

5 Steps to Prepare for Cybersecurity Compliance



ARTICLE 10.23.23 GUI COZZI

Explore the latest insights that can reshape your business's approach to cybersecurity disclosure and gain a deeper understanding of how the evolving landscape of cybersecurity disclosure impacts privately owned businesses.

1. Identify Gaps in SEC's Proposed Disclosure Requirements

- First, analyze the differences between what the SEC is suggesting for disclosures and what your company currently does.
- Assign responsibility for making the necessary improvements.

2. Integrate Disclosure Processes

- Avoid the mistake of creating a new, complex process. Instead, figure out how your cybersecurity practices can be seamlessly incorporated into your existing disclosure procedures.
- Identify the people who need to be involved, including legal experts.

3. Update Incident Management Process

- Adapt your incident management procedures to account for factors like the significance of the event and continuous reporting and monitoring.
- Ensure consistency in how you determine what is significant and how you disclose cybersecurity incidents, similar to how you handle operational or financial issues.

4. Engage Board of Directors Early

- Start a dialogue with your board of directors about the new disclosure requirements.
- Collaborate to identify any changes in governance that may be necessary.

5. Leverage Technology

- Invest in the right technology tools that can help streamline your disclosure processes and communication.
- This could be a single, all-in-one solution or a combination of individual tools that work together effectively.

Companies must take cybersecurity more seriously than ever before after a new rule passed by the SEC.

Have questions? [Reach out](#) today!