GLOBAL KNOWLEDGE BRIEF

Cybersecurity in 2022

Part 2: Critical Partners — Internal Audit and the CISO

The Institute of Internal Auditors

Contents

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.[1]

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.

1. "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[2] 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.[3]

"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,"[4] 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."[5]

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.

2. "2022 Marsh and Microsoft Cyber Risk Survey"
3. "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.
4. ibid.
5. 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.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 210,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit theiia.org.

Disclaimer

Copyright

June 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