predetermined demand in compliance with the level of service requested, including release and remediation timelines. This value is the average percentage of the level of satisfaction achieved, the number of anomalies found, the delays accumulated and the additional budget used, compared with the respective target values.
4. **Efficiency**—This is the ability to provide requested services with only budgeted resources, possibly limiting the economic component to minimum values. This evaluation considers the value of the resources allocated in the budget and the actual commitment in the final balance.

Evaluating the results of planned activities and projects requires a metric that compares the maturity achieved for each of the four objectives. For example, **figure 1** depicts the level of maturity achieved on a scale of 0 to 1 for each objective. This clearly highlights cases where objectives were not achieved.

Evaluating CIOs in this way guarantees a balance between technology knowledge and governance aptitude and between providing strategic direction and verifying regulatory compliance. CIOs produce little value if they focus only on technical issues or cost reduction. A holistic vision of the business is the basis for understanding all the significant aspects of organizational objectives and making informed decisions about potential consequences.

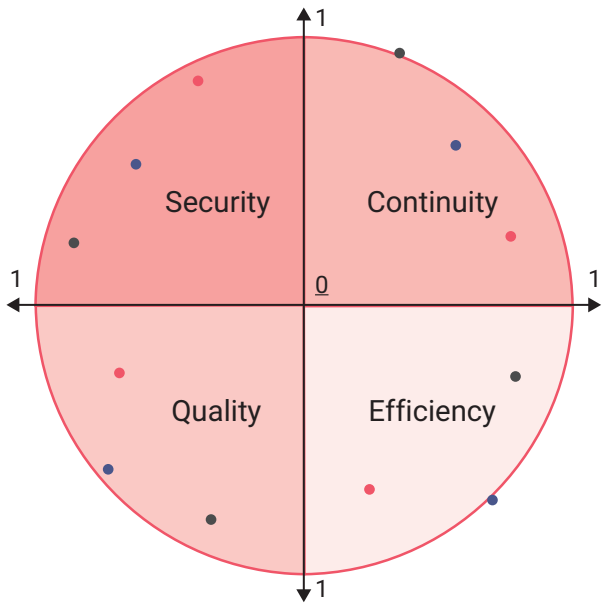
To make I&T management more effective, the role of the CIO must be broadened, which means acquiring greater skills and responsibilities in the GRC area.

Conclusion

To make I&T management more effective, the role of the CIO must be broadened, which means acquiring greater skills and responsibilities in the GRC area and paying the right amount of attention to control from a business perspective rather than basing it purely on technological performance. The CIO must be a C-level position—that is, the level of management that

FIGURE 1

Evaluation of the CIO's Performance



Legend
- **Objective A** (e.g., enterprise resource planning [ERP] upgrade to version 12)
- **Objective B** (e.g., 15 percent reduction in operating costs)
- **Objective C** (e.g., outsourcing the development team)

Note
- The circle is the target normalized to 1.
- Each objective is evaluated on the theme of each quadrant.

sets overall objectives and possesses the authority to allocate the necessary resources for the sole purpose of achieving those objectives.

The role of the CIO is to provide implementation guidelines and evaluate the achievement of results to ensure that information is processed according to real business needs, that information is available in the manner and at the time required, and that information is protected from unauthorized use or access. For this to occur, the CIO must have the skills necessary to understand business requests and associate them with available technologies, to organize activities with the right roles and responsibilities, to supervise the execution of controls, and to evaluate the current state of the I&T process.

The CIO's role has become less technical and financial and more GRC-focused. This requires horizontal competence in organizational processes, including risk analysis, compliance assessment and communication skills. At the same time, the role of the CISO has been partially redefined to avoid overlap, such as greater technical and methodological verticalization related to security, with the CISO reporting directly to the CIO.

Incident Response Automation Through IRP Implementation

A large European managed security services provider (MSSP) and systems integrator (The Enterprise) runs multiple operations centers throughout the region. The Enterprise provides managed security services for more than 850 commercial and public organizations, from small businesses through major enterprises, across diverse industries and federal authorities.

The Enterprise must operate 365 days a year on a 24/7 basis. The Enterprise's mission is to protect its clients from all types of attacks and respond if a cyberevent occurs. To support this mission, The Enterprise must operate best-in-class technology to identify, detect and respond to incidents. These systems include numerous technologies:

- Secure email (through which The Enterprise communicates with its clients and partners)
- Networkcentric detection and response tools
- Security information and event management (SIEM)
- Security orchestration, automation and response (SOAR)
- Incident response platforms (IRPs)
- Threat intelligence
- Other expected technologies found in a traditional SOC

The Enterprise's joint SOC has been in operation since 2012 and currently employs more than 400 cybersecurity experts who provide managed security services (MSSs) and managed detection and response (MDR) services, and build and operate cybersecurity systems for clients.

The Enterprise serves a diverse set of clients, including a major energy company that manages a range of assets across the Commonwealth of Independent States (CIS), Europe and Russia. This energy provider maintains various business units (BUs) including those that oversee the production and sale of electric and thermal energy; the engineering, design and construction of energy facilities; the governance of thermal and hydroelectric power plants, and the maintenance of electric grid and energy trading companies in the CIS and Europe. The customer operates more than 50 branches

KATIE TEITLER

Is a senior product marketing manager at Axonius where she is responsible for the company's cybersecurity asset management product messaging. She is also a co-host on the popular podcast Enterprise Security Weekly. Prior to her current roles, Teitler was a senior analyst at a small cybersecurity analyst firm, advising security vendors and end-user organizations and authoring custom content. In previous roles, she managed, wrote and published content for various research firms including MISTI (now part of the CyberRiskAlliance), and a cybersecurity events company. She was also the director of content at Edgewise Networks, now part of ZScaler.

ALEKSANDR KUZNETCOV | PH.D., CISM, CISSP

Is a security operations center (SOC) architecture team leader and an independent cybersecurity expert. He has more than 15 years of experience in cybersecurity projects within Asia, the Commonwealth of Independent States and Russia. Currently he teaches students about cybersecurity.

across different time zones, hundreds of information systems, internal and external IT services (for citizens, energy buyers, and government agencies), and supervisory control and data acquisition (SCADA) systems. This energy company contracted with The Enterprise to serve as its MDR provider, allowing its employees to focus on their core competencies while securely facilitating digital transformation.

Challenge

The Enterprise's client (The Client), as with most energy companies worldwide, is in the middle of a digital transformation, taking old systems historically used to run energy facilities and modernizing them to serve today's digital economy. The challenges of modernizing energy infrastructure are well known[1] and beyond the scope of this discussion. Needless to say, the consequences of exploitation of vulnerabilities in energy systems could result in dire consequences, not the least of which is loss of human life.

In addition, cyberattackers are increasingly taking advantage of the vulnerabilities in energy sector hardware and software, and the comingling of information technology/operational technology (IT/OT) to affect damage.[2,3] These facts necessitate an increase in staff, monitoring and cybersecurity governance of these systems. The Client employs internal staff (employees) who interact daily with digital systems. These employees have received training and certifications to ensure that they possess the latest knowledge about these systems. However, most of the training and certifications earned by The Client's employees are related to IT systems and not cybersecurity explicitly, leaving gaps in coverage and knowledge, while increasing cyberrisk for the organization.

A logical solution to this problem is to simply hire more experienced staff to oversee the cybersecurity function. However, the worldwide cybersecurity staffing crisis means organizations across every sector are unable to hire an adequate number of trained and skilled security staff. In the case of The Client, to cover its 24/7 operational needs, it would need to hire more than 50 qualified security staff, the majority of whom would have expertise in incident response with a subspecialization in the energy sector. This is not possible given the circumstances.

After a careful assessment, The Enterprise concluded that The Client would need to centralize incident response functions and services at its headquarters or major service locations, making hiring even more challenging due to geographic restrictions.

Manual Processes and Not Enough Staff

Prior to working with The Enterprise, The Client's incident response processes were long and laborious. Reacting to simple alerts or incidents took days and weeks instead of hours because everything was done manually, and teams were not aligned on priorities. Necessary key performance indicators (KPIs) had not been defined to address the most pressing issues first.

In addition to addressing staffing concerns, The Enterprise wanted to ensure that incident response functions were equipped with the right processes and technologies to support a modern-day incident response program able to fend off cyberattacks against the energy sector. Incorporating automation and repeatable tasks were primary factors for The Enterprise.

Reacting to simple alerts or incidents took days and weeks instead of hours because everything was done manually, and teams were not aligned on priorities.

Solution

When The Client hired The Enterprise, its main goals were to gain assistance with overseeing security operations and to help fill the security gaps related to:

- **Staffing**—The Enterprise supported The Client with the appropriate number of technical staff and staff member expertise.
- **Infrastructure**—The Client maintained a heterogenous and extended IT infrastructure which introduced management complexity. The Enterprise deployed and managed tools to provide the right level of monitoring and control over The Client's environments.
- **Network access**—The Client maintained limited network access from its headquarters to its branch locations, thereby restricting the type of work that could be done and hindering visibility into normal and anomalous operations and activity on the

For proper and complete asset management, the data collection process (as defined by the data model) needed to clearly identify and display all connectivity and data transport mechanisms between data sources and data flows.

network. The Enterprise set up secure network access to ensure that network governance and control were managed.

The Client contracted with The Enterprise to assist with incident management and response—in particular, improving detection and response capabilities. At the start of the engagement, all cyberincident work at The Client's site was being done manually, which wasted significant time and effort, was error-prone, and did not lend itself to timely or appropriate response actions that could meaningfully reduce risk.

Further, when The Enterprise was onboarded as a provider, the main incident response support tool between the organizations was email. This meant that many of the follow-up actions recommended by the enterprise (to be executed by The Client) fell into a black hole of communication. The Enterprise could not know whether an active response was being undertaken by The Client or if the recommendations were being ignored or deprioritized. This lack of visibility increased both risk and frustration.

To improve incident response and, thus, cybersecurity and risk management for The Client, The Enterprise implemented functionality in three main areas.

IT Asset Management

To begin any functional cybersecurity or risk program, organizations must uncover and understand the scope of assets and the assets' related operational and security states. Without basic visibility, it is highly challenging and time-intensive to uncover vulnerabilities within systems. Further, due to the time it takes to conduct a manual asset inventory, inventories conducted without automation are highly inaccurate, making it impossible for organizations to effectively triage or remediate any event, incident or active exploit.

The Client leveraged approximately 20 different data sources and services that were already deployed in its environment. The data sources included the SIEM, Internet Protocol Address Management (IPAM), agent-based endpoint management, the antivirus software, various local databases and more. The data sources also included external services such as VirusTotal, GeoIP and others. The Enterprise stitched together data using a general data model to create an inventory that was manageable and fed the data into an incident response platform (IRP) for further analysis.

In addition to pulling together data from The Client's environment to create an asset inventory, The Enterprise created a data model that would be fed into the IRP to enumerate various key points. The Enterprise felt it was critical for the model to be part of any implemented solution because a commercial off-the-shelf solution, without any customization, would not be sufficient for The Client's need.

As such, the data model required an information-gathering step that would allow The Enterprise's staff to understand which data sources and data (primary keys) were present. These data were necessary to achieve the desired outcomes, which included faster response times and risk reduction.

Further, for proper and complete asset management, the data collection process (as defined by the data model) needed to clearly identify and display all connectivity and data transport mechanisms between data sources and data flows.

In addition to tools The Client had already deployed, two tools were added to The Client's environment to ensure that the most accurate and actionable data could be consumed by the IRP: vulnerability management (active security scanners) and an IT asset module within the IRP.

Localization Automation

Within the IRP, team members at The Enterprise created incident localization automation tasks within incident response, a testing technique used to block or isolate suspicious hosts or activities. Localization technology "can facilitate internal process, streamline workflows, increase efficiency, and boost quality"[4] for otherwise repetitive tasks, speeding up time to delivery, increasing accuracy and ensuring scalability.

Three criteria for localization automation tasks were used to determine how The Client's systems would autorespond to various alerts. There was a low-level designation intended to be used for issues such as the validation of false positives or in cases in which the impact of business process interruption was

minimal. A high-level determination would indicate a system compromise. These three criteria (two low and one high) would help automate workflows for response, whether that meant something as simple as ignoring the alert or something more impactful such as locking accounts, blocking devices (i.e., network isolation) or ceasing suspicious processes.

IRP

Before The Enterprise could begin its work, The Client had to select and implement a SOAR IRP platform. The Enterprise felt that any chosen technology must include case and incident management, workflow management and the building of an incident knowledge base.

To choose the right incident response capability, The Enterprise used three criteria to select the most suitable system for The Client:

1. Feature/functionality comparisons
2. Analyses by leading research analyst groups
3. Internal incident management process assessments (to determine an appropriate level of automation needed and identify security coverage gaps)

The third point was the most important for The Enterprise; it is not a standard approach, but the team felt it was the most accurate and appropriate for this circumstance. Further, The Enterprise was able to customize the solution to meet The Client's exact needs using an individual assessment rather than standard industry approaches (i.e., merely feature/functionality comparisons, analyses by leading research analyst groups).

Results

The technical solution to improve The Client's incident response program centered around choosing and deploying the best commercial off-the-shelf incident response solution and then customizing it to its needs. The Enterprise executed several steps to customize the IRP:

- Existing parameters were estimated for every step or decision made within incident response.
- Every response team action was dictated by a process step, as determined by the data model. Every action was designated as "sufficient," "insufficient" or "not applicable" prior to an automated action.
- Criticality was assigned to every issue (IRP function) related to any response team action: block (critical), high, medium or low.
- Response team workflows were automated via IRP customization, depending on the priority and criteria.

Process

It was important to The Enterprise and The Client to create a step-by-step process for both selection and implementation. Just as important, The Enterprise wanted to ensure that the tool could offer ongoing support throughout The Client's entire incident response journey.

The Enterprise created a data model for incident response workflows based on a general data model (**figure 1**). The goal of the model was to build a repeatable process by which The Client could run an ongoing incident response program that would allow it to handle incidents with a prioritization mechanism and thus drive down cyberrisk and organizational risk. The organization included data from integrated systems that would capture data from the IRP to assist with decision-making. Automations are being added so that The Client can easily and efficiently execute incident response playbooks.

Playbooks

One obstacle that arose was the realization that traditional physical playbooks were insufficient for modern-day incident response and modern computing. The Enterprise knew it needed to modernize incident response playbook workflows (**figure 2**).

The Enterprise wanted to ensure that The Client was fully embracing digital transformation and so provided a list of requirements for paper playbook content. Recommendations included:

- Assignment of a procedure ID
- Assignment of a procedure administrator (admin)
- Listing of involved participants
- Duration of the procedure
- Input data
- Output data
- Action algorithms

All paper playbooks were redesigned according to these specifications.

Automation

In addition to the incorporation of playbooks and workflows, The Enterprise was able to initiate some automation for The Client. Not all playbook content was able to be automated at once; however, the primary areas of automation focus were:

LOOKING FOR MORE?

- Explore the *Security Incident Management Audit Program*. *www.isaca.org/security-incident-management-audit-program*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

- **Network isolation**—Reduces malicious lateral movement
- **Disabling Universal Serial Bus (USB) device ports**—Reduces the risk that malicious content will be uploaded to enterprise systems
- **Domain account lockouts**—Locks accounts when suspicious access attempts are made
- **Automatic file deletion**—Deletes unknown or suspicious files to prevent malicious payloads
- **Automatic disabling of anomalous or out-of-band operating system (OS) processes or services**—Prevents malicious execution

Related to cybersecurity and risk management functionality, The Enterprise was able to accomplish:

FIGURE 1

Incident Response Workflow Data Model

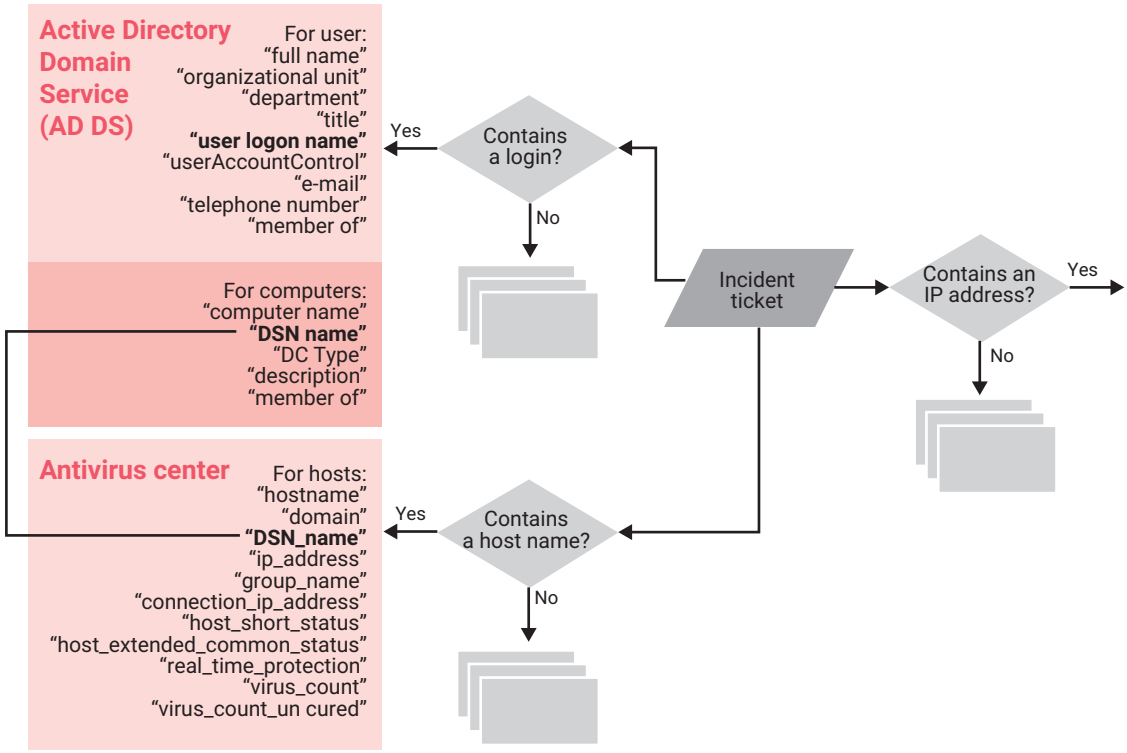


FIGURE 2

Comparison Between a Physical Playbook and an IRP

Traditional Playbook Terminology	Implications for Programming With IRP
Connect to host	• Determine the protocol and port for connection (e.g., SSH/22, RDP/3389, HTTPS/443), which implicate the IRP network connectivity matrix. • Determine the credentials for connection (e.g., an embedded account root, administrator, a named account [user login], a separate service account), which impact the IRP access control matrix.
Isolate host	• How will the host be isolated (e.g., physical, network, program)? There are different solutions for different situations: – **Windows level**—Netsh interface set interface "Interface_name" disable – **Linux level**—Ifconfig_interface_name down – **Switches level**—Interface_name shutdown – **EDRlevel**—isolation/On host_name Each solution is paired with a different integration for IRP.

- **IT asset management**—Using data collected from various technologies in The Client's networking environment, The Enterprise was able to leverage the IRP to accomplish a basic IT asset inventory, understand The Client's digital asset ecosystem, and scan assets to learn about its security state. Using this preliminary information, The Enterprise was able to notify The Client's administrators of any necessary response actions so that The Client could act on any incidents or triage issues that might impact the environment.

  Using the asset management functionality, The Client was able to set up correct routing for notifications about incidents via email and chatbots. Information about IT assets gleaned from the IRP was also instrumental in providing the necessary enrichment for decision-making and tactical enforcement actions around risky assets or assets compromised by tampering.

- **Incident localization automation**—The Enterprise used automated incident localization tasks via integration between deployed tools. Tasks were also used to automate scripting functionality that would identify when malicious or suspicious sources (e.g., hosts or accounts) were trying to obtain system access and set rules for blocking those potentially malicious sources before they could affect system damage.

The mean time to respond to incidents was reduced as a result of the new process, as was the total number of cybersecurity incidents that resulted in some form of damage or disruption to The Client.

The Enterprise is looking to make further improvements to the IRP, including greater use of automation localization tasks, the use of automation and machine learning (ML) to reduce the number of false positives, and automated enforcement actions for remediation.

Benefits

Both The Enterprise and The Client experienced numerous cybersecurity benefits as a result of the described work. The primary benefits include:

- **Time savings**—The time needed for security incident localization was reduced from days to seconds for some incident types. For the remaining incident types, a service level agreement (SLA) was created to ensure that there would be no black hole of communication in regard to incident response and reporting.
- **Risk reduction**—The number of security incidents that had the potential to inflict real harm to The Client's organization was reduced.

Since low-level tasks became automated, the current staff had more time to focus on higher-level activities and more strategic decisions, and contribute to more positive business outcomes for the organization.

Another positive business outcome was cost savings. Due to the IRP implementation and automated workflows built into the technical solution, The Client was able to reduce the number of internal employees required to manage processes by approximately 10 percent.

In addition to cost savings, The Client was able to allocate more human resources to other IT projects. Since low-level tasks were automated, the current staff had more time to focus on higher-level activities and more strategic decisions, and contribute to more positive business outcomes for the organization.

Finally, the difficulty of hiring qualified cybersecurity staff was mitigated significantly as a result of the project and the aforementioned benefits. The Client's human resources (HR) and security teams no longer had to spend time, effort and excess budget looking for hard-to-find cybersecurity talent and could therefore spend that time recruiting for other necessary positions within the organization.

Endnotes

1 Teitler, K.; "Critical Infrastructure Attack Reveals Why Access Should be the Nexus of Your Security Program," HMG Strategy, 19 February 2021, *https://hmgstrategy.com/resource-center/articles/2021/02/19/critical-infrastructure-attack-reveals-why-access-should-be-the-nexus-of-your-security-program*

2 Bailey, T.; A. Maruyama; D. Wallance; "The Energy-Sector Threat: How to Address Cybersecurity Vulnerabilities," McKinsey and Company, 3 November 2020, *https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities*

3 US Department of Energy, *CESR Blueprint*, USA, 2021, *https://www.energy.gov/sites/prod/files/2021/01/f82/CESER%20Blueprint%202021.pdf*

4 Phrase, "How Global Businesses Benefit From Localization Automation," 15 November 2022, *https://phrase.com/blog/posts/top-benefits-localization-automation/*

How to Elevate the SOC to the Next Level

日本語版も入手可能
www.isaca.org/currentissue

The security operations center (SOC) is the nucleus of an enterprise's cybersecurity program. To implement an effective SOC, it is crucial to understand what is an SOC. An analogy may be helpful: All airports have a security team whose job is to identify potential threats and prevent dangerous situations that may arise. Airport security teams are the first line of defense, and they are skilled at choosing those few individuals out of the thousands of people moving through the airport who may pose threats to national security due to their entering the country illegally or being involved in dangerous activities such as drug, human or animal trafficking. This is similar to what an SOC is expected to do, which is why the SOC is commonly referred to as the first line of defense. It plays a crucial role in the early detection of security threats within the environment. There are several essential elements that organizations can leverage to elevate their SOC to new heights.

Essential Tools in the SOC Tool Kit

The SOC relies on different security tools to effectively monitor, detect, analyze and respond to security incidents and threats, including endpoint detection and response (EDR), network detection and response (NDR), security information and event management (SIEM), intrusion prevention systems (IPSs), security orchestration, automation and response (SOAR), user entity behavior analytics (UEBA) and threat intelligence platforms (**figure 1**). Among these tools, SIEM stands as the cornerstone in the SOC analyst's arsenal, playing a pivotal role in around-the-clock monitoring operations. It is also often the starting point when it comes to early detection of security threats within the environment. Therefore, the success of the SOC greatly depends on the implementation of SIEM and the way it is configured and utilized.

Best Practices for an Effective SOC

Ensuring a strong security posture requires the implementation of effective tools and practices within an SOC. The best practices and approaches to empower the SOC to achieve optimal performance and effectiveness include:

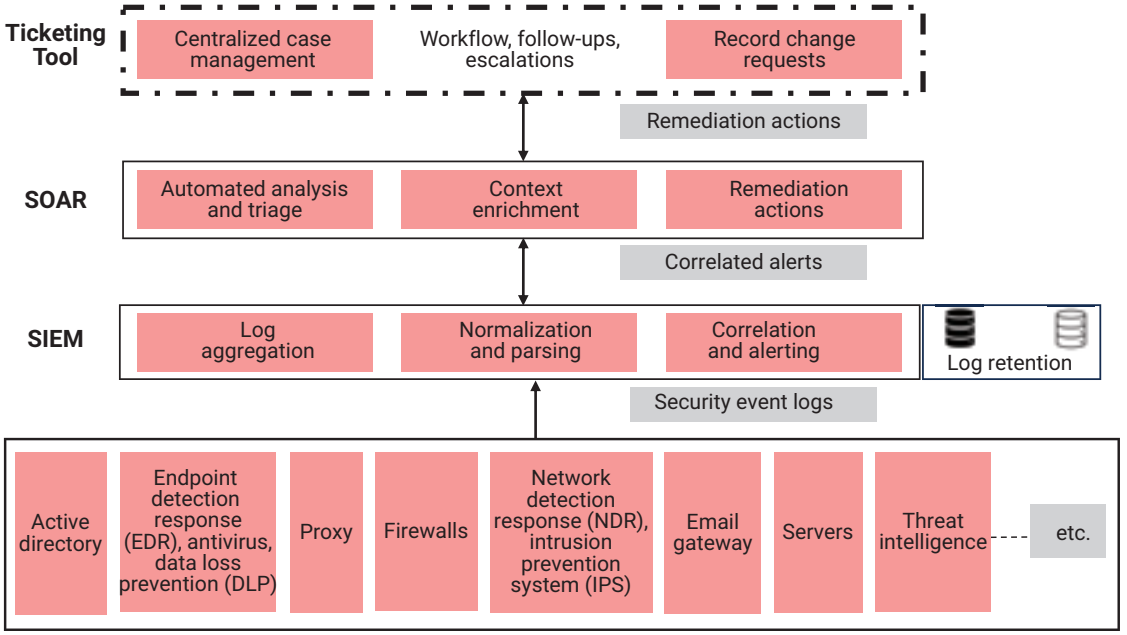
- **Consider only security-relevant logs**—Log monitoring is not equivalent to SOC monitoring, so only two types of log events should be incorporated into SIEM: security events used to build detection rules, and security events that add context to detected events. For example, firewall logs (e.g., threat, malware, Uniform Resource Locator [URL] filtering, intrusion prevention system [IPS] logs), web application firewall (WAF) logs, proxy logs and Windows operating system security logs (especially those detailing login success or failure, audit logs cleared and processes created) are relevant security logs used to create detection rules. Events that do not add value to the security monitoring process include those recorded in performance logs, availability logs, health logs, device failure logs and error logs. Incorporating these into SIEM only overloads the SOC as such events increase noise and false positive alerts and lead to higher SIEM costs.
- **Understand the network architecture**—Understanding the network architecture or how inbound and outbound traffic flows within the network is critical when analyzing an alert. Because SOC teams are often unaware of or have very little knowledge about network architecture, it takes them longer than necessary to act on alerts that are triggered. These delays impact key performance

SHWETA KSHIRSAGAR | CISA, CISSP

Is an information security professional with 18 years of industry experience in various domains of cybersecurity, including cyberincident response, data protection and privacy, information security audit, and compliance. She was recently awarded a DynamicCISO Excellence Award for her project on security operations center modernization. She can be reached at *https://www.linkedin.com/in/shwetaksagar/*.

FIGURE 1

SOC Tools Stack



indicators (KPIs) such as mean time to detect (MTTD) and mean time to respond (MTTR).

- **Leverage security logs for enhanced insight**—Every device, service, data source or cloud platform that has audit-logging capability should record security events and forward them to the SIEM tool. For example, email, virtual private networks (VPNs), virtual desktop infrastructure (VDI) accessible over the Internet, single sign-on (SSO), multifactor authentication (MFA) and remote desktop tools used to provide remote IT support are some of the entry points for attackers. These elements have been targeted and compromised in various attacks. Therefore, incorporating security events from such critical infrastructure into the SIEM and building relevant detection capabilities are important.
- **Customize detection rules**—Detection rules are the main determinants of an SOC's effectiveness, so it is important to define rules that are relevant to the specific enterprise. For example, if an enterprise typically does not operate 24/7 and does not have offices outside of its home country, its system can be designed to detect a spike in login activities on the weekend or login attempts from Internet Protocol (IP) addresses located outside the country. These events can include login events from data sources such as email, VPN, SSO and Azure Active Directory (AAD).
- **Use the MITRE ATT&CK framework**—This is a comprehensive framework that provides in-depth understanding on tactics, techniques and subtechniques used by adversaries in real-time cyberattacks. It includes 41 data sources that defenders can use to log information into their SIEM and build detection logic.[1] Mapping the enterprise's alert logic to the MITRE ATT&CK framework adds value to the entire detection engineering process. Alerts triggered by these detections could be early signals of full-fledged attacks, so it is imperative to align detection methods with tactics, techniques and subtechniques, as described in the MITRE ATT&CK framework.
- **Respond in a timely manner**—The SOC needs to be on high alert and show a sense of urgency when reacting to potential threats. SOC teams should leverage ticketing tools and collaboration platforms to effectively communicate alerts and required actions to the appropriate stakeholders. If there are repeated actionable alerts, the SOC team should implement a systemic and collective fix rather than responding to each alert with the same action. For example, in the case of alerts related to potentially unwanted programs (PUPs), it is important to analyze trends for

the last one or two months and find the root cause, which could be:

- Full Universal Serial Bus (USB) storage access is allowed.
- Proxy rules are ineffective or not enabled.
- Local administrative access is provided to normal user accounts.

Once the trends have been analyzed and the root cause identified, the SOC team can work with the IT team to implement a systemic fix across the organization. Security alerts are most commonly due to:

- Misconfiguration of security controls
- Security design flaws
- Unplanned changes that are not recorded and not approved
- Human oversight, resulting in gaps between what is documented and what is implemented
- Too many policy exceptions and listing allowances for different users within the enterprise, which are often more of a convenience than an actual business requirement
- SIEM detection rules that are not optimized

The Role of Threat Intelligence in an SOC

Threat intelligence is a vital part of the entire SOC process because it helps provide external visibility and context. It includes:

- Operational threat intelligence such as indicators of compromise
- Tactics, techniques and procedures (TTPs) of different attack groups targeting specific countries or industries
- Dark web monitoring of compromised credentials, squatted domains, or look-alike domains that are typically used for phishing attacks
- Information about a vulnerability being exploited in the wild

It is essential to take this external context into consideration. The value lies in using threat intelligence in an SOC framework that consists of not only detection-based alerts, but also situational awareness. For example, during the holiday season, attacks targeting consumer industries that typically hold holiday sale events should be expected and prepared for accordingly.

Automating the SOC

"Automation" has become a popular buzzword, but before automating an SOC, it is important to understand the foundation on which an SOC is built: people, processes and technology. Assuming an enterprise has the right SIEM technology and processes, it can run without automation, but it cannot run without people. An SOC needs to reach a certain level of maturity before introducing automation such as machine learning (ML) or artificial intelligence (AI). These elements should complement the SOC, not replace the people, who should be retrained and repurposed to do intellectually challenging tasks.

Assuming an enterprise has the right SIEM technology and processes, it can run without automation, but it cannot run without people.

Once appropriate maturity has been reached, if an enterprise wants to introduce automation to an SOC, then the enterprise needs to clearly define its objectives. For example, an objective could be a 50 percent reduction in the manual efforts of level 1 analysts by automating their repetitive tasks, such as:

- Enriching alerts with threat intelligence feeds
- Checking the reputations of IPs, domains and URLs
- Tracking trends for each alert category: recurrence, root cause and repeated user violations
- Performing follow-ups and escalations

Although an autonomous SOC has benefits, the components of an autonomous SOC may also introduce risk into the environment. For example:

- If the automation workflow goes wrong, it could revoke the access of a valid, critical user.
- If the test data used to train the ML model are modified in an unauthorized way, the ML model will not be trained correctly.

The Role of SOC in Audit and Compliance

In addition to the essential functions of threat monitoring and detection, threat hunting and incident analysis, the SOC plays a crucial role in the audit and compliance of an organization, such as with:

- Compliance monitoring
- Audit and assessments
- Cyberincident investigations
- Cyberincident reporting to regulatory bodies

For these purposes, retention of security logs and alerts is a critical activity that an SOC needs to plan and implement as part of the SIEM deployment.

Why Security Logs Should Be Retained

Security logs help identify threats early in the attack phase by triggering detection rules. However, if a security incident occurs and an incident response plan and crisis communications have been invoked, historical security logs are needed to answer questions such as:

- What happened?
- Why did the incident take place?
- When was the incident identified?
- How long were the associated activities present in the environment?
- What are the impacted systems and user accounts?

Having historical logs can speed the incident response and forensics process and help identify the root cause.

In addition, cyberinsurance requires enterprises to retain security logs to make a claim in the event of a breach. To determine the scope of a data breach, cyberinsurance organizations may engage experts in the field of incident response and digital forensics. A lack of logs usually delays this determination and can have a negative impact on the claimed amount and the overall claims process.

If a security incident occurs and an incident response plan and crisis communications have been invoked, historical security logs are needed to answer questions.

How Long Do Security Logs Need to Be Retained?

Typically, security logs are retained for a minimum of 180 days, or six months. However, depending on the nature of the business, the geographic regions in which the enterprise operates, and the applicable standards and regulations, retention periods may vary. For example:

- The Payment Card Industry Data Security Standard (PCI DSS) requires security logs to be retained for 12 months, with three months of log data available for immediate analysis.[2]
- Directives issued by the Indian Computer Emergency Response Team (CERT-IN) require logs to be retained for 180 days.[3]

Other country-specific regulations also prescribe the number of days for which the security logs must be retained. It is advisable to have an organizational policy indicating how long security logs need to be retained, and this policy should align with the regulatory requirements of the country within which the organization operates.

Which Logs Should Be Retained?

From an SOC perspective, at a minimum, security logs that contribute directly to the detection rules must be retained for a longer duration. These include:

- Access and authentication logs, such as application, VPN, domain controller, proxy, SSO and email logs
- Server logs, such as Windows security event, authentication on Linux servers, and Internet information services (IIS) web server logs

LOOKING FOR MORE?

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

- Network logs, such as firewall and intrusion prevention and detection system logs
- Cloud platform logs, such as logs that provide information on bulk virtual machine (VM) creation or deletion, storage deletion, and changes to tenant administration or tenant policies

Where Should Security Logs Be Kept?

Considerations for log retention include:

- **On-premises SIEM**—If the organization uses an on-premises SIEM tool, logs can be stored on-premises using network-attached storage (NAS) systems or network storage servers. While this approach may be more cost-effective than cloud-based storage, it may lack speed and scalability.
- **Software-as-a-Service (SaaS)-based SIEM**—For organizations using a SaaS-based SIEM, it is advisable to retain logs in the cloud service provider's data lake solutions. This approach can help reduce costs associated with transferring data out of the service provider's cloud. Some leading SaaS-based SIEM providers have introduced cost-effective solutions through tiering options such as pay-as-you-go and per day consumption.

Organizations should select a log retention solution that they find both cost-effective and operationally manageable.

Conclusion

For a long time, SOCs primarily focused on traditional enterprise infrastructure, such as domain controllers, firewalls, servers and endpoints. However, as the adoption of cloud platforms, the Internet of Things (IoT), blockchain, AI and ML continues to rise, the boundaries between these new technologies and the conventional enterprise infrastructure are becoming less distinct. This situation presents new challenges for SOC teams. In response, SOC analysts must enhance their skills in these emerging technologies, integrate them into the SOC framework and establish specific detection methods to effectively identify and counter threats to this diversified infrastructure.

Endnotes

1 MITRE ATT&CK, *https://attack.mitre.org/*
2 Payment Card Industry (PCI) Data Security Standard (DSS), *PCI DSS Requirements and Testing Procedures, Version 4.0*, March 2022, *https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf*
3 Government of India Ministry of Electronics and Information Technology Indian Computer Emergency Response Team (CERT-In), No. 20(3)/2022-CERT-In, India, April 2022, *https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf*

Harmonizing Cybersecurity Practices

The Requirements and Challenges of the EU NIS2 Directive

Cyberthreats constantly evolve, and new attack vectors, techniques and vulnerabilities regularly emerge. Keeping pace with the ever-changing threat landscape and ensuring regulatory compliance requires investments in technology, training and expertise. Enterprises must continually update their security measures, incident response plans and risk assessments—which require financial resources, proper technology infrastructure and cybersecurity personnel with the necessary skills—so they can address stakeholders' expectations.

To address this, the European Union adopted the NIS2 Directive. This directive highlights the importance of enhancing cybersecurity practices and protecting critical infrastructure and digital assets, including allocating adequate resources, obtaining legal and regulatory guidance, building cybersecurity expertise, and fostering a culture of compliance. It provides enterprises with incident notification requirements, reporting types, timelines and information required for compliance. Enterprises in the eurozone must understand the NIS2 Directive challenges and be proactive in complying with the incident notification requirements to enhance their cybersecurity posture and protect critical infrastructure and digital services.

NIS2 Directive's Rationale

Given the increased digitalization, greater interconnectedness of sectors, and heightened cybersecurity risk in today's world, the effectiveness of the EU Network and Information Systems Directive (EU) 2016/1148 (NIS1) is limited, resulting in fragmentation across the European Union at various levels.[1] Recognizing NIS1's limitations, the Council of the European Union adopted Directive (EU) 2022/2555 (NIS2 Directive) on 28 November 2022, after its earlier adoption by the European Parliament.[2] The NIS2 Directive expands the scope of covered entities, specifies management liabilities, and outlines how to carry out control activities and report breaches. The NIS2 Directive offers better guidance, clarity and harmonization of the cybersecurity requirements and practices across the European Union.[3] It includes new provisions and obligations related to incident response, supply chain security, encryption and vulnerability disclosure, and it imposes cyberrisk management, incident reporting and information sharing obligations on private and many public entities involved in various sectors.[4] It applies to multiple enterprises, including operators of essential services (OESs) and digital service providers (DSPs).

Significance of the NIS2 Directive

The NIS2 Directive is significant because it recognizes the importance of cybersecurity in the

ANTONIO M. VILLAMOR, JR. | CISA, CISM, CDPSE, CFE, CIA, CMA, CRMA, MBCS, MIEEE

Is the head of the internal audit unit of the International Center for Agricultural Research in the Dry Areas, a research institution dealing with international food security.

YIANNA DANIDOU | PH.D.

Is a lecturer at the European University of Cyprus (Engomi, Cyprus) and director of the CYBER.EUC Research Center.

functioning of critical infrastructure—especially the crucial role of DSPs and OESs, which must notify competent authorities of any incidents that significantly affect the continuity of their services.[5] The NIS2 Directive outlines specific requirements that DSPs and OESs (including small and microenterprises) must adhere to, such as incident reporting obligations, risk management, and technical and organizational security measures. By imposing specific cybersecurity requirements, the NIS2 Directive aims to protect the systems and users of all affected enterprises, ensure that critical infrastructure remains operational and resilient in the face of cyberthreats and cyberattacks, prevent confusion, and ensure that everyone is aware of their obligations.

The NIS2 Directive also provides a framework for EU member states to work together to combat cyberthreats and promote a culture of cybersecurity awareness and best practices. It emphasizes the importance of cooperation and information sharing among EU member states, which are essential for dealing with cyberattacks that cross borders and involve multiple actors. EU member states that work together and share information can respond more effectively to cyberincidents and prevent future attacks.

The NIS2 Directive covers a wide range of business sectors that are critical or highly critical, such as the energy, transportation, healthcare, research and financial sectors (**figure 1**).[6] Consequently, a wide variety of enterprises, from large corporations to public entities, are affected and must comply with the directive, making it a significant legal and regulatory development with far-reaching implications for the EU cybersecurity landscape. In addition, the NIS2 Directive does not preclude including small and microenterprises at high risk because it has built-in flexibility to consider them.[7]

Incident Notification Requirements, Reporting Types, Timelines and Required Information

One of the new incident notification requirements for OESs and DSPs is that they must notify the appropriate authorities of incidents within tight time limits, depending on the severity and impact of the incident. In the case of a cyberincident that significantly impacts the security of the network and information systems, OESs and DSPs must notify the competent authority designated by the member state within 72 hours of becoming aware of the incident. Notification must include specific information, such as details about the incident, the potential consequences, and the mitigating measures taken or proposed.

Enterprises must submit two types of incident reports: initial and final. The initial report must provide an overview of the incident within 72 hours of recognition. After resolving the incident, the enterprise must submit a final report, including a comprehensive analysis of root causes, impacts and lessons learned. The timeline for submitting the final report varies, ranging from 14 days for minor incidents to 90 days for major incidents. Enterprises must also provide information about the affected services, systems and networks, and any third-party providers or suppliers suspected of being involved. The NIS2 Directive further mandates that enterprises share information about known vulnerabilities and threats and any relevant technical and organizational security measures in place.

Keeping pace with the ever-changing threat landscape and ensuring compliance with the NIS2 Directive's requirements require investments in technology, training and expertise.

Challenges and Considerations

The emerging and growing cybersecurity threat landscape is the key obstacle to adhering to the NIS2 Directive. Keeping pace with the ever-changing threat landscape and ensuring compliance with the NIS2 Directive's requirements require investments in technology, training and expertise, which may be difficult for small enterprises or those who have limited resources. Enterprises must continually update their security measures, incident response plans and risk assessments, which requires financial resources, proper technology infrastructure, and cybersecurity personnel with the necessary skills. It could also require changes in business processes, technologies and organizational structures, which may necessitate internal coordination, cultural change, and implementation of recent technologies or security measures.

LOOKING FOR MORE?

- Read *Reporting Cybersecurity Risk to the Board of Directors. https://www.isaca.org/reporting-cyberrisk-to-bod*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

FIGURE 1

Highly Critical Sectors

Highly Critical Sectors	Examples
Energy (e.g., electricity, district heating and cooling, oil, gas, hydrogen)	Market participants providing aggregation, demand response or energy storage services; operators of recharging points providing recharging to end users; distribution system operators; and transmission system operators and producers
Transport (e.g., air, rail, water, road)	Air carriers; airport managing bodies and entities operating ancillary installations within airports; traffic management control operators providing air traffic control; railway operators of service facilities; infrastructure managers; inland, sea and coastal passenger and freight water transport enterprises; managing bodies of ports and entities operating works within ports; operators of vessel traffic services; road authorities who handle traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a nonessential part of the general activity; and operators of intelligent transport systems
Banking	Credit institutions
Financial market infrastructure	Operators of trading venues and central counterparties
Healthcare	Healthcare providers, EU reference laboratories, entities conducting research and development activities related to medicinal products, entities manufacturing basic pharmaceutical products and conducting pharmaceutical operations, and entities manufacturing medical devices critical during a public health emergency (public health emergency critical devices list)
Drinking water	Suppliers and distributors of water intended for human consumption, excluding those for which distribution of water for human consumption is a nonessential part of the general distribution of other commodities and goods
Wastewater	Entities collecting, disposing of or treating urban wastewater, domestic wastewater or industrial wastewater, excluding those for which these activities are a nonessential part of the general activity
Digital infrastructure	Internet exchange point providers; domain name service (DNS) providers, excluding operators of root name services; top-level domain (TLD) name registers; cloud computing service providers; data center service providers; trust service providers; providers of public electronic communication networks; and providers of publicly available electronic communication services
Information and communications technology (ICT) service management (business-to-business)	Managed service providers and managed security service providers
Public administration	Public administration entities of central governments and regional levels
Space	Operators of ground-based infrastructure owned, managed and operated by EU member states or private entities that support space-based services, excluding providers of public electronic communication networks
Other Critical Sectors	**Examples**
Postal and courier services	Postal service providers, including providers of courier services
Waste management	Entities conducting waste management, excluding those for which waste management is not the principal economic activity
Manufacture, production and distribution of chemicals	Entities manufacturing and distributing substances or mixtures and those producing articles from substances or mixtures
Production, processing and distribution of food	Food businesses engaged in wholesale distribution and industrial production and processing
Manufacturing of medical devices and in vitro diagnostic medical services; computer, electronic and optical products; machinery and equipment; motor vehicles, trailers and semitrailers; and other transport equipment	Entities conducting any economic activities referred to in section C, divisions 26–30, of Statistical Classification of Economic Activities in the European Community (NACE) Rev. 2[a]
Digital providers	Providers of online marketplaces, online search engines and social networking services platforms
Research	Research organizations

Source: a) Eurostat, *NACE Rev. 2: Statistical Classification of Economic Activities in the European Community*, Luxembourg, 2008, *https://ec.europa.eu/eurostat/documents/3859598/5902521/KS-RA-07-015-EN.PDF*

Enterprises may find it difficult to determine the severity of incidents and classify them correctly to meet the directive's reporting timelines and other requirements.

The requirements of the directive may be complex and challenging to implement and may require considerable time, effort and resources, including cybersecurity, legal and regulatory expertise. Enterprises may face resource constraints that hinder their ability to implement the NIS2 Directive,[8] including budget limitations, lack of skilled cybersecurity personnel and inadequate technology infrastructure. In addition, enterprises may need to navigate complex legal and regulatory frameworks at the national and EU levels involving specific industry sectors, geographic regions and legal environments. The NIS2 Directive also requires interactions with multiple stakeholders, including regulatory authorities, industry regulators and law enforcement agencies. Managing these interactions, coordinating incident notifications, and ensuring compliance with varying requirements can be challenging, particularly for enterprises operating under several different authorities.

Noncompliance with the NIS2 Directive can have profound consequences, including fines, penalties and reputational damage. Devoting the significant effort and resources required to address these new requirements may be difficult, but EU member states must establish effective, proportionate and dissuasive sanctions for noncompliance. Enterprises that cannot comply with the incident notification requirements may face financial penalties of up to EU€10 million or 2 percent of worldwide annual turnover, whichever is higher. Repeat or serious noncompliance may lead to fines of up to EU€20 million or 4 percent of worldwide annual turnover, whichever is higher.

Complying with the incident notification requirements of the NIS2 Directive may also pose challenges for OESs and DSPs, including the need for effective incident response plans, and communication protocols to ensure the timely and accurate reporting of incidents. Enterprises may find it difficult to determine the severity of incidents and classify them correctly to meet the directive's reporting timelines and other requirements.

The NIS2 Directive mandates that enterprises share sensitive information about incidents and security measures with relevant authorities, which may raise concerns about data privacy, confidentiality and potential legal liability. Enterprises must navigate data privacy considerations, such as compliance with the EU General Data Protection Regulation (GDPR), when sharing incident-related information, which can complicate compliance efforts.

The NIS2 Directive has an extraterritorial reach and applies to various sectors, including OESs and DSPs. Even non-EU enterprises may be subject to its requirements if they provide services to EU-based enterprises or citizens.[9] Like the GDPR, the NIS2 Directive is important for enterprises operating outside the European Union that deal with enterprises within the European Union or that provide services to EU citizens. For example, the directive has important implications for enterprises operating in the ecommerce and digital marketing sectors, where cross-border transactions are common. These enterprises must comply with the requirements of the NIS2 Directive, even if they are not physically located within the European Union. OESs, DSPs and other enterprises inside and outside the European Union may have diverse levels of cybersecurity maturity, varying sizes and different operational complexities, making it difficult to achieve consistent compliance across such a diverse organizational landscape.

Best Practices for Incident Notification and Compliance

Enterprises need robust incident response processes and protocols to ensure quick incident responses and adherence to notification timelines. However, they must take proactive measures to address these issues, including allocating adequate resources, obtaining legal and regulatory guidance, building cybersecurity expertise, and fostering an organizational culture of compliance.

Despite the NIS2 Directive's novelty, enterprises can still rely on existing incident notification and compliance practices. Foremost are proper technical and organizational security measures to prevent, detect and proactively and regularly respond to cybersecurity incidents. These technical measures may include firewalls, intrusion detection and prevention systems, security information and event management (SIEM) systems, security monitoring

tools, threat intelligence, and security analytics that can identify and respond to cybersecurity incidents in real time. Organizational measures include fostering a culture of cybersecurity awareness among all employees, from top management to frontline staff, by promoting cybersecurity best practices, providing ongoing training and education on cybersecurity risk and incident reporting requirements, instituting employee awareness and training programs, and encouraging employees to report any potential incidents they encounter. Another good approach is assigning legal or compliance staff members to regularly review relevant legislation, guidance documents and industry best practices and to incorporate any necessary changes into incident response plans and procedures. Enterprises must also have strong vendor management practices, including conducting due diligence on vendors' cybersecurity practices and incident reporting capabilities and reviewing contracts to ensure that they require early notification of any cybersecurity incidents that may affect the vendors' services.

An effective incident response and escalation plan should outline the roles and responsibilities of the incident response, management, legal and communication teams and the procedures for detecting, responding to and reporting cybersecurity incidents. This plan should be reviewed, updated and periodically evaluated to ensure its effectiveness, especially during enterprise IT environment changes. Performing simulated incident response drills can identify gaps or weaknesses in the incident response plan that could be devastating in the event of an incident.

This plan should also contain clear communication protocols to ensure that DSPs, OESs and other enterprises report incidents accurately and promptly to the competent authority. It must include designated points of contact, communication channels and escalation procedures to ensure that incident reports reach the proper authority within the allotted time.

Enterprises should provide staff with regular training and education on the criteria for determining the severity of incidents, the information they must include in incident reports, and the timelines for reporting. Staff members should be able to identify and report incidents promptly and accurately, and to comprehensively analyze cybersecurity incidents, including root causes, impacts and lessons learned. In addition, enterprises should maintain accurate and up-to-date documentation and records of all incidents, including initial and final reports, and any relevant technical and organizational security measures in place. These records can indicate compliance with the NIS2 Directive and demonstrate an effort to comply with incident notification requirements. Equally important, enterprises should stay updated on the latest regulations and guidelines related to incident notification, including any updates or amendments to the NIS2 Directive.

Organizations should conduct thorough postincident analyses to identify incident response processes in need of improvement. They should incorporate lessons learned into updated incident response plans and procedures. Likewise, OESs and DSPs should conduct regular penetration testing and vulnerability assessments to identify and address any system and network vulnerabilities or weaknesses.

Conclusion

The NIS2 Directive is a legal instrument that guides the improvement of cybersecurity practices in the European Union. It sets specific cybersecurity requirements for DSPs, OESs and other enterprises that are vital in ensuring systems' and users' continuity, safety and security. It serves as a framework for establishing comprehensive and consistent cybersecurity practices across the region, aiming to prevent and combat cyberthreats and cyberattacks and promote a culture of cybersecurity awareness and best practices.

DSPs, OESs and other enterprises must recognize the importance of complying with the NIS2 Directive. Compliance with its incident notification requirements is crucial to avoid severe consequences such as economic loss, reputational damage and legal liability. Enterprises must establish robust incident response plans, foster cybersecurity awareness and implement effective communication protocols. Regular drills and simulations, continuous monitoring and detection of incidents, clear incident escalation processes, and thorough postincident analysis and improvement are essential steps toward compliance. In addition, it is important to regularly review and update incident response plans to align with emerging threats and best practices.

Compliance with the NIS2 Directive will help DSPs, OESs and other enterprises improve their cybersecurity measures and reduce the risk of cyberthreats and cyberattacks by enhancing their cybersecurity postures and protecting their critical infrastructure and digital services. Taking proactive steps to manage cybersecurity incidents and protect digital assets effectively ensures resilience in the face of growing cyberthreats. Organizations should consider an ongoing process that requires continuous attention and adaptation. However, implementing the NIS2 Directive may present challenges, such as allocating adequate resources, obtaining legal and regulatory guidance, building cybersecurity expertise, and fostering a culture of compliance. The NIS2 Directive is crucial for enhancing cybersecurity practices in the European Union and globally, and compliance with its incident notification requirements can better safeguard critical infrastructure and digital assets, contributing to a safer digital environment for everyone.

The NIS2 Directive is crucial for enhancing cybersecurity practices in the European Union and globally, and compliance with its incident notification requirements can better safeguard critical infrastructure and digital assets.

Endnotes

1 Chatain, B.; "Cybersecurity: Parliament Adopts New Law to Strengthen EU-Wide Resilience," European Parliament News, 11 October 2022, *https://www.europarl.europa.eu/news/en/press-room/20221107IPR49608/cybersecurity-parliament-adopts-new-law-to-strengthen-eu-wide-resilience*

2 Persoff, S.; S. Phillips; H. Ovaisi; R. Flakoli; *NIS2 Directive: Europe Revamps Its Cybersecurity Framework,* Clifford Chance, United Kingdom, November 2022, *https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/11/nis-2-directive-europe-revamps-its-cybersecurity-framework.pdf*

3 Wulff, F. G. H.; "NIS2.0—EU's New Network and Information Security Directive (Explained)," Tricent Blog, 12 December 2022, *https://www.tricent.com/blog/nis2*

4 International Association of Privacy Professionals (IAPP), "European Parliament Approves NIS2 Directive," IAPP Daily Dashboard, 10 November 2022, *https://iapp.org/news/a/european-parliament-approves-nis2-directive/*

5 Enterprise Defense, "NIS2: How Will It Impact Your Organisation?" 2 February 2022, *https://enterprisedefence.com/blog/nis2/*

6 The European Parliament and the Council of the European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council, 14 December 2022, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN*

7 Barina, E.; "NIS2 Directive: How Will It Affect Companies?" *Blaze*, 6 March 2023, *https://www.blazeinfosec.com/post/nis-2-directive/*

8 Nicaise, V.; "NIS2 Directive: What's Changing?" Stormshield, 26 September 2022, *https://www.stormshield.com/news/eu-nis2-directive-whats-changing*

9 Vladimirova-Kryukova, A.; "The Influence of the NIS2 Directive in and Outside of the EU," ISACA Now, 10 November 2021, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/the-influence-of-the-nis2-directive-in-and-outside-of-the-eu*

Avoiding a Compliance-First Mindset and Choosing a Risk-First Attitude

Compliance is a subset of risk. Failure to comply with standards or laws can involve legal or financial risk, yet it is difficult to identify emerging risk with a compliance-first mindset. For example, as one article notes:

> *When the unsinkable* Titanic *sank in 1912, it was fully compliant with all marine regulations. In fact, it exceeded the number of lifeboats mandated by the British Board of Trade at the time. But when catastrophe struck, the ship was not equipped with enough lifeboats to save all passengers on board. The problem? Management, too focused on meeting compliance, undermined real-world risks. Cybersecurity compliance too is a lot like that. There's a compliance document where every checkmark becomes as valuable as the next checkmark. Security teams develop a kind of checkmark mentality because the end goal is not to be secure but to be compliant.*[1]

Many compliance standards cannot keep pace with new risk scenarios, and many do not rank controls based on risk. In addition, compliance audits are generally based on one point in time, yes or no questions are often the norm, and guidelines may fail to address the purpose of controls.[2] Enterprises that may truly be compliant at the time of audit may lack resilient security controls and still be vulnerable to breach (e.g., Target, Equifax).[3] A compliance-first mindset focuses on implementing regulatory controls and enterprise rules leading to a belief in safety (e.g., the *Titanic*). It may also result in unnecessary expenditures and time spent checking off boxes to meet audit requirements.[4] On the other hand, taking a risk-first approach means an enterprise focuses on policies, processes and controls that protect it while also considering its culture and maturity (**figure 1**).

Toward a Risk-First Attitude

What does it mean to have a risk-first attitude? First, it is important to understand the tone from the top. Cybersecurity management is about reducing risk to an acceptable level. Therefore, a security program must have management buy-in and policies that support management's defined risk tolerance. In practice, the quantification of risk is not well understood because the technical definition of risk may not be management's definition of risk. The US National Institute of Standards and Technology (NIST) defines risk as "The level of the potential impact on an organization['s] operations (including mission, functions, image, or reputation)…assets, or individuals of a threat or a given likelihood of that threat occurring."[5]

Cybersecurity professionals should understand this definition, as it identifies impact categories for organizational operations and the likelihood of an adverse event happening. This can be used to begin the conversation with leaders about how cyberrisk affects the bottom line. Then the risk can be quantified using tools such as Factor Analysis of Information Risk (FAIR), which enables the quantification of risk in financial terms.[6]

Risk assessment is the first step in any risk-aware cybersecurity program. A mature enterprise should

FIGURE 1

A Compliance-First Mindset vs. a Risk-First Attitude

Compliance-First Mindset	Risk-First Attitude
Security controls are not ranked based on risk.	Security controls are ranked on specific risk.
Audits are a point in time.	Compliance standards are part of a continuous risk management program.
Audit controls generally serve to meet regulations (perceived safety).	The compliance program focuses on security controls functioning effectively (risk-aware protection).

KAREN MACDOUGALL | CRISC, CCSP, CEH, CISSP, PCIP, SECURITY+

Has an academic background in finance, computer science and information security. During her 25-year career, she has worked at start-ups, major corporations and in government. Her interests include applying risk concepts to cybersecurity programs and monitoring emerging threats.

also have a continuously monitored risk management program. Policies, procedures and processes should reflect the enterprise's risk appetite. Staff, contractors and third parties that are expected to adhere to administrative controls should also be trained to effectively implement the organization's policies, procedures and processes. The risk management program, in turn, should accommodate changes in risk, technology and emerging threats.

Continuous improvement is important to ensure that risk management strategies and processes address new and emerging threats.

Using Frameworks as Strategic Approaches to ERM

A framework provides a guide to follow when building something according to certain standards. Enterprises can choose from a multitude of risk management frameworks. As is applicable in making any organizational decision, factors influencing the choice of the framework include enterprise culture and the maturity of processes. Senior management buy-in influences the success of the implementation of any framework chosen. As such, the successful implementation of a risk-first attitude depends on the given framework's suitability and implementation in the enterprise.

One important development in the field of enterprise risk management (ERM) is the framework developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). It was first developed in 2004 when internal audit was still a main driver for risk management. It was later updated in 2017 to focus more on strategy and performance.[7]

The five main COSO ERM components are:[8]

1. Governance involves the tone from the top.
2. Strategies to develop a risk-aware culture include policies, procedures and training.
3. Performance involves the quantification of identified risk factors because one cannot manage what cannot be measured.
4. Review and revision are related to risk management monitoring and improvement.
5. Information communication and reporting include continuous monitoring and measurement.

An example of a culture that implements the COSO ERM well is the US Internal Revenue Service (IRS) outlining structure, roles, responsibilities and processes.[9] Its ERM program is considered one of the most mature in the US government because it focuses on addressing threats before they impact the agency,[10] employees have channels to report risk and employees can be certified as risk advocates.[11]

The NIST Internal Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management,* examines two vital but different controls that support ERM: internal controls such as COSO, and security controls. It outlines how lower-level risk reporting can be integrated into organizational processes and decision-making, and it defines an approach using a risk register, which forms the basis for a risk profile to highlight the major risk to be addressed, which then flows into the ERM cycle.[12] The benefits of combining cybersecurity risk with enterprise risk include:

- The board can exercise due care and avoid legal or financial penalties by addressing high-risk vulnerabilities.
- Senior management can achieve the organization's mission through a broadened ERM approach that reduces operational risk.
- Cybersecurity events' impact to financial statements and enterprise objectives can be understood.

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*

For ERM to work successfully, cybersecurity risk needs to be considered during the ERM process. In addition, continuous improvement is important to ensure that risk management strategies and processes address new and emerging threats.

To implement NIST (IR) 8286, a risk management framework is needed to determine risk response strategies, and a risk profile should be developed to inform and communicate leadership decisions.

Conclusion

Moving from a focus on compliance to developing a risk-first attitude results in improved security with a better understanding of and ability to mitigate potential threats; better decision-making by addressing likely cybersecurity threats; and senior management's support and investment in security controls that reduce risk.

Moving from a focus on compliance to developing a risk-first attitude results in improved security with a better understanding of and ability to mitigate potential threats.

Endnotes

1 Sjouwerman, S.; "Five Reasons Why Compliance Alone Is Not Efficient at Reducing Cyber Risks," *Corporate Compliance Insights*, 8 June 2022, *https://www.corporatecomplianceinsights.com/compliance-not-enough-cybersecurity-risk/*

2 *Ibid*.

3 Moldes, C.; "Compliant But Not Secure: Why PCI-Certified Companies Are Being Breached," *Cybersecurity and Information Systems Information Analysis Center*, 9 May 2018, *https://csiac.org/articles/compliant-but-not-secure-why-pci-certified-companies-are-being-breached/*

4 Hyperproof Team, "When Organizations Take a Risk-First Approach to IT Compliance, They're Better at Avoiding Security Incidents," *Hyperproof*, 24 March 2022, *https://hyperproof.io/resource/risk-first-approach-to-compliance/*

5 Ferraiolo, H.; R. Chandramouli; N. Ghadiali; J. Mohler; S. Shorter; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-79-2 *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, USA, 30 July 2015, *https://csrc.nist.gov/publications/detail/sp/800-79/2/final*

6 FAIR Institute, "What Is FAIR? From a Compliance-Based to a Risk-Based Approach to Cyber Risk Quantification and Operational Risk," *https://www.fairinstitute.org/what-is-fair*

7 Claypole, A.; "The COSO ERM Framework Explained," Ideagen, 3 May 2021, *https://www.ideagen.com/thought-leadership/blog/the-coso-erm-framework-explained*

8 *Ibid*.

9 Internal Revenue Service (IRS), "Part 1. Organization, Finance, and Management, Chapter 4. Resource Guide for Managers, Section 60," Enterprise Risk Management (ERM) Program, USA, 24 February 2021, *https://www.irs.gov/irm/part1/irm_01-004-060*

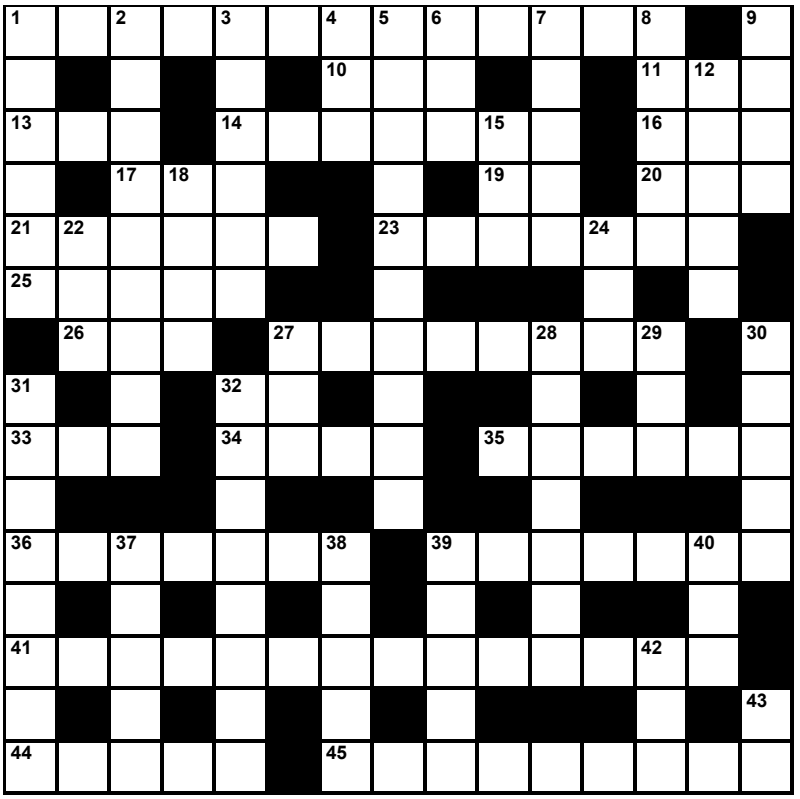
10 Dunkin, R.; "Seven Steps to Create a Risk-Aware Culture," *Treasury and Risk*, 21 September 2020, *https://www.treasuryandrisk.com/2020/09/21/7-steps-to-create-a-risk-aware-culture*

11 Ogrysko, N.; "IRS Launches Designated Channel for Employees to Raise Agency Risks," Federal News Network, 12 November 2019, *https://federalnewsnetwork.com/management/2019/11/irs-launches-designated-channel-for-employees-to-raise-agency-risks/*

12 Stine, K.; S. Quinn; G. Witte; R. Gardner; National Institute of Standards and Technology (NIST) Internal Report (IR) 8286 *Integrating Cybersecurity and Enterprise Risk Management*, USA, 13 October 2020, *https://csrc.nist.gov/publications/detail/nistir/8286/final*

CROSSWORD PUZZLE

By Myles Mellor
www.themecrosswords.com



ACROSS

1. Essential factor in the face of cyberattacks: teamwork
10. Atomic energy unit
11. It is strummed at luaus
13. Co. name ender
14. Changed
16. Organizational culture in an enterprise
17. Tease
19. Branch of computer science, abbr.
20. Bar staple
21. Gets around
23. Temporary suspension of computer operations
25. Locations
26. Access numbers
27. Period during which an organization or part of it is inoperational
32. Prefix meaning mutual
33. Watch closely
34. Back
35. Crafty and smart
36. Copies of data in separate storage devices, 2 words
39. Creative and unrestrained, as in _____ _____ thinking, 2 words
41. Defining capability or advantage that distinguishes an enterprise from its competitors, 2 words
44. Noisy public fight
45. Negotiator's look, often; 2 words

DOWN

1. Major emergencies
2. Profitable
3. Proverbs
4. Mine vein
5. Malicious software that involves extortion
6. Include
7. One of the top outsourcing providers worldwide
8. Remind
9. Average
12. Filled-dough snack
15. Bother, with "at"
18. Arabian port city
22. Big shot, briefly
24. Sweet stick
27. Anonymous litigant
28. Done by company staff, not external personnel, 2 words
29. Watch
30. Unclear
31. Hiccups in a business project
32. Give up, 2 words
37. Ahead of the ___ (faster than the competition)
38. Put in a nutshell, 2 words
39. Fold under pressure
40. Pivotal
42. Number cruncher, for short
43. "__, myself and I"

Answers on page 59

Take the quiz online.

https://bit.ly/3qnRfpU

Based on Volume 3, 2023—Governing the Sustainable Organization

Value—1 Hour of CISA/CRISC/CISM/CGEIT/CDPSE Continuing Professional Education (CPE) Credit

TRUE/FALSE

Moyle Article

1. One limiting factor in meeting sustainability goals is that the effectiveness of environmental, social and governance (ESG) programs depends solely on what items are under an organization's direct control.
2. When automating elements to achieve ESG goals, consistently using the same cloud service provider to run workloads is not necessary.

Liu Article

3. With distributed workforces now commonplace, the most reliable approach to securing user-owned endpoints is IP address-based network access control, which is ideal for mobile workers who need to connect to enterprise networks from a variety of remote locations.
4. Cloud workload protection platforms (CWPPs) tend to be more efficient than other container orchestration systems at preventing malware from spreading between assets because CWPPs provide a graphical user interface (GUI) that more easily enables visualization and control.

Cano Article

5. Relying on a defined risk framework, focusing on competitors' benchmark reports, and examining the approaches others have used to manage risk can be counterproductive, giving adversaries greater leeway in creating attack plans that may evade an organization's defenses.
6. Executives must give up the comfort of standards to determine the right balance between maintaining operations with the fewest possible negative effects and reconfiguring capabilities to adjust to the uncertainties, instabilities and tensions that generate new cyberrisk.

Mazula and Lamprecht Article

7. An effective cloud governance strategy should consist of a variety of implementation approaches tailored to organizational divisions or business units because it is necessary to apply different principles to mitigate different types of risk.
8. One of the main advantages of a cloud-hosted governance framework is that enterprises are relieved of responsibility for monitoring the risk mitigation systems and controls of their cloud service providers.

Cheng Article

9. While fostering internal collaboration is important for the enterprise, it is advisable to strictly limit the sharing of threat intelligence and incident information with other businesses or government agencies.
10. It is possible to measure collaboration within an enterprise and to track behaviors that contribute to a healthy collaborative culture.

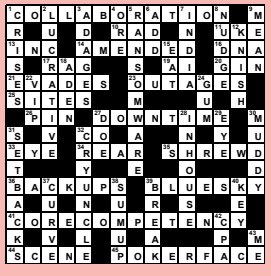
Axelrod Article

11. Even the most advanced artificial intelligence (AI) systems currently available are unable to combine the functions of different lobes of the brain and are, thus, unable to emulate multiple processes in a complex manner.
12. Less autonomous systems are more trustable than fully autonomous systems due to their relative transparency, which makes it easier to predict their behavior under different sets of conditions.

Bryant and Esteban Article

13. Although there is little business value to be derived from investments in data protection and information governance, avoidance of fines is motivation enough for enterprises to place compliance high on their priority lists.
14. It is possible for organizations with remote and hybrid workforces to track data flows, prevent data leakage, and establish practices for appropriate data categorization and retention through well-managed governance controls.

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



ADVERTISERS/WEBSITES

AUDITBOARD	*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

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

Introduction to Digital Trust Online Course

Online Course – Member Free/Non-member $79

Digital trust is central to every digital interaction. In today's world, people are more connected than ever before. The Internet has brought more opportunities to exchange ideas and information within our neighborhood and across the globe. Customers can purchase goods online and receive them the same day. Technology works in the background to support these interactions and transactions between individuals, enterprises, and external parties.

This introductory course breaks down the definition, value, and foundations of digital trust to help learners better understand how technology fully impacts their daily lives and the enterprises they support. Those who participate in this virtual, self-paced course will gain a holistic understanding of digital trust. At the end of this course learners should be able to:

- Define digital trust.
- Explain the value and impact of digital trust on various relationships.
- Describe the role of ISACA's domains in digital trust.
- Summarize the foundations of Digital Trust Ecosystem Framework.

Learners will have access to the course for one year from the date of purchase and will earn 1 CPE upon completion. This course has a seat time of approximately 60 minutes.

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

Digital Resource – Member Free/Non-member $49

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

CRISC Questions, Answers & Explanations Database – 12 Month Subscription

Online Interactive Tool – Member $299/Non-member $399

CRISC® Questions, Answers & Explanations Database—12 Month Subscription is a comprehensive 600-question pool of items that contains the questions from the CRISC® Questions, Answers & Explanations Manual, 6th Edition. The database is available via ISACA PERFORM, a web-based learning platform, allowing CRISC candidates to log in at home, at work or anywhere they have Internet connectivity.

Exam candidates can utilize an interactive planner to build a custom study plan, and a personalized dashboard serves as the primary method to navigate studies and track progress. Candidates will be presented with randomly selected practice question sets and be able to view the results by job practice domain, allowing for concentrated study in particular areas. Each question-and-answer set includes in-depth explanations for each answer choice, allowing the learner to fully understand the rationale behind each correct—and incorrect—answer choice.
Learners will have the ability to review previously answered questions, allowing CRISC candidates to identify their strengths and weaknesses and focus their study efforts accordingly. Other features of the database include:

- The ability to select practice question sets by specific domain and sub-category and choose the length of study sessions, giving learners the ability to customize their approach to fit their needs
- Two full-length timed practice exams intended to mimic the blueprint and feel of an actual ISACA exam and help candidates manage their time when answering questions
- Flashcards and interactive games to help reinforce key terms and concepts

CRISC Review Questions, Answers & Explanations, 6th Edition

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

The *CRISC Review Questions, Answers & Explanations Manual, 6th Edition* has been expanded and updated to include even more practice questions. This study aid is designed to familiarize candidates with the question types and topics featured in the CRISC exam with the use of 600 questions.

Many questions have been revised or completely rewritten to be more representative of the current CRISC exam question format, and/or to provide further clarity or explanation of the correct answer. These questions are not actual exam items but are intended to provide CRISC candidates with an understanding of the type and structure of questions and content that have previously appeared on the exam.

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

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.

Order online at www.isaca.org/resources

Train Your Way with ISACA's Online Courses

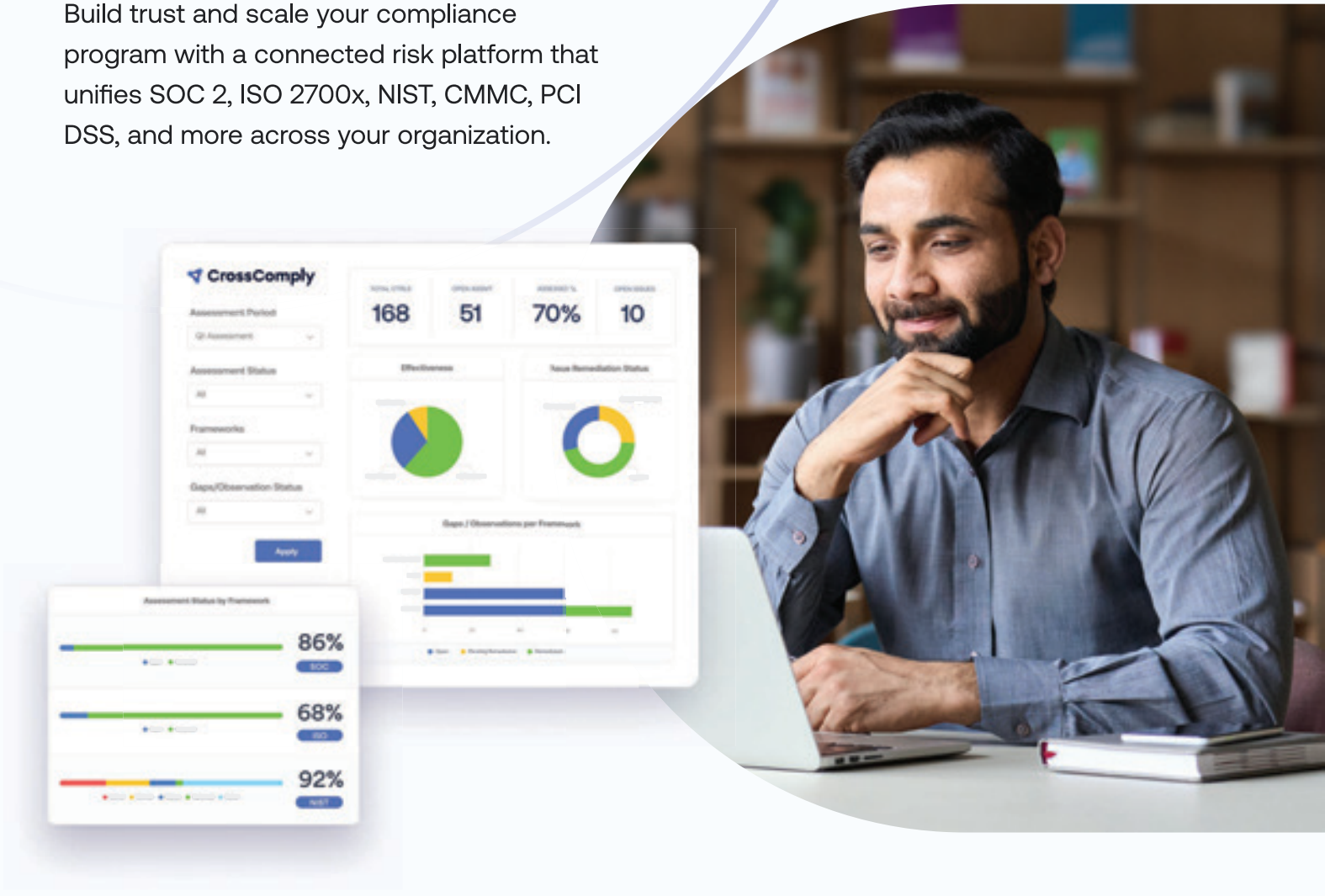
ISACA's wide range of flexible course options coupled with around-the-clock access to course materials empower professionals like you to grow their knowledge and skills in a way that fits their schedule and career goals.

Explore ISACA's training options today, earn CPE credits and start the journey to advancing your career at **www.isaca.org/tyw-jv5**

ISACA

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 ★★★★★

Capterra ★★★★½