



Talking to Your Board

March 30, 2022

Background: What Does a Board Do?

- Every business should have a board of directors to oversee its operations.
- The board creates governing documents, sets policy, and hires and directs executive employees.
- Board members have a fiduciary duty of responsibility for the corporation's assets and its shareholders.
- A good board member must have integrity, leadership experience, and a commitment to the company.



What Does a Board Do (Cont'd.)

- Recruit, supervise, evaluate, and compensate management and executives
- Provide direction for the business through a mission statement
- Establish bylaws and a system of governing the business
- Act as fiduciaries to protect the business assets and shareholder investments
- Monitor and control business functions
- Exercise fiduciary responsibilities to oversee financial and legal requirements of an organization.





What Does a Board Have To Do With Privacy & Cybersecurity?

- Enterprise risk assessments typically reveal Privacy and Cybersecurity as part of an organization's Top 10 risks.
- As a governance function, the Board is responsible for overseeing the general direction of a company. Understanding key areas of enterprise risk enables an oversight Board to ensure management of a company is focusing on the right priorities.
- Since the COVID-19 pandemic began, Cybersecurity has jumped up to a Top 3 priority for many organizations. (source: McKinsey)



Audit Committee

- For U.S. publicly traded companies, the Audit Committee is responsible for the financial reporting process, selection of a company's independent auditor, and receipt of audit results (internal and external). The Sarbanes Oxley Act requires a Board of Directors for publicly traded companies to have an Audit Committee and tasks this Committee with oversight of the company's independent auditor.
- Depending on Audit Committees bylaws or charter, it also have oversight of **regulatory compliance** and **risk management activities**.



Understanding Your Board

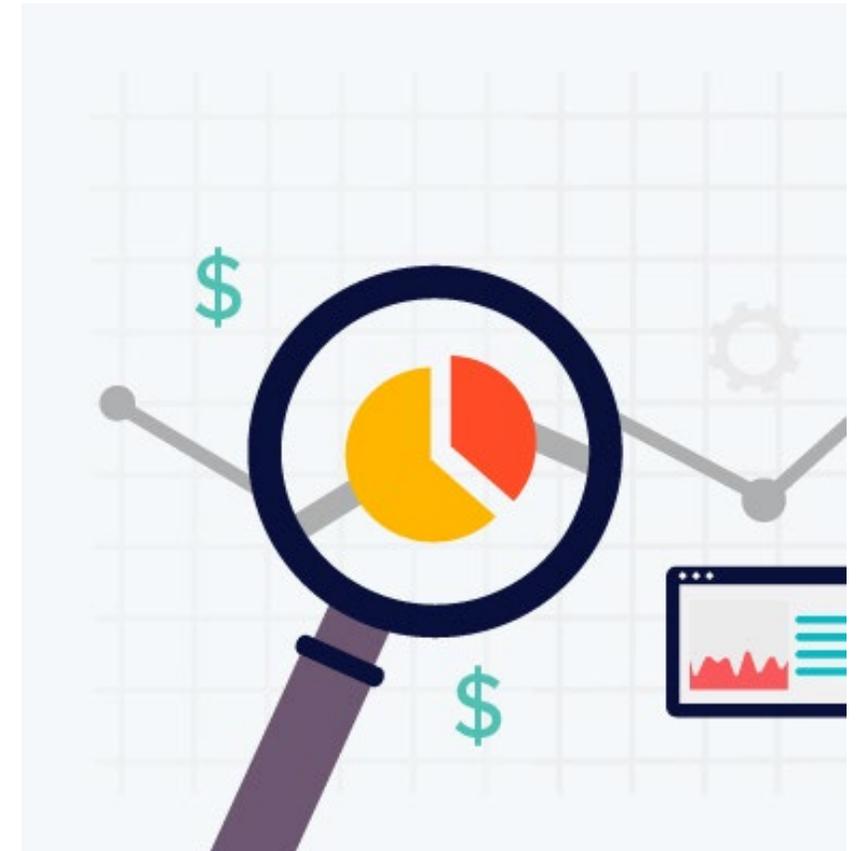
Prior to a presentation, it is always helpful to have a background of the members of the Audit Committee (or other committee which may oversee key compliance areas)

- Do the members have relevant expertise and knowledge in Privacy & Cybersecurity? Depending on their level of awareness and comfort, there may need to be some educational component with your presentation.
- What membership do the members have in other boards or organizations? This may also guide their understanding of certain governance requirements and risk tolerance.



Provide a Program Assessment

- **How does the cybersecurity/privacy program enable business objectives?** The Board is primarily responsible for overseeing that primary business objectives and the company's mission is being realized.
- **What is the maturity level of the program?** This helps the relevant committee understand the starting point and assist with assessing where such a program needs to be in the future for the company, based on its operational and brand size. This can also assist with oversight of ensuring the program remains funded and prioritized.
- **What will future phases of the program look like?** This can serve to educate the committee as to where the program is going and what the resourcing needs may be.
- **What are the common threats based on your company's industry?** This helps explain the relevance of prioritizing certain actions or processes within your privacy or cybersecurity program.
- **What are the program's areas of weakness?** To the extent that remediating the program's weaknesses can assist with realizing the company's primary business objectives, the Board should be made aware so that it can devote proper attention to oversight.
- **Use metrics (KPIs and OKRs) to tell the story**
- **Key takeaways:** Don't get so bogged down in key details that you miss concluding where should resources or priority be allocated. Your presentation should conclude with what action the Board needs to take.



Action/Resources Needed

As oversight bodies for a company's direction, Boards are empowered to ensure that certain actions be prioritized and resources allocated by management.

- **Be explicit and specific.** Briefly explain the cause of the change (e.g., a new law or new market has opened up) and use statistics, examples, and specific metrics. Have a specific monetary or resource request (e.g., headcount) and explain how that monetary or resource request will be used.
- **Use examples from the industry.** Examples of best practices from the industry or enforcement activities of peer companies can assist with telling the story of why certain resources or attention should be allocated.





Adopt the 3-3-1 Approach

Realistically, any more than three goals is too many to focus on and execute against.

Therefore, identify no more than **three goals, three strategies per goal, and one metric for each strategy.**

Given the quarterly frequency of board meetings, you should set and track quarterly targets for each strategy, best represented through bar charts showing the specific target for each metric and the actual results by quarter.