GLOBAL PERSPECTIVES & INSIGHTS

Cybersecurity in 2022

PART 1: How the New SEC Proposals Could Change the Game

PART 2: Critical Partners — Internal Audit and the CISO

PART 3: Cyber Incident Response and Recovery

The Institute of Internal Auditors

CONTENT

Part 1:

How the New SEC Proposals Could Change the Game

About the Experts

Andy Watkin-Child

Watkin-Child is a 20-year veteran of cybersecurity, risk management and technology, and co-founder of The Augusta Group, a solutions provider for the management, oversight, and assurance of cybersecurity and cyber risk. He has held international leadership positions in 1st and 2nd Lines of Defence (LoD) for cybersecurity, cyber-risk management, operational risk, and technology, working with leadership teams of companies with balance sheets over €1 trillion across the engineering and manufacturing, financial services, and publishing and media industries. He is an experienced member of management boards, global risk leadership teams, and cybersecurity, operational risk, and GDPR committees.

Manoj Satnaliwala

Satnaliwala is chief audit executive and SVP of internal audit for Caliber Home Loans and is responsible for all audit activities, working directly with the audit committee. Prior to his current role, he led the audit function for Radian Group Inc., the third-largest publicly traded mortgage insurer in the United States, and was a director of internal audit for PwC, where he managed the validation of controls for internal audit as part of the CCAR project for a large bank holding company.

Introduction

New regulatory proposals could have huge implications

The news cycle in 2022, and in fact, the last several years, has seen little positivity, and cyber threats have loomed large in a mix that includes the Ukraine crisis, persistent COVID-19 threats, and growing U.S.-China tensions. Together, these variables and more have combined to give cybersecurity a significant — and indeed a leading — spot on internal auditor risk maps.

However, 2022 has also seen cybersecurity-related developments that promise to impact a broad spectrum of organizations, will require more effort to understand, and whose implications will take time to fully grasp. Chief among these are two regulatory proposals from the U.S. Securities and Exchange Commission (SEC). The second proposal is particularly worthy of note because it would require publicly traded businesses that operate in the U.S. to disclose their cybersecurity policies, procedures, and governance strategies, as well as the board's knowledge and experience — if any — in the cybersecurity realm. If implemented (as they are likely to be in some form), publicly traded organizations, regardless of industry or size, will be subject to these new rules. Without hyperbole, these developments represent a new chapter for cybersecurity and a new — if familiar — topic for the internal audit community, which will play a critical role in navigating their organizations through this challenge.

Although this is not a challenge to be taken lightly, internal audit fortunately understands the tools and skills it needs to provide assurance over this evolving risk area. Part 1 of The IIA's three-part Global Knowledge Brief series on cybersecurity presents an overview of the new SEC proposals, including the implications they have for cybersecurity reporting regulation in the U.S. as well as abroad. It also explores how internal auditors can play an important role in helping their organizations manage an altered compliance landscape that new regulations could soon create.

Setting the Stage

Cybersecurity dominating the risk landscape

The top risk of our time

Cybersecurity remains top of mind at all levels of all organizations in all industries in 2022, and that concern is clearly reflected in data from The IIA's *2022 North American Pulse of Internal Audit* (*Pulse*)[1]. When asked to rate the level of risk for their organizations among 13 major risks, internal audit leaders responding to the Pulse survey ranked technology-related risks among the top three — cybersecurity, IT, and third-party relationships (which often include IT services). Even among these top three, cybersecurity easily took the top spot, with 85% of respondents rating it as a high or very high risk, 24 percentage points higher than ratings for IT, the second-highest-rated risk.

Such concern is warranted. In 2021, cyberattacks of nearly every kind increased by alarming margins. According to the *2022 SonicWall Cyber Threat Report*[2], the number of encrypted threats in 2021 spiked by 167% (10.4 million attacks), ransomware rose by 105% (623.3 million attacks), cryptojacking (attacks on computers to mine cryptocurrency) rose by 19% (97.1 million attacks), intrusion attempts rose by 11% (5.3 trillion attacks), and malware directed at the Internet of Things (IoT) rose by 6% (60.1 million attacks).

What's more, all these attacks carry a significant cost for the damage they inflict. The total annual costs of cyberattacks are expected to reach $10.5 trillion by 2025, an average growth of 15% year-over-year, according to the latest version of Cisco/Cybersecurity Ventures' 2022 Cybersecurity Almanac[3].

And this doesn't even factor in the dramatic changes to the geopolitical landscape that impact cybersecurity. Even before Russia's invasion of Ukraine, there was ample evidence that suspected state-sponsored cyberattacks, with high levels of sophistication, were increasing in impact and frequency. The 2020 breach of Texas-based SolarWind's systems, which was conducted by a hacking group reportedly[4] directed by the Russian Foreign Intelligence Service, saw the digital infrastructure of up to 18,000 customers[5] — including Microsoft, Cisco, Intel, Deloitte, parts of the Pentagon, the U.S. Department of Homeland Security, the Department of Energy, and the National Nuclear Security Administration — compromised and undetected for months.

In 2021, another major suspected state-sponsored attack on a U.S. company was seen on the Colonial Pipeline Co.[6] The attack temporarily disrupted the flow of nearly half the gasoline and jet fuel supplies to the East Coast. Ultimately, Colonial paid a ransom of nearly $5 million to hacking group DarkSide to restore the network and recover the data.

---

[1]. The IIA, *2022 North American Pulse of Internal Audit*, March 2022, https://www.theiia.org/en/content/research/pulse-of-internal-audit/2022/2022-north-american-pulse-of-internal-audit/

[2]. SonicWall, *2022 SonicWall Cyber Threat Report*, 2022, https://www.sonicwall.com/2022-cyber-threat-report/.

[3]. Steve Morgan, "2022 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics," Cybersecurity Ventures, Cisco, January 19, 2022, https://cybersecurityventures.com/cybersecurity-almanac-2022/.

[4]. Joe Hernandez, The Russian Hacker Group Behind the SolarWinds Attack Is At It Again, Microsoft Says," NPR, updated October 25, 2021, https://www.npr.org/2021/10/25/1048982477/russian-hacker-solarwinds-attack-microsoft.

[5]. Isabella Jibilian and Katie Canales, "The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal," Business Insider, updated April 15, 2021, https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

[6]. Andrew Marquardt, "As Biden Warns of a Russian Cyberattack, What Are the Precedents? Here's What Happened When a Major Oil Pipeline Was Hacked Last Year," Fortune, March 22, 2022, https://fortune.com/2022/03/22/biden-warns-russian-cyber-attack-pipeline/.

Geopolitical breaking point

Since these attacks, concerns regarding Russia have only escalated, reaching a peak with the invasion of Ukraine. Indeed, Russia's aggression against Ukraine includes cyber warfare — a large-scale attack on Ukraine's power grid[7] — in addition to traditional warfare, and there is increased concern Russia could retaliate against myriad economic sanctions placed on it by the NATO and the U.S. Just one week before Russia's formal move into Ukraine, the Cybersecurity and Infrastructure Security Agency (CISA) issued a rare "Shields Up[8]" statement warning U.S. businesses of all sizes to adopt a heightened posture regarding cybersecurity and the protection of critical assets. "Recent Advisories published by CISA and other unclassified sources reveal that Russian state-sponsored threat actors are targeting the following industries and organizations in the United States and other Western nations: COVID-19 research, governments, election organizations, healthcare and pharmaceutical, defense, energy, video gaming, nuclear, commercial facilities, water, aviation, and critical manufacturing," CISA wrote in a March 2022 statement[9] assessing Russian cyber threats.

In May 2021, President Biden signed an executive order[10] designed to improve the state of national security in the U.S. The order specifically addressed the need for government agencies to review and develop new guidelines and standards for cybersecurity, and for organizations to focus on enhancing software supply chain security and threat information sharing. More recently, the President also issued a statement reiterating the Russian cybersecurity threat and highlighting CISA's evolving guidance[11] on the subject.

Russia is not the only state actor allegedly backing destabilizing cyberattacks. According to a 2021 report[12] from The Evanina Group, China has become increasingly aggressive on the cyber front, especially in regard to data acquisition of personal information and data privacy.

"China's ability to holistically obtain our Intellectual Property and Trade Secrets via illegal, legal, and sophisticated hybrid methods is like nothing we have ever witnessed," said William Evanina, former director of the National Counterintelligence and Security Center.

Evanina referenced numerous cyber incidents linked to the Chinese Communist Party, including the 2017 Equifax cyber breach; a 2011-2018 campaign by four Chinese nationals to hack into dozens of companies, universities, and government entities; and a 2011-2013 state-sponsored cyber campaign attacking U.S. oil and natural gas pipeline companies (the DOJ released a report on this incident in July 2021). He also referred to a July 2021 report from the National Security Agency (NSA), Federal Bureau of Investigation (FBI), and CISA that released more than 50 cyber tactics and tools used by Chinese state-sponsored hackers against the U.S.

It is in this complex and overall dangerous cyber environment that the SEC has taken historic steps to address cyber health and preparedness across the organizational landscape, particularly in regard to reporting to the SEC and (in some cases) the public. Such steps are the first of their kind and could have significant implications not just for publicly traded U.S. companies but companies across the globe.

---

7. IANS, Ukraine Foils Russia-backed Cyber Attack on Power Grid," April 14, 2022, https://www.nationalheraldindia.com/international/ukraine-foils-russia-backed-cyber-attack-on-power-grid.
8. Cybersecurity and Infrastructure Security Agency (CISA), "Shields Up," accessed April 22, 2022, https://www.cisa.gov/shields-up.
9. Cybersecurity and Infrastructure Security Agency (CISA), "Russia Cyber Threat Overview and Advisories," Department of Homeland Security, accessed April 22, 2022, https://www.cisa.gov/uscert/russia.
10. U.S. General Services Administration (GSA), "Executive Order 14028: Improving the Nation's Cybersecurity," May 12, 2021, https://www.gsa.gov/technology/technology-products-services/it-security/executive-order-14028-improving-the-nations-cybersecurity.
11. Cybersecurity and Infrastructure Security Agency (CISA), "Shields Up."
12. William Evanina, "Statement of William R. Evanina, CEO, The Evanina Group, Before the Senate Select Committee on Intelligence, at a Hearing Concerning the Comprehensive Threat to America Posed by the Communist Party of China (CCP), The Evanina Group, August 4, 2021, https://www.intelligence.senate.gov/sites/default/files/documents/os-bevanina-080421.pdf.

The Big Change

A historic first step toward cyber incident disclosures

The proposals

Within a two-month span, the SEC unveiled two long-anticipated proposals addressing cybersecurity in the business sector. The first proposal[13], revealed in February 2022, focuses on registered investment advisers, registered investment companies, and business development companies or funds. Under the proposed rules, advisers and funds would be required to:

- Adopt and implement written cybersecurity policies and procedures designed to address cybersecurity risks that could harm advisory clients and fund investors.
- Report significant cybersecurity incidents affecting the adviser or its fund or private fund clients to the SEC on a new confidential form.
- Publicly disclose cybersecurity risks and significant cybersecurity incidents that occurred in the last two fiscal years in their brochures and registration statements.

Additionally, the proposal would set forth new recordkeeping requirements for advisers and funds designed to improve the availability of cybersecurity-related information, as well as help facilitate SEC inspection and enforcement capabilities.

"Cyber risk relates to each part of the SEC's three-part mission, and in particular to our goals of protecting investors and maintaining orderly markets," said SEC Chair Gary Gensler in a press release[14]. "The proposed rules and amendments are designed to enhance cybersecurity preparedness and could improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks."

While these rules reflect — if implicitly — SEC expectations for how regulated entities should manage cybersecurity risks and report cybersecurity incidents, the second proposal makes such expectations explicit. Directed at all publicly traded companies, the second proposal[15], issued in March 2022, seeks to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934." To do so, the new rules would require public companies to provide disclosures regarding:

- The company's policies and procedures to identify and manage cybersecurity risks. Included with the rules is an extensive but non-comprehensive list of risk management strategies, policies, and procedures that may be subject to disclosure, including:
    - Whether the registrant has a cybersecurity risk assessment program.
    - Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program.

[13]. U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies," February 9, 2022, https://www.sec.gov/rules/proposed/2022/33-11028.pdf.
[14]. U.S. Securities and Exchange Commission (SEC), "SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds," press release, February 9, 2022, https://www.sec.gov/news/press-release/2022-20.
[15]. U.S. Securities and Exchange Commission (SEC), "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," March 9, 2022, https://www.sec.gov/rules/proposed/2022/33-11038.pdf.

- Whether the registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider.
- Whether the registrant undertakes activities to prevent, detect, and minimize the effects of cybersecurity incidents.
- Whether the registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident.
- Whether previous cybersecurity incidents have informed changes in the registrant's governance, policies and procedures, or technologies.
- Whether cybersecurity-related risks and incidents have affected or are reasonably likely to affect the registrant's results of operations or financial condition.
- Whether cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation.

- Management's role in implementing cybersecurity policies and procedures, including:
  - Whether certain management positions or committees are responsible for measuring and managing cybersecurity risks.
  - Whether the registrant has designated a chief information security officer or someone in a comparable position.
  - Whether processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents.
  - Whether such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risks, as well as how frequently they report.
  - Whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks.
  - Whether the board is informed about cybersecurity risks and the frequency of its discussions on such risk.
  - Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

- The board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risks. This includes information on:
  - Whether the board has work experience in cybersecurity.
  - Whether the board has obtained a certification or degree in cybersecurity.
  - Whether the board has knowledge, skills, or other background in cybersecurity.

Additionally, the proposal includes an amendment to Form 8-K, which would require public companies to disclose cybersecurity incidents within four business days, just as they are already required to do for any other unscheduled material event. Such disclosures would include:

- When the incident was discovered and whether it is ongoing.
- A brief description of the nature and scope of the incident.
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose.
- The effect of the incident on the company's operations.

- Whether the company has remediated or is currently remediating the incident.

These disclosures, according to the SEC, would provide investors with "consistent, comparable, and decision-useful" information. "Today, cybersecurity is an emerging risk with which public issuers increasingly must contend," said Gensler[16]. "The interconnectedness of our networks, the use of predictive data analytics, and the insatiable desire for data are only accelerating, putting our financial accounts, investments, and private information at risk. Investors want to know more about how issuers are managing those growing risks."

The historical significance

In many ways, the structure of these described rules mirrors other SEC disclosure rules, such as those related to financial conditions and operating results (Sarbanes-Oxley), insider information, and organizational strengths, weaknesses, opportunities, and threats. However, taking the additional step of elevating cybersecurity risks to point of necessitating such disclosures is largely unprecedented.

"The U.S. is probably the first country, and I would say only country, in the world to regulate cybersecurity," says Andy Watkin-Child, founding partner of The Augusta Group and Parava Security Solutions, and the founder of Cybersecurity Maturity Model Certification Europe (CMMC Europe). "Companies in the U.S. may be familiar with the EU's General Data Protection Regulation (GDPR) and may be quick to group these proposals together, but data protection and cybersecurity are two different paradigms. There's a big difference, and other than arguably the Department of Defense (DoD) Financial Management Regulation — which could result in even foreign contractors getting investigated by the Department of Justice for cybersecurity vulnerabilities — there's nothing else like it in the cybersecurity realm."

Watkin-Child also explains how the significance of the new rules could have strong ripple effects abroad. "The Ukraine crisis has proven that cybersecurity is a weapon, and indeed NATO has considered it a degree of operation since 2016," he says. "Cybersecurity is an offensive tool right alongside nuclear weapons. The problem with that is because it's a domain of operation, it poses a grave threat to national infrastructures. The SEC proposal is hitting the big players first — the trading firms — but my belief is that this will hopefully trickle down into organizations beyond SEC purview because the business landscape, as well as the federal landscape, is so intertwined on a global level."

In war, says Watkin-Child, one cannot consider cybersecurity within just a single military; if one ally is vulnerable, that has a direct effect on the entire joint operation. Cybersecurity protection for public — and private — companies is no different. "If American weapons systems can't get hacked while British systems can, there's no point in having protection at all," he says. "There's a reason the [U.S.] president has spoken to NATO regarding, among other things, common cybersecurity standards. It's the right thing to do, because if an entity like Russia uses the business sector to attack power generators, for example, your water, your electricity, your gas, your healthcare — it's all gone."

Such potential consequences are obviously macro in nature, but it is important not to discount organization-level consequences, as well. And despite what one might feel seeing the extensive lists of elements that could warrant inclusion in cybersecurity disclosures, not all the consequences are negative.

"Of course, there's the legal side to the disclosures," says Watkin-Child, "But, as it states in the proposals, you're not just reporting to the SEC. You are reporting to all the market participants who might have an impact on your business. The investment community, credit rating agencies, insurance companies — they are all going to see alongside the SEC how good you are at cybersecurity, or not, as the case may be. Such transparency comes with risk, but it also represents an opportunity."

[16]. Gary Gensler, "Statement on Proposal for Mandatory Cybersecurity Disclosures," U.S. Securities and Exchange Commission (SEC), March 9, 2022, https://www.sec.gov/news/statement/gensler-cybersecurity-20220309.

Internal Audit's Role Remains Consistent

Identify, assess, communicate

The tools are in place

The Sarbanes-Oxley Act of 2002 (SOX) provided additional responsibilities and unlocked new opportunities for internal audit functions to add value to their organizations. Indeed, as organizations navigated the new legislation, internal audit to many became synonymous with SOX compliance. Due to the nature of the new SEC proposals, there is cause to believe the same could happen in the realm of cybersecurity.

At first blush, this may seem like at least a short-term impossibility due to the complex nature of the cybersecurity field. According to Pulse survey[17] respondents, cybersecurity makes up on average just 9% of audit plan allocation in publicly traded organizations, which is up from 7% the previous three years but far below the 35% allocated for financial reporting. There are several reasons why this might be, such as budget limitations, lack of sufficient resources, and lack of knowledge or experience.

The real value internal audit can provide, however, is not necessarily through cybersecurity knowledge, but knowledge of risk identification, communication of risk, and the evaluation of controls to address risk. Indeed, these are the very things the SEC proposals wish to emphasize for one specific risk.

"It's important to realize that these proposals are not really about cybersecurity, they are about cybersecurity risk management," says Watkin-Child. "When people think cybersecurity, they all think about implementing controls and fixing stuff. What the SEC is looking for is something completely different; they're looking for organizations to assess their cybersecurity risks. They want boards in organizations to have the governance structures in place to evaluate and assure oversight of their cybersecurity risk management program, whatever form it may take."

"What the SEC wants to see is boards taking responsibility for oversight and assuring the rest," says Manoj Satnaliwala, chief audit executive of Caliber Home Loans, Inc. "The gap isn't really in cybersecurity standards — there are frameworks in existence to guide organizations, such as the NIST Cybersecurity Framework. The real gap is in accountability, which can quickly become a responsibility seesaw."

The role of internal audit can help bring balance to this seesaw. "Boards and management, they need help. Internal audit through assurance ensures accountability and, through enhanced visibility across the organization, promotes shared risk ownership," says Satnaliwala. "The risk is different, but the role of internal audit really remains consistent. Audit functions don't have to start fresh, and it's unreasonable to expect every internal audit shop to be in the nitty-gritty of a cybersecurity program, but in regards to this challenge, it's little more than looking at the SEC proposals and asking, 'What are the SEC's expectations?' As long as there are at least some cybersecurity resources already in place, I don't think any changes are needed in the average internal audit function other than tweaking approaches to ensure proper risk coverage."

However, having access to such cybersecurity resources is often easier said than done. Developing any degree of expertise in cybersecurity through training and certifications will not happen overnight, and especially for small internal audit functions with limited budgets to recruit costly, high-demand talent, options to perform any kind of role beyond process-driven compliance is limited. In these cases, internal audit must have a comprehensive understanding of where the knowledge can best be accessed. This can be:

[17]. The IIA, "2022 North American Pulse of Internal Audit,"

- **Within the organization's own talent base.** Those with experience in a more traditional IT audit capacity often have the knowledge base to complete technical cybersecurity training relatively quickly. Additionally, certain cybersecurity fundamentals can be incorporated into areas such as change management, access controls, IT operations, and disaster recovery, which could reduce the need for outsourcing long term.
- **Through collaboration with both the second line and trusted external audit functions.** While internal audit's independence and objectivity must be maintained in conformance to the *International Standards for the Professional Practice of Internal Auditing* (IPPF), establishing a more collaborative working relationship with relevant functions such as IT can provide auditors with indirect access to technical competencies that otherwise may be difficult or costly to obtain.

Conclusion

Time to prepare

Cybersecurity, as a subject, is always evolving as bad actors continue to innovate in their approaches and companies continue to innovate to thwart them. However, as the history of cybersecurity continues to be written, 2022 will be remembered for the milestones reached in an effort to counteract the dire trends seen across the business landscape. Although the SEC proposals must both complete a 60-day period for comments before official rules are issued, there should be little in the way of surprise for publicly traded companies and their internal audit functions.

Internal audit can and should use the time it has, if it has not already done so, to take stock of the full scope of the assets of its organization that should be accounted for in a cybersecurity strategy. Without that knowledge, internal auditors will find it difficult to assess whether current cyber-related controls, policies, and governance strategies are sufficient. Such assessments are not just important for organizational security purposes, but indeed for the entire market community. The world is becoming more interconnected by the day, and this means responsibilities regarding risks such as cybersecurity are largely shared. After all, as history has shown time and again, the breach of one organization could have a very real impact on the security of another.

A chain is only as strong as its weakest link.

PART 2

Critical Partners — Internal Audit and the CISO

About the Experts

Jerry Perullo

Jerry Perullo is the founder of Adversarial Risk Management, a Cybersecurity Program Strategy and Governance firm enabling growing companies to quickly establish mature cybersecurity programs. Prior to founding Adversarial, Perullo retired as the Chief Information Security Officer of IntercontinentalExchange (NYSE:ICE) after 20 years building and leading the cybersecurity program across a global family of critical economic infrastructure including the New York Stock Exchange. NACD Directorship Certified®, Perullo also served on the Board of Directors of the Financial Services Information Sharing and Analysis Center (FS-ISAC) for 6 years, most recently as Chairman. Perullo also lectures at the Georgia Institute of Technology where he is a Professor of the Practice in the School of Cybersecurity and Privacy and shares his experiences with technology risk leaders via his lifeafterCISO.com podcast.

Hassan NK Khayal, CIA, CRMA, CFE

Hassan NK Khayal is an Internal Audit Manager based in Dubai. Hassan was featured by the Institute of Internal Auditors (IIA) as one of the top 15 under 30 global Emerging Leaders. Hassan holds a BBA, an MBA, and a certificate in Middle Eastern Studies. Hassan is also a CIA, CRMA, and a CFE. Hassan also holds professional certifications in Robotic Process Automation (RPA), Data Analytics, Internet of Things (IoT), Quality Management, Health and Safety, Environmental Management, and Risk Management.

Alan Maran

Alan is the Head of Internal Audit (CAE) at Chewy, Inc. He has been with the company since January 2019. In this role, he is responsible for overseeing the overall Strategic and Execution activities for the Internal Audit Function, including performing Agile enterprise risk assessments, providing continued and timely Advisory support for various activities championed by Management; and Assurance over appropriateness of controls on key risks identified for the organization, alignment with operations, corporate systems and IT governance, risk and compliance (GRC) across the company, continued focus on the development of the Internal Audit Team members, with increased focus on data analytics, cybersecurity, data privacy. Alan is a seasoned Audit executive with more than 22 years of experience in eCommerce, Fintech, Technology and Manufacturing Companies that continues to be passionate about learning. Prior to joining Chewy, he held progressive leadership roles starting his career at Ernst & Young, LLC, and then progressed into other various Internal Audit positions in multi-national, Fortune 500 organizations. He holds an MBA; and a Masters in Finance from Washington State University; is a Certified Fraud Examiner (CFE), a Certified Blockchain Expert, and affiliate with the local Chapters of the Institute of Internal Auditors.

Srini Srinivasan, PMP, CBIP

Srini Srinivasan is the Chief Information Security and Data Officer at Chewy, Inc. He has been with the company since October 2019, when Srini joined as the Head of Security, Data and Corporate Systems. In this role, he is responsible for overseeing information security, management of data and analytics platforms, corporate systems and IT governance, risk and compliance (GRC) across the company. Srini is a seasoned technology executive with more than 25 years of experience that span eCommerce, Banking & Financials Services, Retail and Marketing. Prior to joining Chewy, he held leadership roles at Citizens Financial Group. He holds a master's degree in Computer Science from Bharathidasan University, and an MBA from Bentley University.

Introduction

Cybersecurity partnerships critical to success

Cybersecurity remains among the top risks for all organizations. Surveys consistently reflect unrelenting and brazen efforts by cyber criminals to hack into sensitive data or lure the untrained and unsuspecting into divulging sensitive information or allowing access to bad actors.

For example, the 2022 Verizon Data Breach Investigations Report reflects a startling 13% increase in ransomware-related breaches in 2021, greater than the past five years combined. However, the report finds the most successful methods of ransomware attacks remain consistent — abuse of desktop sharing and remote access software (40%) and email (35%), according to the Verizon report.[18]

New guidance from The IIA, Auditing Cybersecurity Operations: Prevention and Detection (GTAG), is designed to help organizations examine and prioritize assurance over cybersecurity operations. It aims to help internal auditors define cybersecurity operations, identify its components, consider relevant control guidance in IT control frameworks, and understand approaches to auditing cybersecurity operations.

One key to improving cybersecurity assurance not covered in the guidance is having a healthy relationship between heads of internal audit and chief information security officers (CISOs). This potentially symbiotic relationship can help align internal audit and information security on frameworks, risks, and controls while supporting managing the expanding cybersecurity risk profile.

This Global Knowledge Brief examines the benefits of a strong relationship between heads of internal audit and their information security counterparts, looks at paths to establishing and nurturing such relationships while ensuring internal audit independence, and assesses how these partnerships can add value to the organization.

18. "3 Takeaways From the 2022 Verizon Data Breach Investigations Report," J. Mack, Rapid7, May 31, 2022, https://www.rapid7.com/blog/post/2022/05/31/3-takeaways-from-the-2022-verizon-data-breach-investigations-report/.

The Case for Collective Cybersecurity

Cyber risk demands enterprisewide approach

Cybersecurity remains a growing and evolving risk area with each year seeing the schemes of cybercriminals grow more sophisticated and abundant. There is no shortage of statistics to show organizations remain vulnerable to cyberattacks. At the same time, pressure grows for organizations across the industry spectrum to embrace data-driven business strategies that rely heavily on collecting, managing, analyzing, and utilizing data while leveraging new technology to improve performance and the bottom line.

As with other significant risk areas, cyber risk should be understood and managed across the organization. Yet few organizations take an enterprisewide approach to managing cybersecurity, according to "The State of Cyber Resilience", a report from Microsoft and insurance brokering and risk management firm Marsh. Based on a survey[19] of more than 600 cyber risk decision makers, the report found only about 4 in 10 organizations involve legal, corporate planning, finance, operations, or supply chain management in making cyber risk plans.[20]

"One thing holding back confidence is that most companies have not adopted an enterprisewide approach to cyber risk; one that at its core is about broad-based communication and fosters collaboration and alignment between stakeholders during key decision–making moments of truth on their cyber resilience journey,"[21] according to the report.

Among the key risk trends identified in the report:

"Cyber-specific enterprisewide goals — including cybersecurity measures, insurance, data and analytics, and incident response plans — should be aligned to building cyber resilience versus simply preventing incidents, as every organization can expect a cyberattack."[22]

To support an effective enterprisewide approach, heads of Internal audit can contribute significantly by establishing and nurturing relationships with CISOs. Such relationships must be based on mutual understanding, aims, and respect.

Veteran CISO and Adversarial Risk Management founder Jerry Perullo, formally with NYSE-parent Intercontinental Exchange (NYSE:ICE), said poor communications or unclear understandings of information security and internal audit roles can hurt alignment on cybersecurity. Conversely, a good relationship between the heads of internal audit and information security opens the door to a deeper understanding of goals, strategy, operations, and policies that can make internal audit—and by extension its findings and recommendations — more relevant to cyber risk leaders, executive management, and the board, he said. What's more, a strong relationship between internal audit and information security teams expands knowledge of each area's critical mission and how they both support overall cybersecurity.

"At the end of the day, internal audit wants to get educated about information security," Perullo said. "There are many ways to do this, but there's nothing like learning from the (information security) team itself."

In his consulting work with start-ups, Perullo often begins by setting up governance programs for cybersecurity. That typically involves creating a cross-functional cybersecurity governance committee that can include executive management, finance, legal, and information security. They also often include senior internal audit executives as observers, he said.

19. "2022 Marsh and Microsoft Cyber Risk Survey"
20. "The state of cyber resilience," Marsh Microsoft, 2022, https://www.marsh.com/us/services/cyber-risk/insights/the-state-of-cyber-resilience.html?utm_source=forbes&utm_medium=referral-link&utm_campaign=gl-cyber-risk-2022-the-state-of-cyber-resilience.
21. ibid.
22. ibid.

Five Keys to Success

Benefits of a solid internal audit, CISO relationship

Internal audit and CISOs identify numerous benefits of a well-crafted partnership. The details and sophistication of such partnerships can vary depending on the size of the organization, the level of regulation in each industry, or an organization's cybersecurity risk profile. However, five areas emerge where collaboration and cooperation can create clear benefits no matter the size of the organization or the industry in which it operates.

Understanding and aligning on the organization's cyber risk profile

A risk profile is a quantitative analysis of the types of threats an organization faces. From a cybersecurity perspective, such an analysis identifies assets and cyber risks, examines policies and practices designed to manage those risks, and strives to understand any vulnerabilities that may be present. Internal audit's understanding of the cyber risk profile provides a foundation to build an audit plan that not only supports the organization's overall approach to cybersecurity but can also improve internal audit's relevance and value in this critical area.

Alan Maran, head of internal audit at Chewy, Inc., has developed a strong relationship with the organization's CISO, Srini Srinivasan, over the three years since the online retailer of pet food and other pet-related products went public. Srinivasan said information security partnered with internal audit, legal and other stakeholders to comprehensively assess and measure the company's cyber risk profile based on the NIST Cybersecurity Framework.

"That is our baseline," said Srinivasan. "We then set out a three-year roadmap for cybersecurity and governance, and we tailored it and enhanced it based on the cybersecurity framework assessment that we did. We now do an assessment on an annual basis to see if we are making improvements in those areas of opportunity and assess how our overall risk scores measure up."

This collaborative approach involving internal audit from the onset allowed for a mutual strategy that incorporates internal audit assurance and advisory services with the goal of consistently improving Chewy's overall cybersecurity posture.

"It isn't a perspective of, 'I always need to audit IT and security.' We need to also support it," Maran said. "From the internal audit side, we see we are a partner with a strong mentality of supporting Srini and his team into developing a whole strategy."

An added benefit of the collaboration is that information security and independent assurance are being incorporated into new projects early on. In other words, information security, internal audit, and governance controls are no longer afterthoughts, Srinivasan said.

"What we do is, as the project initiatives are getting underway, both our teams are getting involved and partnering with the engineering teams, product teams, the business teams. . . What are the security considerations? Are we following the best practices?" said Srinivasan.

This approach helps identify, minimize, and, if possible, eliminate cyber risks by building appropriate processes and controls as the project is developed, Srinivasan said. "So, when the project goes live, it becomes very easy for both our (teams) because we have a solid understanding. When we follow through with either audit control assessments or access reviews or governance controls, we have a lot more insights."

Understanding roles

The relationship built by Maran and Srinivasan was aided greatly by Chewy being a relatively new publicly traded company, which provided an opportunity to shape the relationship from the ground up. This also set up an expectation of open and frequent communication between Maran, Srinivasan, and their teams.

“It was an ideal way to establish this transparency and trust among the key stakeholders, so we didn’t want to let this opportunity go by,” Srinivasan said.

This is not to say that there are never disagreements. But when conflicts do arise, the relationship makes it easier to debate them and come up with a solution that serves both sides, Srinivasan said.

“There is no benefit for me to keep anything away from internal audit,” he said. “The more that they know about what we are doing . . . the greater level of appreciation they have. In the same way from the internal audit perspective, I can tell you that I think there are no ‘gotchas’ here.”

Ultimately, the collaborative approach allows for operating in an agile fashion where internal audit is part and parcel to a process where deficiencies can be detected and addressed earlier, Srinivasan said.

Maran adds that the frank interplay affirms and reinforces the mutual understanding of roles.

“Srini is not assuming that we know it all, but at the same time, he’s being respectful of our concerns and our point of view,” he said.

Relevance

Providing assurance insights and findings on critical issues at the right time is one of internal audit’s biggest challenges in any risk area, but particularly so for cybersecurity. This ever-evolving and fast-paced risk demands that assurance be relevant and timely.

Perullo warned that internal audit engagements and related recommendations that don’t align to the organization’s cybersecurity mission can do more harm than good. They can create confusion within information security about what internal audit wants to see, particularly if internal audit isn’t sure.

“Internal audit may not initially have a good idea of what it wants to see,” he said. “It’s better to collaborate pre-audit and observe the cyber governance process to ensure audits are aligned with the mission.”

Hassan Khayal, an internal audit consultant with expertise in cyber, said this is an area where internal audit is particularly vulnerable to criticism. Too often, internal auditors resist getting to know members of the IT or information security teams and learning more about the subject under the guise of protecting internal audit independence.

“I shamelessly went with my first assignments and would tell the IT person, ‘Listen, I’m here more to learn from you more than anything else.' I would take the person with the process understanding or the technical understanding and have a friendly lunch conversation so that I got to know exactly the nitty gritty parts of what they’re doing.”

This education process also helps the internal auditor understand the organization’s cybersecurity maturity, which is critical to providing relevant recommendations, Khayal said.

“If you’re talking about the small-to-medium-size enterprise, or even a larger organization that is not publicly traded, then there is only so much you can do or should do,” he said. “At a certain point, recommendations can be too aggressive, so the recommendations you’re making are not realistic.”

Building a strong relationship between internal audit and information security teams reduces the likelihood of irrelevant or misguided audit engagements and recommendations. That benefit has been affirmed at Chewy.

“Alan’s team and Alan himself are very conversant with what is our overall security strategy, from a technology perspective, what are we doing about it, and what are some of our top risks,” Srinivasan said. “So, we don't have the huge gap between the risk ratings and our internal capabilities. This is going to continue to help us do a better job in terms of improving the overall knowledge of our team or our team members at Chewy as well as our leadership team.”

Communicating to the board and executive management

Chewy's organizational culture provides a greater risk view supported by open conversations. Maran and Srinivasan have taken on the roles of educating stakeholders — executive management and the board — about their collaboration and the benefits it has yielded.

"In a lot of organizations out there, people are taking the siloed approach. It's like, 'Oh, it's IT security, so we will talk with the CISO, and the CISO will take care of it.' But within an integrated risk management or enterprise risk management perspective, any risk that we see for the company can come back to the whole enterprise," Maran said. "A cyberattack can impact your operations, your deliverables, and your financials. Srini also has done a good job of educating leadership on what we're doing and on the risks we're mitigating. So, from that perspective, it's been a collaboration."

This also translates into timely and nimble responses to changing risk and regulatory cyber landscapes. For example, Maran and Srinivasan have growing confidence that the organization can respond to the proposed cybersecurity reporting rules from the U.S. Securities and Exchange Commission unveiled in the first quarter of 2022.

That collaboration goes beyond information security and internal audit, as well. "It's not limited to the security of the organization," Srinivasan said. "We have other key stakeholders where we have similar partnerships, including the accounting team and legal team. I think establishing these transparent relationships sets us up very well when these evolving regulations and additional requirements come into the picture."

While Chewy's leadership benefits from consistent and unified messaging, Khayal warns of significant dangers when leadership isn't kept up to date on the organization's cybersecurity status and needs. IT and cybersecurity can quickly become viewed simply as cost centers when leaders aren't informed and educated about it, he said. When internal audit shies away from understanding information security, they are less likely to provide valuable and relevant assurance in this area, Khayal said. This affects views on cybersecurity from the executive management and the board perspective.

Protecting and respecting independence

Khayal, who is working on becoming a certified information systems auditor (CISA), said his commitment to achieve the certification has already boosted his credibility among IT and information security professionals. It also has allowed him to interact with those co-workers at their level, making it more likely they will volunteer information that might be deemed too advanced or complex for an auditor who comes in only when carrying out an audit engagement. What's more, he doesn't see that interaction as a threat to his ability to conduct an independent and objective audit engagement.

"At the end of the day, you are at the workplace," he said. "When we tell auditors to be independent, I personally don't believe that we're telling them, 'You cannot have friends at work; you should always go have lunch by yourself.'"

Khayal said he takes this approach across all areas of the organization. He'll talk Linux with computer staff, or social media with marketing staff.

"It is a good opportunity to develop yourself professionally while maintaining relationships," he said. "It's like when we tell our audit clients or auditees, 'We are looking at the process and the transactions; we're not going after the people.' So, when you take people out to lunch, you're not taking the process or the transaction."

At Chewy, the close working relationship between Maran and Srinivasan supports mutual understanding of the need for independent verification, Maran said.

"The nature of our profession is to trust but verify. From an objectivity standpoint, I have a duty to do that," he said. "So, yes, we trust to a certain level, especially incremental things we have tested. In most cases we validate that things have not changed. But I continue to also test the integrity of the information provided by management. We don't look at a report just at face value; we go back to the source to ensure we are getting the same results as they are to ensure it is complete and accurate."

Ultimately, understanding each other's' role in the organization makes it easier, Maran said.

“There’s an agreement here. Here’s what I need to do. Here’s the assurance I need to provide to senior leadership — the board, stakeholders and to the audit committee,” he said. “We are aligning on the audits we’re going to do for the year. We align on the scope. Yes, we sometimes have conversations about our point of view and how each other sees it, but we rarely disagree in the risk areas we need to provide assurance over.”

Srinivasan adds that the focus on a data-driven approach to cybersecurity assumes there will be agreement on the facts between information security and internal audit.

“If there is any disagreement, we need to work through and get to the same set of facts,” he said. “Then you can have some level of subjectivity that individually we may say, ‘Okay I feel this is medium criticality or high criticality or low criticality’. I think that leads to a healthy discussion and outcome, rather than butting heads without having a common frame of reference.”

Adding Value

Enhancing cybersecurity resilience

Srinivasan said his approach from the onset was to stay true to Chewy's mission. That meant accomplishing three things: practicing the company's internal operating principles, ensuring alignment between information security and internal audit, and building trust through transparency.

"I think we have come a long way, and this is really paying off a lot in terms of what it takes from the team members and leadership to kind of keep each other up to date," he said.

As noted earlier, the high degree of communication, collaboration, and cooperation supports an agile approach that incorporates internal audit in the cybersecurity process continually. Srinivasan notes that major forces, such as the growing focus on sustainability, supply chain considerations, market conditions, geopolitical developments, and more require resilient approaches to cybersecurity and related assurance.

"I think that forces us to be alert and nimble and responsive and relevant," he said. "If we go with a classical waterfall approach with longer lead times, we will miss the boat. So, I'm glad for the level of engagement that we have."

Expanding knowledge

Another intrinsic benefit from the partnership is how both teams have evolved and grown in their understanding and appreciation of each other's approaches to achieving the same goal — keeping the organization cyber-secure.

"We're always checking each other's technical knowledge in terms of, 'Did we look at this? Are you thinking about that? Here's my angle on this risk analysis — does it align with your perspective, as well?'," Maran said. "So, from the get-go we're already thinking about where we will be looking, and Srini is participating in the kickoff meetings. He's in the conversation before we start auditing. There are truly no surprises."

But the real added value comes from the collaboration once audit engagements are executed and internal audit deals directly with IT and security personnel.

"From the career development perspective, especially with IT and cybersecurity mindset, it's actually really rewarding because you do see a lot more than just checking boxes and saying, 'Did you do this?'," Maran said. "There's a lot more. There's interpretation; there's technical expertise that needs to be done right, so I think that's where my team learns a lot."

Conclusion

A healthy relationship between internal audit and information security offers multiple benefits to the organization, primarily in aligning and understanding the organization's cyber risk profile — from vulnerabilities and opportunities to maturity and penetration testing.

What's more, a sound relationship can enhance resilience and agility should the organization need to respond to cyber incidents, changes in factors that influence cybersecurity, or the evolving regulatory landscape. It helps provide consistent and unified messaging to the C-suite and board about cybersecurity risks, needs, priorities, and health. Internal audit independence can be successfully protected, even enhanced, when both sides develop deeper understanding and appreciation of roles, approaches, and duties. Ultimately, a solid relationship between heads of audit and CISOs can strengthen IT security by supporting an enterprisewide approach to cybersecurity.

"The mindset is shifting from simply auditing — 'I need to come in and assess and come in with meaningful observations' — to really saying, 'This is my company; this is what I really care for; and this is how I'm going to help this team to be successful,'" Maran said.

PART 3

Cyber Incident Response and Recovery

About the Experts

Brian Tremblay

Brian Tremblay leads the Compliance Practice at Onapsis, where he is responsible for helping customers understand and navigate the challenges and opportunities created by the increasing overlap of compliance, cybersecurity, and business continuity related to IT general controls and regulatory and compliance matters such as Sarbanes-Oxley (SOX) and the General Data Protection Regulation (GDPR). Prior to Onapsis, he was the CAE for high-tech semiconductor company Acacia Communications. In addition to founding and leading all activities of the internal audit function, he helped prepare the organization to go public (including implementing SOX) and facilitated its implementation of enterprise risk management (ERM). Previously, Tremblay was the Director of Internal Audit at Iron Mountain, overseeing all audits and projects within North America as well as liaising with global quality managers. Prior, as a senior manager at Houghton Mifflin Harcourt, he built out an internal audit department and executed a SOX implementation. Earlier in his career, he worked at Raytheon and Deloitte.

DaMon Ross Sr.

In 2020, DaMon Ross Sr. started Cyber Defense International, where he and his team leverage elite cybersecurity operations and cyber threat intelligence capabilities to deliver affordable cybersecurity solutions and services to organizations that lack the means to build the capabilities themselves. Prior to starting Cyber Defense International, Ross served as the Senior Vice President for Cybersecurity Operations at SunTrust Bank. In this role, he was tasked to create SunTrust's 24/7/365 cybersecurity operations center. As such, Ross built teams specializing in cyber intelligence, cyber threat monitoring, cyber incident response, and cybercrime. Notably, he also successfully partnered with legal, human resources, corporate security, and enterprise ethics and risk partners to establish the bank's first insider threat monitoring program. Ross also facilitated the establishment of numerous information-sharing partnerships, including those with the United States Secret Service Electronic Crimes Task Force and Department of Homeland Security.

Introduction

Back to basics

Cybersecurity has long been a prominent focal point of organizations and their internal audit functions, and with the introduction of the Securities and Exchange Commission's (SEC's) new proposals on cybersecurity risk management, strategy, governance, and incident disclosures, 2022 has been no exception. The impetus for these and other regulatory proposals is warranted. According to a report from the Identity Theft Resource Center, there were 1,862 high-profile data breaches recorded in 2021, a figure that surpassed 2020's total by 68%, as well as the all-time record set in 2017. No industry has been spared from the trend.[23]

In this environment, organizations desire, indeed require, clear, robust cybersecurity controls and processes built on core fundamentals, including continuous learning about the risk and its related regulations, as well as communication and alignment among the board, management, and internal audit. Part 1 of The IIA's three-part series, Cybersecurity in 2022, focuses on potential regulatory impacts, while Part 2 examines the benefits of a symbiotic relationship between chief information security officers (CISOs) and their internal audit counterparts. This final part emphasizes the development and implementation of an organization's cyber incident response strategy, and more specifically, where internal audit can provide organizational value in assessing the controls critical to quickly recovering from a cybersecurity breach.

[23]. Identify Theft Resource Center, "Identify Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," January 24, 2022, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/.

Key Controls

Giving internal audit a role to play in cyber response

The fallacy of incident response

Although the terms "cyber incident response" and "cybersecurity response and recovery" are accurate and useful definers, they also imply a somewhat incomplete view of what such plans require to be effective.

Internal audit in its most essential role provides organizations with independent assurance over risk management. This includes not only assurance for appropriate response to cyber incidents, but also proper evaluation of controls to ensure that the risk and its effects are mitigated or, ideally, prevented. To attain such a lofty standard over any given risk, attention should not just be reserved for simply responding to a risk. Instead, it is more effective to view cyber incident response in a holistic, cyclical manner that prioritizes preventive controls as well as active response measures.

"Risk management is kind of like a wheel," said Brian Tremblay, compliance practice leader at Onapsis, Inc. "At the start of the wheel, we have the right controls, and the processes are what we think they should be. And then, when something happens, the conversation immediately becomes, 'Did the controls perform as expected, and did what we think was going to happen happen?' Then, from there, we learn what needs to change, and the cycle begins again. If the only time you're responding to an event is after the fact, you're likely being inefficient with your time and resources. The present and the future should be granted equal weight because we're not just building the business of today, we're building the business of the future. Since organizations so often struggle with this, this is a really important place for internal audit to focus."

Unchanging fundamentals

Risks seldom become less complex, and because cybersecurity is inherently highly technical, the learning curve to understand both the risk itself and the systems necessary to mitigate it have only grown steeper with every subsequent technological advancement. However, this does not necessarily mean that the fundamental structure of a cyber incident response plan, and the controls within it, change dramatically.

These controls are outlined in The IIA's latest Supplemental Guidance, *Auditing Cyber Incident Response and Recovery*, and can be grouped into four high-level business objectives:

- **Incident Response Planning.** Policies and procedures should be established to guide the determination of whether an incident has occurred and what to do about it. The planning should involve key stakeholders, define roles and responsibilities, and be tested as appropriate to promote awareness and execution.
- **Incident Identification.** Processes to analyze data from detective controls lead to the determination of the existence of a cyber incident, which typically is the trigger for the execution of one or more response plans.
- **Communications.** There are many potential stakeholders in cyber incidents, so each response plan should incorporate a communications strategy for appropriate and timely notification of impacts and resolution efforts.

- **Technical Response and Recovery.** The nature of the incident largely determines the necessary technical remediation and restoration controls, often involving coordination of efforts internally and externally.[24]

Accomplishing these business objectives and adhering to an established cyber incident response framework such as the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity requires technical knowledge relating to implementation, maintenance, and improvement that information security and information technology teams can provide — knowledge that internal audit teams may or may not possess. However, there is simultaneously ample space for others with less technical but equally valuable disciplines to provide significant value. Internal audit, with its unique access to and understanding of organizational functions across all departments, as well as its independent perspective critical to providing objective assurance, is just such a discipline.

"From the internal audit perspective, the approach to cyber incident response is no different from any other risk in that the focus is on the actual process and the output of that process," said DaMon Ross Sr., founder of Cyber Defense International, LLC, and former senior vice president, head of cybersecurity operations at SunTrust. "Even with the technical nature of materials, any internal auditor used to operating in a process space will pick up what matters pretty quickly."

Such a process bears more than a passing resemblance to what internal audit may see in Sarbanes-Oxley (SOX) compliance programs, crisis response plans, or any established risk management strategy. "Different organizations have different terminologies, but a cyber incident plan is essentially a governing policy that outlines when a cyber incident occurs, what all applicable parties' roles and responsibilities are, and who needs to be at the table for decision-making," said Ross.

Tremblay expressed a similar sentiment. Controls relevant to cyber risks are also part of frameworks used to manage compliance risks associated with Sarbanes-Oxley, he said.

For example, one of the first steps hackers take when they break into any technology is to access the necessary rights and privileges to accomplish their objective. In the grand scheme of risk, this falls under the risk of unauthorized access. There is no difference whether that applies to SOX or a cyber risk, Tremblay said. "The risks when boiled down to their simplest forms, and the controls to mitigate those risks, are essentially identical."

Documentation controls

As Tremblay mentioned, the controls that are contained within such a policy also have significant overlap with what can be seen with other organizational risks. One example is having an effective documentation process. Ross agrees. Organizations must understand what workflows look like that properly document cyber incidents, and how all the moving parts running in parallel coalesce, he said.

"This isn't just for big incidents. Every organization should have a function that deals with this day-to-day. Let's say a computer gets malware on it. It's small incidents like that that can turn into bigger incidents, and in the case the worst occurs, proper documentation helps to understand how it escalated. That function is a control in itself."

Detection and physical infrastructure controls

Another critical control, and one that falls under the rubric of unauthorized access risks, is physical infrastructure. Although such controls may not immediately come to mind when discussing cybersecurity, unauthorized access to hard drives or servers where sensitive information is stored was responsible for 10% of all malicious breaches in 2020, costing organizations an average of $4.36 million per breach, according to research from the Ponemon Institute published by IBM Security.

[24]. The IIA, *Auditing Cyber Incident Response and Recovery*, Supplemental Guidance, Practice Guide, https://www.theiia.org/globalassets/documents/content/articles/guidance/gtag/2022/gtag_auditing_cyber_incident_response_and_recovery_final.pdf.

Such infrastructure can include secure server rooms with restricted access, as well as more basic security measures, such as locked doors throughout facilities. While infrastructure security is important, having controls in place to detect and document potentially suspicious activity can be more relevant.

“When I talk about physical infrastructure, I’m not talking about locked doors so much as making sure there is notification and documentation of the action that creates the real risk. It’s like the main course of the meal as opposed to the appetizer,” said Tremblay.

Identifying and providing assurance for such systems falls squarely within internal audit’s established skillsets, said Ross, adding, “Internal audit has the ability to identify systems that are most high risk or critical to the organization’s livelihood. It’s likely, in fact, that internal audit already has these systems identified as part of providing assurance for compliance to federal laws and regulations related to other risks. All that’s needed is to expand that thinking to include new types of provisioning that can offer elevated access.”

Alignment of recovery expectations

Effective documentation in all stages of a cyber incident response plan is critical. Equally critical, however, is the communication of the data such documentation provides and the alignment of organizational detection and recovery expectations.

According to Tremblay, this is one of the largest gaps he has seen in organizations’ cyber response plans — and where internal audit can provide the greatest value. “Internal audit’s role in cyber disaster recovery is two-fold,” he said. “One, make sure the incident exists, and you can prove it exists through documentation or whatever technology or process you use. The second thing, and the thing I don’t see being done enough, is sitting down with all key stakeholders [to determine] what the realistic recovery timetable will be based on the organization’s risk appetite.”

The timetable, said Tremblay, will be established by the ‘owner’ of the application in question in the organization, which could be the CISO, head of supply chain, or any other leader, depending on where the incident occurs. The key for internal audit is to function as the link between that party and all other parties dependent on that application for day-to-day duties.

“For example, the CISO may say that a 48-hour recovery time is acceptable, but if you don’t go to the CFO or other leaders or functions who rely on that technology being up and running and getting their input, you are setting yourself up for a potential mess,” said Tremblay. “For example, the CFO may say that 48 hours is fine, but only if we’re not closing the books. But if we are closing the books, no downtime is acceptable because the organization would have to file an extension, which would look really bad in the public markets.”

Such conversations do not necessarily require one party to override the other. Rather, through such communication, internal audit can broker consensus in line with the organization’s risk appetite. “In cases where discrepancy exists,” said Tremblay, “what internal [audit] can ask is, ‘Is it really worth it to have that happen?’ The CEO might say, ‘Yeah, it is, because it’s going to cost a million dollars to solve that problem.’ What we’re really doing is making sure that the plan has been truly developed around the stakeholders around the technology.”

He continues, “I think this is an area we, as a profession, have not been particularly good at. I think we try to check the box on validating certain things without really saying, ‘Hey, as part of the review of the controls around incident response, we identified a gap in requirements between stakeholders of particular technologies.’ That’s very valid. That’s identifying a previously unidentified business risk that is valuable to the organization.”

Cross-functionality

It is a common misconception that primary ownership of cybersecurity response falls to the CISO and the security team. This is only partially true. While the experience and expertise needed to implement the more technical aspects of a cyber strategy will most likely be found in that department, it is dangerous to assume that the department will have the bandwidth — or the desire — to shoulder the burden on its own.

“Cyber incident response is, at least it should be, a cross-functional process,” said Ross. “The biggest reason for lag time in organizational response times I see is not the information security department itself in terms of knowledge, it’s establishing roles and responsibilities cross-functionally with departments where security is not their primary responsibility. They have other things to do.”

According to Ross, correcting this misconception and fostering the idea of shared responsibility across all stakeholders should be a key area of internal audit focus. “The emphasis doesn’t necessarily need to be on the security team and what they’re doing, but rather on how their process is being supported by other entities across the enterprise that have a stake in it. The security team knows what to do, but they can’t force the IT teams and back-end developers to help in critical ways. There’s a lot of organizational politics involved, and when I was in that position, I found a valuable partner in internal audit. Security teams can’t fight those battles alone. If you can get a somewhat neutral party to help identify where the organization has gaps in the process, it helps everyone.”

A useful strategy for highlighting these gaps and clarifying roles, said Ross, is for internal audit, usually in collaboration with an external consultant, to facilitate tabletop simulations. “Once you have your cyber incident response plan in a place it can be tested, a tabletop simulation brings the CIO, CISO, IT leaders, the CEO, internal audit — all applicable stakeholders — together in a conference room or Zoom call to walk through a plausible scenario. Even without technical expertise, internal audit can facilitate discussion by asking who does what and assessing how those responsibilities align with reality. They could say, ‘At this point, your team should be executing X and Y according to our plan, but in reality, you could be doing Z.’ That’s when you’re going to hear the real dirt. Most organizations have to do them at least once a year, but internal audit should really take charge of these.”

Conclusion

Evolving with the risk environment

Internal audit, by way of its unique place in the organization, deserves a seat at the table when it comes to an organization's cyber incident response plans. But this success does not excuse internal audit from striving for deeper exploration and understanding of cybersecurity. Indeed, in a future that is quickly dispensing with physical infrastructure in favor of cloud-based technology, greater expertise from internal audit will inevitably become necessary and expected.

"When I began my career in internal audit, one of the great selling points was it was a very generalist role," said Tremblay. "You got to see and learn a lot of stuff about a lot of things you don't have to be an expert in. But there has been such a massive shift around technology, I'm starting to wonder if the internal auditor generalist days are numbered. Instead, maybe internal audit will one day become more of a subject matter expert (SME) around things that are inherently critical to organizations. So, instead of having audit teams comprised of 8-10 operational and compliance and financial statement auditors, organizations will have a cybersecurity auditor, one ESG auditor, etc."

Ross agrees. "At a certain point with emerging technology, how do you really understand the gaps in the response process at a deep level if you can't go that deep? You would never really."

There is much that can be achieved with the knowledge and resources at hand, but an exciting and radically new future is coming. Internal audit needs to be a part of it.

Previous issues

To access previous issues of Global Perspectives and Insights, visit www.theiia.org/GPI.

Reader feedback

Send questions or comments to globalperspectives@theiia.org.

About The IIA

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 215,000 global members and has awarded 180,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized as the internal audit profession's leader in standards, certification, education, research, and technical guidance throughout the world. For more information, visit theiia.org.

Disclaimer

Copyright

August 2022

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101