As the impact of cybersecurity incidents and data breaches becomes broader and deeper, more organizations are recognizing cyber risk as an enterprise risk and taking corresponding steps to establish appropriate oversight. But as corporate cybersecurity capabilities mature, how have the roles of the board, audit committee, and internal audit changed, and what can they look forward to in the future? According to a new survey jointly conducted by Compliance Week and Mazars USA, while organizational cybersecurity oversight capabilities are maturing, many companies still suffer from a lack of formally assigned roles and responsibilities, and a loosely defined cybersecurity framework.

“Internal audit departments are playing an increasing role in achieving cybersecurity goals, and accomplishing them in different ways. But they need to ensure that their efforts are aligned with their companies’ overall cybersecurity oversight approach,” said Brian Browne, Principal and Cybersecurity Practice Leader at Mazars USA.

“Overall the approach to cybersecurity oversight seems to be taking hold and maturing, but there seems to be a disconnect among the roles, especially when it comes to the three lines of cybersecurity defense,” Browne says. “It is very important to make sure that the cybersecurity conversation is happening at the board or the committee level.” The three lines of cybersecurity defense are defined in The Institute of Internal Auditors (IIA) Global Technology Audit Guide (GTAG), “Assessing Cybersecurity Risk—Roles of the Three Lines of Defense.” The first line of cybersecurity defense consists of business units and cybersecurity teams that manage the processes and controls that are in place to manage cyber risks. The second line consists of risk managers with risk, control, and compliance oversight functions for ensuring that the first line processes and controls exist and are operating effectively. Internal audit acts as the third line of defense, providing senior management and the board with independent and objective assurance of the cyber risk management.
implemented in the first and second lines of defense.

The Compliance Week/Mazars Cybersecurity Oversight Survey polled more than 150 executives responsible for cybersecurity at their organization. The respondents represent a wide variety of industries, with nearly a quarter from financial services, and another 12.5 percent from insurance organizations. The majority of respondents were chief audit executives, chief information security officers, or chief compliance officers.

Nearly 32 percent of respondents said that their audit committee primarily owned responsibility for the enterprise’s cybersecurity oversight, followed by the technology committee (22 percent) and the risk committee (15 percent). Some 10 percent of respondents said cybersecurity oversight was not formally assigned anywhere within the enterprise, which Browne sees as an area of concern.

Nearly 43 percent of respondents said that cyber security is discussed regularly at audit committee meetings as an established agenda item, and another 36 percent said it is not an established agenda item, but it is discussed occasionally. This is an area where the level of dialogue can stand to improve. “More and more, the responsibility for cybersecurity oversight is falling on the audit committee,” Browne says. “It’s the right place in a lot of organizations to talk about cyber risk. While many audit committee meetings have this as a regular agenda item, we should see that continue to grow year over year.”

Roughly 20 percent of internal audit departments perform all of their cybersecurity-related internal audit services themselves; however, almost half (46 percent) co-source these internal audit services with an external provider. What drives co-sourcing, Browne says, is that it allows an organization to marry internal audit organizational knowledge with external cybersecurity expertise to provide senior management and the board with an independent assessment of the effectiveness of management activities in managing and mitigating cybersecurity risks and threats.

Usually, companies turn to external providers because they lack the time/budget, talent, and/or tools assess their cyber risk. This is all fairly normal, Browne says, but he did find it concerning that some 27 percent of respondents said that their cybersecurity was assessed by another internal or external assurance provider (i.e., non-internal audit personnel). “That’s all well and good, but the role of internal audit is to be that third line of defense on cybersecurity and independently assess and report to the board on how the organization is managing its cyber risk,” Browne says. “In a way, you’re saying, ‘somebody else is doing that so we don’t have to.’ In reality internal audit should still be responsible as the third line of defense.”

Nearly 79 percent of respondents said that their internal audit department covered cybersecurity in some way as cyber security was rated a high enterprise risk; some 36 percent also said it came by way of direct board or audit committee request. “That’s good,” Browne says, “because the board is ultimately responsible for overall cybersecurity oversight. The fact that they are asking internal audit to do something there is a good thing. I would hope over time, that number goes even higher.”

But when asked to what degree their organization had adopted the IIA three lines of cybersecurity defense model approximately 60 percent indicated that they have not formally defined or assigned any roles and responsibilities across the three lines. Nearly 21 percent of respondents were not even aware of the three lines of cybersecurity defense, which Browne said was disappointing, but not surprising, given the wider lack of formal assignment of cybersecurity roles and responsibilities.

When asked how their internal audit department independently assesses their organization’s cybersecurity, the most common answers were assessing the cybersecurity control framework such as people, process, and technology (57 percent); assessing the compliance status against one or more regulations or frameworks such as the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, Health Insurance Portability and Accountability Act (HIPAA), or the European Union (EU) General Data Protection Regulation (GDPR) (44 percent); and assessing a specific cybersecurity operational area such as vulnerability management, logging and monitoring, etc. (42 percent).

Only 33 percent of respondents said they assessed asset inventories such as hardware, software, and sensitive data, which is another area Browne says should rate higher, but is not a surprising result, given what he has seen in the field. “Asset inventories are foundational from security perspective, to understand exactly what hardware and software you have deployed in the organization and what sensitive data

“The board is ultimately responsible for overall cybersecurity oversight. The fact that they are asking internal audit to do something there is a good thing.”

Brian Browne, Principal and Cybersecurity Practice Leader at Mazars USA
you have,” Browne says. “Without that awareness, you may not be aligning your cybersecurity protection and detection mechanisms appropriately to effectively manage your risk.”

Browne added that the defined EU GDPR data subject rights will probably drive more attention to asset inventories of personally identifiable data.

When asked to identify their top cyber security threats, the respondents’ most common answers were phishing (63 percent), malware/crimeware (55 percent), and third-party risk (43 percent). This is an opportunity for internal audit to gauge the organization’s overall risk in these areas, especially since things like phishing and malware are what Browne considers the “point of the spear” for much larger cybersecurity issues. “This is an opportunity for internal audit to ask, ‘Do we have the right protection on mechanisms at the perimeter and on user endpoints, so if they do click on a link or open an attachment, there is some countermeasure there to thwart the attack?’” Browne says.

Third-party risk is trending upward, Browne notes, in part because regulators are paying more attention to those risks as well. “Look at the New York cybersecurity regulations,” Browne says. “Regulators are paying more attention because more and more security incidents and data breaches involve third parties. Those all align, so that’s good to see the recognition of that as a risk.”

When it comes to measuring cyber risk programs against a maturity model, some 41 percent of respondents said they leverage the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). Other frameworks were mentioned, but none came close to the prevalence shown for the NIST CSF. “That is the one most people have heard of, and is familiar to them,” Browne says. “The challenge with the NIST is that it is so big, intimidating, or even onerous to implement. Organizations tracking to it need to take the time to understand and tailor that framework to their organization.”

What is surprising, Browne said, was that 25 percent of respondents said they did not track the maturity of their cyber risk program at all. “Talking about the control frameworks that define the people, processes and technology in your organization is key to managing cyber risk on an ongoing basis,” Browne cautions. “If you do not have a framework in place, you are going to be haphazard in your approach to managing your cyber risk, and your results are going to show that.”

Some 31 percent of respondents said they felt the overall maturity level of their cyber security efforts were “managed”—processes were monitored and performance was measured. Results steadily fell from there, with 23 percent saying their programs were defined (processes formally defined with without sophistication or monitoring), 21 percent saying their programs were repeatable (processed follow a recognizable pattern but based on intuition or individual knowledge), and 13 percent saying they were initial (processes are ad hoc and disorganized).

Overall, this shows a trend in the right direction, Browne says, pointing out that the relatively high number of respondents reporting their programs as managed is a very good result, and higher than expected. Only 3 percent of respondents said their programs were optimized—that is, highly refined and automated—which was not a surprise, given that many organizations, once they hit the “managed” level feel they have their risk managed to within an acceptable level.

Perhaps the most telling result was from the survey’s final question, in which respondents noted how much they felt their organization was managing its cyber risk. The majority of respondents (60 percent) said they felt they were keeping up with their level of risk, while 21 percent said they were falling behind. Surprisingly, 19 percent said they were getting ahead of their cyber risk.

“Frankly, I don’t know if I would ever feel comfortable enough to say I am ‘getting ahead’ of my cyber risk,” Browne says. “To say you’re getting ahead, you are truly identifying risks before they’re actually becoming realized. I think that’s a difficult thing to say, and having been in this field for over 25 years, I don’t know if I would ever say I was getting ahead. I am even surprised over that 60 percent of organizations are keeping up with managing their cyber risks.”

Conclusion

The fact that nearly 43 percent companies discuss cybersecurity as an established agenda item audit committee meetings is promising from an oversight perspective, we should see that trend upward moving forward based on the role that many internal audit departments are playing with respect to cybersecurity. In addition, there is much to be gained from
a fruitful partnership between internal audit and external resources when it comes to managing and assessing cybersecurity, Browne says. “From an internal audit perspective, in order to function as the third line of cybersecurity defense, going through some sort of formalized risk assessment method or process to determine your cyber risk and corresponding cybersecurity related audits is really important.”

Once those risks have been identified, Browne says, the decision of how much of the performance of those audits can be handled in-house. “The vast majority of internal audit departments need some external help when it comes to cybersecurity because it’s typically not a core skill set that they are going to maintain as part of their department. That would be the key to providing that third line of cybersecurity defense.”

The complete results for this survey will be published later this year. For additional information on this survey’s results, please contact:

Brian Browne, CISSP
Principal - Cyber Risk
Mazars USA LLP
1 215.292.2222
brian.browne@mazarsusa.com

Bill Mellon, CPA, CRMA
Partner - Governance, Risk and Compliance Services
Mazars USA LLP
1 215.287.0468
bill.mellon@mazarsusa.com

<table>
<thead>
<tr>
<th>Which statement best describes who provides cybersecurity-related internal audit services for your organization?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ANSWER CHOICES</strong></td>
</tr>
<tr>
<td>All cybersecurity-related internal audit services are provided by the internal audit department</td>
</tr>
<tr>
<td>Cybersecurity-related internal audit services are co-sourced between internal audit and external providers</td>
</tr>
<tr>
<td>All cybersecurity-related internal audit services are outsourced</td>
</tr>
<tr>
<td>No cybersecurity-related internal audit services are provided within my organization</td>
</tr>
</tbody>
</table>