BOARD OVERSIGHT OF CYBERSECURITY

Questions Directors Should Be Asking

The board's role in the oversight of organizational risk is increasingly complicated by cybersecurity concerns. Cybersecurity risk is pervasive and will affect companies in a variety of ways. The responsibility for detailed cyber risk oversight within the board should be well documented and communicated; and may often touch various committees across the board including but not limited to risk, audit and compliance. With the increasing complexity surrounding cybersecurity, it is also important for the board to evaluate existing experience and skills, identify gaps and address those gaps through succession planning or leveraging advisors. Additionally, all 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.

BDO has 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 board structure, company strategy, organizational risk profile, cyber maturity, metrics, cyber incident management and resilience, continuing education and disclosure. 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

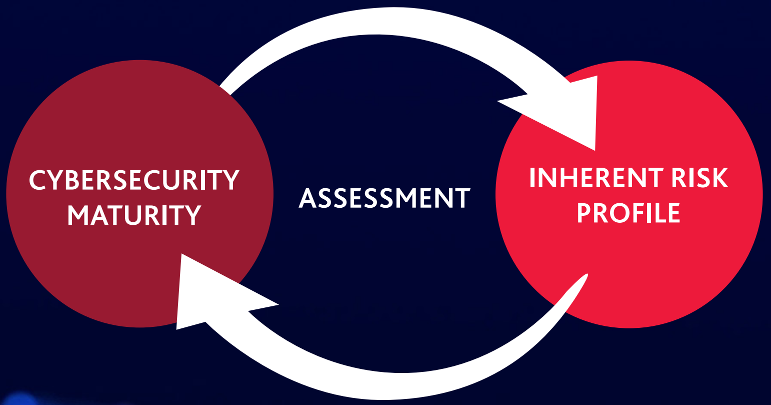
- What is the threat profile and risk tolerance of our organization based on our business model and the type of data our organization holds?
- Is the cyber risk management plan documented, including the identification, protection and disposal of data?
- Has the cyber risk management plan been tested?
- Does our organization's cybersecurity strategy align with our threat profile and risk tolerance?
- Is our cybersecurity risk viewed as an enterprise-wide issue and incorporated into our overall risk identification, management and mitigation process?
- What percentage of our IT budget is dedicated to cybersecurity?
  - Does that allocation conform to industry standards?
  - Is it adequate based on our threat profile?
- What are stakeholder demands and priorities for cybersecurity? Data privacy? Data governance? What interactions has the company or board had with shareholders regarding cybersecurity?
- What is the interaction model between senior management and the board for communications regarding cybersecurity?
- Has the regulatory focus on the board's cybersecurity responsibility been increasing? If so, what is driving that focus?

BOARD CYBERSECURITY OVERSIGHT

- How is oversight of cybersecurity structured (committee vs. full board) and why? Is this structure well documented in the appropriate governance charters?
- Is cyber an area considered and reported as a director competency? If so, have skill/experience gaps been identified together with plans to resolve those gaps?
- Is there a cyber expert on the board?

OVERALL CYBERSECURITY STRATEGY

- Does the board play an 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 do management and the board (or appropriate board committee) make this process part of the organization's enterprise-wide governance framework?
- How do management and the board (or appropriate board committee) support improvements to the organization's process for conducting a cybersecurity assessment?



RISK ASSESSMENT: RISK PROFILE

- What are the potential cyber threats to the organization?
- Who is responsible for management oversight of cyber risk?
- Has a formal cyber assessment been performed? Does it need to be updated?
- Do management and the board understand the organization's vulnerabilities and how it may be targeted for cyber-attacks?
- What do the results of the cybersecurity assessment mean to the organization as it looks at its overall risk profile?
- Is management regularly 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, managing and monitoring the risks posed by changes to the business strategy or technology and are those individuals empowered to carry out those responsibilities?
- Is there someone dedicated full-time to our cybersecurity mission and function, such as a Chief Information Security Officer (CISO)?
- Is our cybersecurity function properly aligned within the organization? (Aligning the CISO under the CIO may not always be the best model as it may present a conflict. Many organizations align this function under the risk, compliance, audit or legal functions - some with direct or "dotted line" reporting to the CEO.)
- Do the inherent risk profile and cybersecurity maturity levels meet risk management expectations from management, the board and shareholders? 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?
- Are there controls in place to ensure adequate, accurate and timely reporting of cybersecurity related content?
- How does the company remain apprised of laws and regulations and ensure compliance?
- What cloud services does our organization use and how risky are they?
- How are we protecting sensitive data?

Threat Intelligence and Collaboration

- What is the process for gathering and validating inherent risk profile and cybersecurity maturity information?
- Does our organization share threat intelligence with law enforcement?

External Dependency Management

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

CYBERSECURITY METRICS

- Have we defined appropriate cybersecurity metrics, the format and who should be reporting to the board?
- How regularly should a board obtain IT metric information?
- 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?
- How is the board actively monitoring progress or lack of progress and holding management accountable?

CYBER INCIDENT MANAGEMENT & RESILIENCE

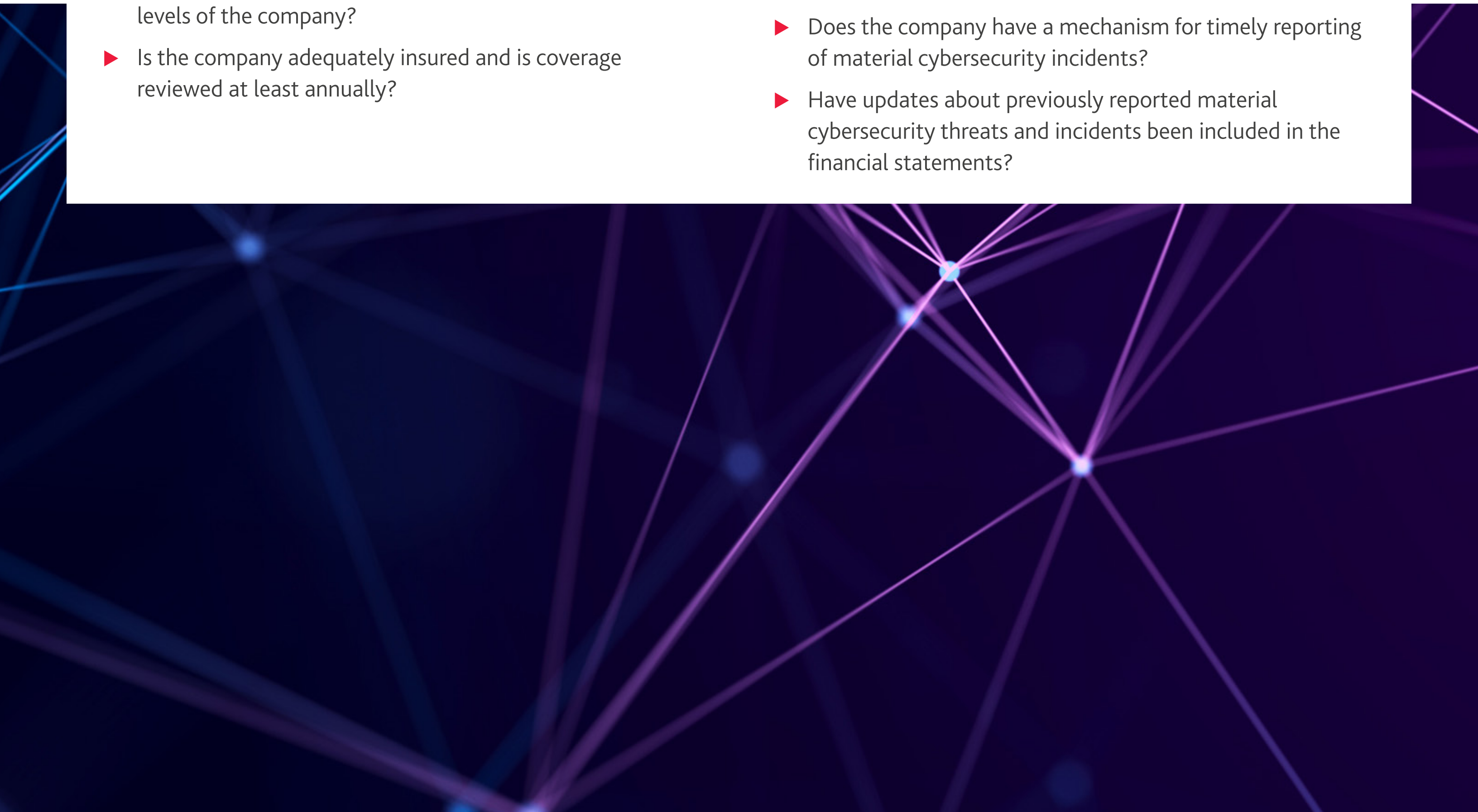
- How does management validate the type and volume of cyber-attacks?
- Does the organization have a comprehensive cyber incident response and recovery plan? Does it involve all key stakeholders - both internal and external? Does it include a business disaster recovery communication process?
- How does an incident response and recovery plan fit into the overall cyber security strategy?
- Is the board's response role clearly defined?
- Is the cyber incident response reviewed and rehearsed at least annually? Do rehearsals include cyber incident exercises?
- Is there a culture of cyber awareness and reporting at all levels of the company?
- Is the company adequately insured and is coverage reviewed at least annually?

CYBERSECURITY EDUCATION

- How does the board remain current on cybersecurity developments in the market and the regulatory environment?
- Currently, how does the board evaluate director's knowledge of the current cyber environment and cybersecurity issues impacting their organizations?
- Do boards currently have the skill sets necessary to adequately oversee cybersecurity? How is the board identifying and evaluating the necessary director skills and experience in this area?
- Are directors provided with educational opportunities in this area?
- Is regular cybersecurity education provided to the entire organization?

CYBERSECURITY DISCLOSURE

- Has oversight of cybersecurity reporting been defined for management and the board?
- Are company policies and procedures to identify and manage cybersecurity risk, management's role in implementing cybersecurity policies and procedures, board of directors' cybersecurity expertise and its oversight of cybersecurity risk, being included within the financial statement and proxy disclosures?
- Does the company have a mechanism for timely reporting of material cybersecurity incidents?
- Have updates about previously reported material cybersecurity threats and incidents been included in the financial statements?



NEXT STEPS FOR ALL

We invite you to explore additional resources of interest and educational programming via BDO's Center for Corporate Governance.

Available resources:

PODCAST

What May the SEC's Proposed Cybersecurity Disclosure Rules Mean for Those in Governance Oversight Positions?

THOUGHT LEADERSHIP

The Board's Role in Enterprise Information Governance

2022 Board Committee Priorities

Five Ransomware Themes Keeping Directors Up at Night

ARTICLES

SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure

10 Cybersecurity Best Practices For Your Business

PAST WEBINAR

Data Protection Academy: The Foundations of Privacy Program management, European Data Protection Plus Blockchain in Privacy

Contact Us

GREG SCHU
Partner Cyber Compliance & Assessments
612-367-3045 / gschu@bdo.com

AMY ROJIK
Managing Partner - Corporate Governance,
Communications & Emerging Issues
617-239-7005 / arojik@bdo.com

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. www.bdo.com

Material discussed in this publication is meant to provide general information and should not be acted on without professional advice tailored to your needs.