Williams Overman Pierce, LLP
Certified Public Accountants and Consultants

Elevating Cybersecurity to the Board – Questions Boards Should Be Asking

The board's role in the oversight of organizational risk is increasingly complicated by cybersecurity concerns. Directors need to maintain continual knowledge about evolving cyber issues and management's plans for allocating resources with respect to the preparedness in responding to cyber risks. Such knowledge helps boards assess the priority-driven and investment decisions put forth by management needed in critical areas.

We have prepared the following compilation of critical questions that boards and management should be considering with respect to mitigating cyber security risk for their organizations. Questions contemplate the general to the specific, with concentrations on strategy, organizational risk profile, cyber maturity, metrics, cyber incident management and resilience, and continuing education. These questions may be useful as a starting point for boards to use in their discussions with and in the oversight of management's plans for addressing potential cyber risks.

General

- What are the potential cyber threats to the organization?
- Currently, do boards feel they are adequately up to speed on cybersecurity issues impacting their organizations?
- Do boards currently have the skill sets necessary to adequately address cybersecurity?
- What should the board be focused on with respect to cybersecurity?
- What is a suggested interaction model between senior management and the board for cybersecurity?
- Has the regulatory focus on the board's cybersecurity responsibility been increasing? If so, what is driving that focus?

Overall Cybersecurity Strategy

- Does the board need to play a more active part in determining an organization's cybersecurity strategy?
- What are the key elements of a good cybersecurity strategy?
- Is the organization's cybersecurity preparedness receiving the appropriate level of time and attention from management and the board (or appropriate board committee)?
- How can management and the board (or appropriate board committee) make this process part of the organization's enterprise-wide governance framework?
- How can management and the board (or appropriate board committee) support improvements to the organization's process for conducting a cybersecurity assessment?

Risk Assessment: Risk Profile

- Is the organization a direct target of cyber attacks?
- What do the results of the cybersecurity assessment mean to the organization as it looks at its overall risk profile?
- What are the organization's areas of highest inherent risk?
- Is management updating the organization's inherent risk profile to reflect changes in activities, services, and products?

Risk Assessment: Cyber Maturity

Oversight

- Who is accountable for assessing and managing the risks posed by changes to the business strategy or

technology and are those individuals empowered to carry out those responsibilities?

- Do the inherent risk profile and cybersecurity maturity levels meet management's business and risk management expectations? If there is misalignment, what are the proposed plans to bring them into alignment?

Cybersecurity Controls

- Do the organization's policies and procedures demonstrate management's commitment to sustaining appropriate cybersecurity maturity levels?
- What is the ongoing practice for gathering, monitoring, analyzing, and reporting risks?
- How effective are the organization's risk management activities and controls identified in the assessment?
- Are there more efficient or effective means for achieving or improving the organization's risk management and control objectives?

Threat Intelligence and Collaboration

- What is the process for gathering and validating inherent risk profile and cybersecurity maturity information?

External Dependency Management

- What third parties does the organization rely on to support critical activities?
- What is the process to oversee third parties and understand their inherent risks and cybersecurity maturity?

Cybersecurity Metrics

- How should a board obtain IT metric information?
- Who should deliver IT metrics?
- What should IT metrics contain? In what format should it be presented?
- Is the information meaningful in a way that invokes a reaction and provides a clear understanding of the level of risk willing to be accepted, transferred, or mitigated?

Cyber Incident Management & Resilience

- How does management validate the type and volume of cyber attacks?
- Does the organization have a comprehensive cyber breach response and recovery plan?
- How does an incident response and recovery plan fit into the overall cyber security strategy?

Cybersecurity Education

- How does the board remain current on cybersecurity developments in the market and the regulatory environment?