GLOBAL KNOWLEDGE BRIEF

Cybersecurity in 2022

Part 3: Cyber Incident Response and Recovery

The Institute of Internal Auditors

Contents

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.[1]

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.

[1] 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.[2]

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.

[2] 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.

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

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

July 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