NDI Executive Exchange

The Board’s Role in Overseeing Cyber Security

1. **Cybersecurity is an enterprise risk management issue.**

   The Board should understand and approach cybersecurity as an enterprise risk management issue, not just an IT issue. The Board should be trained on its duties related to overseeing cybersecurity risk. Boards may be trained by legal, the CISO or his/her designee, risk management, third party consultants, or in other ways.

2. **The Board should understand the legal implications of cyber risks as they relate to the organization’s specific circumstances.**

   The Board should understand which laws or standards regulate the organization and how these laws and standards should impact the preparation and response for a data event.

3. **The Board should have adequate access to cybersecurity expertise and give cyber risk management regular and adequate time on Board meeting agendas.**

   The Board should set the expectation that management will establish a holistic, enterprise-wide risk management framework with adequate staffing and budget. Internal and external IT consultants should work together. If external IT consultants are hired, consider having outside counsel directly hire those consultants on the organization’s behalf to enhance the attorney-client privilege. The reports prepared by these consultants may become discoverable by third-party plaintiffs in the event the organization experiences a data breach.

4. **The Board should be consulted in choosing the cybersecurity framework the organization will adopt and should understand the resulting impact on the policies and procedures developed to comply with that framework.**

   The organization’s policies and procedures will be measured against the cybersecurity enterprise-wide risk framework chosen by the organization. Security, privacy and other cyber-related policies and procedures should be compared against best practice models and legal and regulatory requirements and be updated based on the results of the most recent risk assessment. The organization should also have a security incident response plan that meets applicable law and best practices to help the company prepare for and respond to a data breach.

5. **Organizations should identify risks and vulnerabilities through a security risk assessment.**

   Organizations should review current security risk assessments and identify areas for improvement and recommendations, such as improving documentation of the risk assessments to better ensure regulatory compliance, enhancing the attorney-client privilege of the risk assessment, and approaching future assessments in a way that maximizes their effectiveness and minimizes risk of a cyber-attack.

6. **Organizations should assess risk management plans.**

   Organizations should also assess risk management plans to ensure measures have been taken to reduce the risks and vulnerabilities identified in the security risk assessments. The organization should seek appropriate expertise to ensure the risk management plan contains best practice approaches used across the industry. Management discussions should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance.

7. **Organizations should conduct table top exercises on a regular basis.**

   The purpose of such exercises is to see how the company performs in a mock data breach scenario.

8. **Organizations should conduct employee security awareness training.**

   The purpose of such training is to reduce the risk of phishing and other employee related cyber-attacks.

9. **The Board should understand the risk that comes from vendors and that not all vendors are equivalent.**

   Vendor management programs should include a review of cloud and other vendor contracts to ensure appropriate security controls are in place and liability and risk are appropriately allocated between the parties. The security posture of these vendors should be assessed, such as through vendor questionnaires or third-party audits. Organizations should be aware of GDPR's requirements for vendor management if applicable to the organization.

10. **The organization should determine whether to obtain cyber insurance, and understand the coverage and limits of such coverage.**

    Practically speaking, some organizations choose to purchase cyber insurance and others do not. The Board should have an understanding of this. If the organization chooses to purchase cyber insurance, the organization should ensure the organization has control to choose its data breach panel of experts, including preferred legal counsel.