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 affects companies in many ways. The board's responsibility for cyber risk oversight should be clearly documented and communicated, involving various committees such as risk, audit, and compliance. Cybersecurity oversight should be collaborative, integrating technological innovation and related risks.

With the increasing complexity surrounding cybersecurity, it is also important for the board to evaluate existing experience and skills, identify possible gaps in experience with technology and security, and develop a plan to address methods to enhance the skills required. This may include recruiting additional board members, incorporating succession planning or leveraging third-party advisors. Also, all directors need to maintain continual knowledge about evolving cyber issues and understand management's plans for allocating resources with respect to the preparedness in responding to cyber risks and not deferring to those with expertise. Having knowledge of threats, risks, and impacts of a cyber issue helps boards assess the priority-driven and investment decisions put forth by management and the intention of reducing risks in areas identified as critical by management.

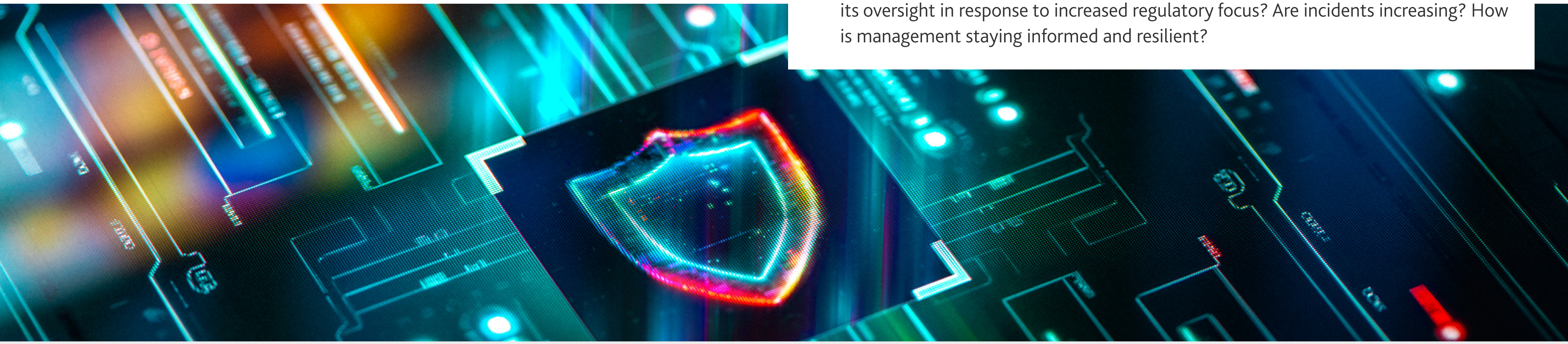
BDO has prepared the following compilation of critical questions for boards and management to consider in mitigating cyber security risk for their organizations. Questions contemplate the general to the specific, covering board structure, company strategy, organizational risk profile, cyber maturity, 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.

BOARD OVERSIGHT OF CYBERSECURITY

- How is oversight of cybersecurity structured (committee vs. full board) and why? Is this structure well documented in the appropriate governance charters?
- 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 for the organization?
- If gaps have been identified, is there a plan to resolve those gaps within a timeline that helps the company address the risk of the gap?
- Is there a minimum expectation for "technology literacy"? How does the board evaluate levels of literacy?
- Is there a cybersecurity expert on the board?
- What is the frequency and priority of cybersecurity board discussions? Does that frequency lag or lead the pace of change internally and with the cybersecurity threat landscape in your industry?
- Does the board occasionally verify information received from management pertaining to cybersecurity? (trust but verify)
- Does the board provide technology education for directors?
- What has the board implemented to help stay current on cybersecurity developments in the market and the regulatory environment?

GENERAL CYBERSECURITY MANAGEMENT

- What is the company's technology management structure? Does the structure establish a multi-disciplined approach?
  - What are the job titles, descriptions, and reporting structure for those leading the management of cybersecurity? What is their skillset and experience?
  - Are structure, roles and responsibilities well communicated and documented?
  - Is Separation of Duties (SoD) reflected in the structure sufficiently to allow for independence and assurance of both internal and external reporting?
- Are the cyber security and risk management plans documented?
  - Do they cover the identification, protection, and disposal of data?
  - Do they cover Third-Party Risk Management?
- Have the cyber management plans been tested?
- Is our cybersecurity risk viewed as an enterprise-wide issue and incorporated into our overall risk identification, management, and mitigation process? How are risks communicated and monitored? Which risks has management accepted?
- 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?
- What is the external environment around cybersecurity? How is the board adapting its oversight in response to increased regulatory focus? Are incidents increasing? How is management staying informed and resilient?



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?
- Does the organization's cybersecurity strategy align with its threat profile and risk tolerance?
- What IT security standards and frameworks has the company selected, and do they still align with strategy and regulations?
- 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 the organization's process for conducting a cybersecurity assessment?
- Is the cybersecurity assessment performed annually and completed internally or using an independent third-party?

RISK ASSESSMENT: RISK PROFILE

- What is the cyber threat profile and risk tolerance of the organization based on the business model and the type of data the organization holds?
  - Have potential financial, reputational, and operational weaknesses been contemplated? This should include impacts on customers, other businesses, and day-to-day activities should systems be unavailable (which could include email, applications, the network, or the intranet).
- Is there an accurate and complete inventory of the technology in use, including end-of-life evaluation (e.g., unsupported, not patched, etc.)? Who is responsible for the maintenance of this list and associated recommendation?
- What is the process for gathering and validating issues to build the inherent risk profile and cybersecurity maturity rating?
- How does cybersecurity management stay informed about emerging and/or recent cybersecurity incidents and emerging risks?
- How are the potential cyber threats to the organization inventoried, analyzed, and monitored?
  - How are they reported to management and the Board?
  - Do management and the board understand the organization's vulnerabilities and how it may be vulnerable to cyber-attacks (whether targeted or due to lack of adequate controls)?
  - Is management regularly updating the organization's inherent risk profile to reflect changes in activities, services, and products?
- Has a holistic cyber assessment been performed, taking into account internal, external as well as third party factors?
- What do the results of the cybersecurity assessment mean to the organization as it looks at its overall risk profile?
- What percentage of our IT budget is dedicated to cybersecurity? What are the investment priorities?
  - Does that allocation conform to industry standards?
  - Is it adequate based on our threat profile?
  - What is the total capital budget and prior spend?
  - What is the allocation to tech debt and upgrading legacy systems?
  - How many of our systems are "end of life" and not supported?
- What cloud services does the organization use and how has risk been quantified for each cloud solution in use?
- What is the process for identifying and protecting sensitive data?
- What is the process for monitoring GenAI capabilities and what does this mean to cybersecurity?

RISK ASSESSMENT: CYBER MATURITY

Oversight

- Who is accountable for management oversight of cyber risk including assessing, managing, and monitoring the risks posed by changes to the business strategy or technology? Are those individuals empowered to carry out the responsibilities assigned to them?
  - Is this process aligned with the overall ERM process & framework?
- Is there someone dedicated full-time to the cybersecurity mission and function, such as a Chief Information Security Officer (CISO)?
- Is the 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. Organizations have aligned 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 the cybersecurity maturity levels align with the risk expectations established by 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?
  - How often are they reviewed and revised?
  - How are they communicated and monitored broadly across the organization?
  - How are professionals at all levels educated on technology use, ethics, and policies?
- 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 for adequate, accurate and timely reporting of cybersecurity related content?
- How does the company remain apprised of laws and regulations for compliance purposes?
- Is appropriate threat intelligence from the organization shared with law enforcement?
- Has the organization considered performing a System and Organization Controls (SOC) for Cyber report (when the organization is a third-party providing services to other companies)?
- Did the external auditor identify cybersecurity risks or deficiencies in controls?
- Has internal audit reviewed any aspect of cybersecurity management and/or controls? If so, what were the recommendations, and have they been remediated? If not, should this be a priority?
- Has the organization evaluated the cost and ROI associated with leveraging AI to monitor and detect bad actor activity?

External Dependency Management (Third-Party Risk Management)

- Is an inventory of third parties the organization relies on to support critical activities being maintained and does the organization regularly audit third-party access and corresponding permissions?
- What is the process to oversee third parties and understand their inherent risks and cybersecurity maturity?
- What has been implemented to extend beyond core compliance activities for corporate security and resiliency?
- What is the strength of management's vetting (due diligence) process for third-party partnerships?
- How are third-party products certified as tolerable, and any compensating controls assured over time?
- Are third party vendors actively engaging in their own business disruption simulations?

Mergers & Acquisitions – Technology Impacts

- Does due diligence factor in the data posture/ hygiene of the target and the potential impact to the deal valuation?
- Is the current "technology debt" of the target known?
- Have IT systems — for both the target as well as the acquiror — been maintained and can they be integrated without creating significant risk and additional cost?
- Has the company consulted an advisor regarding integration complexities?

CYBERSECURITY METRICS

- Have strategically aligned cybersecurity metrics been defined, including the format, cadence to evaluate, and who should be reporting to the board?
- 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 toward goals and holding management accountable?
- Is regular cybersecurity education provided to the entire organization?

CYBER INCIDENT MANAGEMENT & RESILIENCE

- How does management classify the type and volume of cyber-attacks?
- Does the company maintain a Business Impact Analysis (BIA) to define the relative value of each service and group to the mission and to the business?
- 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 system and process?
- How does an incident response and recovery plan fit into the overall cyber security strategy?
  - How often is it reviewed and updated?
  - Is it easily accessible? Would it be during an outage?
  - Does it include business continuity?
  - Is there a well-documented and accessible communication chain in case of a breach?
- Is the board's response role clearly defined, documented, and communicated?
- Is the cyber incident response reviewed and rehearsed periodically, in line with the pace of external threats and risk tolerance? Do rehearsals include cyber incident exercises?
- When was the last tabletop exercise performed? Were both the board (or key representative from the board) and management involved?
- Is there a culture of cyber awareness and reporting at all levels of the company?
  - Does the company perform frequent and sophisticated employee testing to monitor compliance?
- Is the company adequately insured and is coverage reviewed at least annually?
  - Are the conditions of coverage understood and accounted for in the security and risk management plans, and tested?
- Have external communication draft templates been created in case of a breach and have communication responsibilities been assigned to a person/team?

Ransomware

- Is there adequate documentation of preparedness for responding to ransomware — does this take in to consideration capital allocation and estimates of potential downtime of operations and alternatives to reduce/eliminate risk?
- Have appropriate consultants, attorneys, and law enforcement agencies been defined to guide discussions/decisions-making should an incident occur?
- How does the control environment factor into the likelihood of success in terms of competence (e.g., training, employee policies, VPNs) and the timely restoration of viable data per the continuity plan?
- Pay now, pay later, or do not pay — decisions:
  - What is the plan?
  - When was it last revised? Were changes made (e.g., pay ransom vs. update/rebuild systems)

CYBERSECURITY DISCLOSURE COMPLIANCE

- Has management and the oversight of cybersecurity reporting been separately defined for management and the board?
- Are company policies and procedures with respect to risk management, strategy, and governance — including management's role in implementing cybersecurity policies and procedures, management's cybersecurity expertise, as well as how the board oversees cybersecurity risk — being incorporated into the financial statement and proxy disclosures?
- Does management incorporate input from legal counsel and the compliance department regarding cybersecurity disclosures?
- Do cyber oversight disclosures align across internal and external reporting mechanisms (e.g., 10K, MD&A, risk profile, proxy statement, board/committee charters, agendas, and minutes)?
- Has management performed a preliminary materiality analysis in case of a breach? Does the analysis contemplate both quantitative and qualitative aspects?
  - Does the board understand and agree with management's materiality definition and analysis?
- Does the company have a mechanism and definition for "timely reporting" of material cybersecurity incidents?
- Have updates about previously reported material cybersecurity threats and incidents been included in the financial statements?

As directors navigate their oversight cybersecurity responsibilities, they need to remain informed and be confident in information provided by management. Enlisting a broader lens to understand the opportunity costs and strategies that contemplate ERM complexities such as digital transformation, movement to the cloud, and threat security and responsiveness.

The BDO Center for Corporate Governance endeavors to support directors in engaging in effective governance by providing insights, learning, and networking opportunities in collaboration with BDO subject matter specialists and advisors designed specifically for boards of directors.

CONTACT US

AMY ROJIK
National Managing Principal - Corporate Governance
arojik@bdo.com

LEE SENTNOR
Professional Practice Director
lsentnor@bdo.com

GREG SCHU
Assurance Market Managing Principal
Risk Advisory Services - Cyber Compliance & Assessments
gschu@bdo.com

DENNIS GLENDENNING
Microsoft Technology Director
dglendenning@bdo.com

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, 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. For more information, please visit: www.bdo.com.

© 2025 BDO USA, P.C. All rights reserved.