Corporate governance and data issues

OSLER

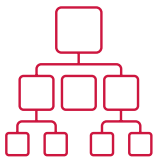
Corporate boards are under pressure to make data security a key priority in an age where it is not ***whether*** but ***when*** a data security incident will happen. A cybersecurity strategy must be in place to prioritize and protect the organization's critical data and information systems and to manage the risk of data security incidents.

Your cybersecurity strategy

Your cybersecurity strategy must:

- assign ***roles and responsibilities*** to different groups within your organization,
- ***coordinate and integrate*** group activities to guard against gaps in security; and
- ensure that these groups are ***held accountable*** for their responsibilities.

The cybersecurity strategy must include an evergreen data breach response plan – so that the organization is ***ready to respond*** – not just prepared for a data security incident. Your plan must also provide the framework to drive a coordinated and integrated response to a data breach.



Your company's board of directors is responsible for overseeing the implementation of the organization's cybersecurity strategy, including its data breach response plan, and should receive regular ***reporting*** on the integrity of the organization's data and information systems and related risks.

Questions counsel should be prepared to answer in advising the board:

- ☑ What is the corporation's risk tolerance?
- ☑ What sources of cybersecurity risk apply to the organization? Has adequate due diligence been conducted to assess the risk?
- ☑ What assets, information and data are at risk?
- ☑ Where does accountability for data security reside within the corporation?
- ☑ Does the organization have a coordinated and integrated cybersecurity strategy? Have silos been eliminated from the management of the strategy and data breach response plan? Have people been assigned appropriate ownership and responsibility and are they held accountable for their responsibilities?
- ☑ Are security incidents and the cost of responding to them measured?
- ☑ Have policies on security, information sensitivity and ethics been documented and communicated within the organization?
- ☑ Are security initiatives adequately funded in light of the corporation's risk tolerance?
- ☑ Is there a plan in place to evaluate the ongoing effectiveness of the cyber risk program?
- ☑ How will the organization's security initiatives be disclosed?

Framework for board oversight, accountability and organization coordination