WHA WISCONSIN HOSPITAL ASSOCIATION
ADVOCATE. ADVANCE. LEAD.
The Valued Voice

Vol. 67, Issue 21 Thursday, May 23, 2024

Guest Column: Cybersecurity in the Board Room

By Kelsey Haag and Matthew Thompson, M3 Insurance (WHA's Premier Partner)

Today, the IoT (internet of things) is a fundamental part of business operations – are board members having the right conversations around cybersecurity?

Harvard recently surveyed 600 board members with findings that 65% [1] believe their organizations are at risk and 50% [1] feel ill-equipped to handle the risk. Following several high-profile breaches (Change Healthcare, Target, JP Morgan, Anthem), these results aren't surprising. Given our litigious environment and progression in the regulatory landscape, boards and executives should consider cybersecurity as a foundation of the organization. Cyber hygiene is no longer the sole responsibility of the CIO and IT team, moreover the entire executive team and board members must understand the risks associated with a breach and the strategies in place to prevent one.

What is the risk to the board?
"Are we protected?" The answer to this commonly asked question can be murky. Directors and officers have a fiduciary duty of oversight, and if the company has inadequate safeguards, directors could be personally held accountable for damages. Board members are looking for peace of mind that the business's reputation and finances are protected, in addition to their personal liability.

How do we protect our organization – and ourselves?
One effective way to combat the financial risk is transferring the risk to an insurance policy. Depending on the circumstance of the claim, there are two coverages that may come into play: cyber liability and directors & officers (D&O) liability.

There are coverage gaps that exist for the board when comparing D&O vs. cyber liability insurance. Cyber liability is ever evolving, and there is no standardized policy. Cyber policies generally have an exclusion for claims brought against the executive team and board members. Should a cyber breach occur, the actions (or inactions) of the executives and board members might come under scrutiny. D&O will provide protections for both individual directors & officers, along with the entity.

Further, boards should have an understanding that the total cost of a cyber incident is more than just paying a ransom. Ensuring adequate coverage for litigation fees, notification costs, rebuild costs, PR, regulatory fines/penalties and business interruption should be considered when purchasing coverage.

Some considerations board members should keep in mind include cybersecurity updates as a regular topic during meetings, including education to understand the current threats and landscape. The CISO should be reporting to the board on a regular and continual basis.

- Integrate cybersecurity into all aspects of the organization.
- Focus on resilience rather than protection.
- Lead by example in protecting sensitive data.

Industry Insight: Healthcare
Healthcare facilities are attractive targets for cyber criminals for several reasons: size, dependency on technology, and sensitive patient health information (PHI). Medical records are still the most profitable item compared to other data on the black market. A medical record can range from $250-$1,000/record, while a credit/debit card sells on average for $100. (3)

The Office for Civil Rights (OCR) data from 2018 to 2022 shows a 93% increase in reported large breaches (369 to 712), with a 278% increase for large breaches involving ransomware. (2)

From a regulation perspective, there has been a lot of movement. From potential HIPAA updates coming in 2024 and HHS imposing cyber requirements to get payment from Medicare/Medicaid, to states enacting or proposing privacy bills, it's hard to keep up with all the change.

To add, the SEC issued a final ruling on July 26th, 2023, for public companies to disclose their board's cybersecurity experience, governance methods, and details about cyber incidents. While this hasn't hit the private sector yet, it's a leading indicator of what's to come. The FTC is another federal entity that has shown greater interest in directors' and officers' roles in cybersecurity incidents.

In the current state, navigating numerous cybersecurity standards and guidance can create confusion about which practices to prioritize. The HHS has made their focus on cybersecurity clear, creating Healthcare and Public Health Sector-specific Cybersecurity Performance Goals (HPH CPGs), which challenge healthcare organizations to put cybersecurity practices into effect that will have the highest impact on their overall security. "HPH CPGs will include both 'essential' goals to outline minimum foundational practices for cybersecurity performance and 'enhanced' goals to encourage adoption of more advanced practices." (1)

The introduction & increase in utilization of AI further exacerbates the need for boards to be educated and prepared for the emerging technology.

- AI for recruitment
- Wearables
- Robots

Key Takeaways:
High-profile breaches have made cybersecurity top of mind for organizations of all sizes. However, when considering the financial risks that a potential cyber attack poses for an organization, many individuals only think of the cost of paying a ransom. In fact, there could be financial implications for the board of directors as well.

Organizations with boards of directors, especially those in the healthcare industry, should be aware of the risks they are facing regarding cybersecurity. There are ongoing regulatory efforts to make businesses implement cybersecurity measures to receive funding, to disclose their cybersecurity efforts publicly, and to meet industry-specific standards. Boards should have a comprehensive understanding of these regulations and what it means for them and their organizations.

Reach out to your M3 team to discuss your current protection for your organization and your board, and to learn more about cybersecurity risk management and risk transfer strategies.

References:

1. *1. https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity*
2. *2. https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf*
3. *3. https://405d.hhs.gov/Documents/HICP-Main-508.pdf*

Other Articles in this Issue

- DWD and Tech College Leaders Join WHA Council on Workforce Development
- WHA Foundation Board of Directors Approves New Area of Funding to Support HOSA Wisconsin
- Guest Column: Cybersecurity in the Board Room
- 2024 WHA Silver Level Corporate Member Feature: The MedPro Group Presents Risk Management in Health Care
- WHA Information Center Data Spotlight: May is Mental Health Awareness Month