Compliance Today - June 2024

Michael R. Rinard II (michael.rinard@mymlc.com) is the Chief Compliance Officer and Chief Legal Officer at Mosaic Health System in St. Joseph, MO.

Have you prepared your board for the next cyberattack?

by Michael R. Rinard II

A hospital system's boardroom has become key to the organization's cybersecurity risk management program. As courts define the governance responsibilities of board members, it is important to assess whether your compliance program is setting the proper controls and providing access to information about the organization's cybersecurity readiness and preparedness. As healthcare becomes more innovative in its delivery of care and more dependent on technology, so does the risk of a cyberattack on its daily operations.

It is common for organizations to believe cyberthreats are the job of the technology security team alone. This could not be further from the reality of the risk. Courts have expanded the responsibility and the role of board members to not only simply be aware of known risks, such as 1996 *In re Caremark* decision,[1] but also be involved in the active monitoring and active oversight of those risks as part of the board members' duty of good faith to the organization.[2] Board members are expected to be actively involved in the implementation and monitoring of the organization's compliance and reporting systems and not merely passive consumers of compliance concerns.[3]

Cybersecurity risk

Trends in healthcare

Healthcare has become a popular target for cybercriminals due to the sensitive nature of the data that it holds and the criticality of the data for operations. "In 2023, the healthcare industry reported data breaches costing an average of $10.93 million per breach — almost double that of the financial industry, which came in second with an average cost of $5.9 million [per breach]."[4] This makes it the 13th year in a row that healthcare leads the highest average per breach.

This risk is much more than simple financial concerns. Consider that many biomedical technologies are linked to the same servers that the rest of the organization uses for normal routine operations. When a cyberattack happens, cybercriminals can shut down medical devices, which impairs the safety of patients who may depend on those devices to survive.

How can board members fulfill their duty of care?

The boardroom is a crucial control in every organization's cybersecurity risk management system. A lack of board member engagement creates an overall weakness in the whole system of cybersecurity preparedness. As economic growth depends more on innovative digital systems, boards may put their organizations at serious risk when they are not engaged in the cybersecurity system of protection. Although courts do not detail what they specifically expect boards to do, the following are some good guidelines for discussion with your board members in board meetings.

Recommendations

One of the most serious hurdles and jobs of the compliance team is helping board members understand that they are critical and significant in the control of the overall system of cybersecurity governance. Although a board member is not expected to be a cybersecurity expert, they are expected to help govern the process and policies that the operations team executes. They should ask questions, become educated about the risks, and ask engaging questions to ensure that the compliance, cybersecurity, and operations team are prepared for the risks that come with running an operation.

The second critical feature for a board to meet its obligations is ensuring a resolute committee is dedicated to privacy and cybersecurity. It is common for privacy and cybersecurity issues to be brought before an audit committee, where it is "squeezed in" to make sure it is discussed. With the limitation of time that meetings have and the immense issues that boards face in healthcare today, it is imperative to have a separate group dedicate their time and report to the overall board the risks, opportunities, and preparedness plans. In addition, the U.S. Securities and Exchange Commission (SEC) released a new rule regarding cybersecurity disclosure and board governance rules.[5] The SEC has required disclosure of material cybersecurity incidents and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations. In addition to disclosure obligations, the SEC has also emphasized cybersecurity experience and expertise of at least one board member on a cybersecurity committee to advise the board.[6] Company annual reports will monitor this reporting under Form 10-K.[7] Although the SEC governs public trading companies, private organizations should expect to see the expansion of these requirements by the U.S. Department of Health and Human Services Office for Civil Rights at some point in the future. It is an opportunity to begin building these processes today and educate on how they improve our readiness for any cyberattacks.

The third critical feature is making sure that hospital operators, compliance professionals, legal professionals, and board members are viewed as part of the cybersecurity team. It is vital that a chief information officer and chief security officer have the support and collaboration of all to ensure they successfully prevent and mitigate attacks. It is easy for members of your organization to believe that the cybersecurity professional has the sole job of protecting digital assets; however, cyber professionals will not only have difficulty becoming effective, but your organization will have difficulty retaining such expertise. Continuity of the program is as essential as establishing one.

Finally, as you are building a cybersecurity committee, make sure that the organization is looking for board members who not only have an interest in the topic but also have some technical background in it. It is expected that private companies will eventually be required to do so, but more importantly, if you have already established such practices if a breach occurs, the likelihood of a massive breach is lower, and any investigation by the government will be mitigated due to having these controls in place. It provides the organization with credibility as well as best practices to mitigate and help prevent such incidents. Not only will it help when the government comes to investigate, but it also helps control cybersecurity insurance costs by being proactive and innovative rather than waiting for a legal requirement to "force" the issue.