

5 Things to Include in a Board Member **Cybersecurity Agreement**

Human error is a leading cause of data breaches. According to a Verizon Data Breach Investigations report, 74% of incidents involve some human element, such as clicking on a phishing link. To safeguard sensitive data and intellectual property, boards must follow cybersecurity best practices.

This guide examines the importance of having a cybersecurity agreement, how to obtain a security commitment from your board, and identifies secure best practices for the whole governance team.

1. Start with the ‘Why’

- Include an up-front paragraph about the importance of cybersecurity. Most board members now understand the concept of cybersecurity, but it helps to detail potential risks to the company, who it would affect, and the consequences if a hack or attack occurs.

2. Password Management

- Since board members aren't logging on daily to their board portal or other areas to view materials, passwords can be difficult for them to remember. Nevertheless, it's important to outline some email best practices:
- Use a combination of lower and upper case characters.
- Update passwords at regular intervals.
- Refrain from using a password that is used on other sites.
- Don't store passwords on sticky notes or other obvious locations.



5 Things to Include in a Board Member Cybersecurity Agreement



3. Update, Update, Update

- Always use the most updated version of any software being used to access board materials. The same holds true for internet browsers. Software companies and browsers are always updating their software to stay ahead of hackers and cybersecurity threats. Things change fast, so check frequently to be sure you're using the latest versions of software.

4. Secure Devices & Portable Media

- When leaving desks be sure to lock computers and other company devices. All portable devices should be enabled with the most security features allowed.
- Board members should turn on passwords to access all devices.
- Report any lost or stolen devices that may include board materials immediately. Remote wiping and disabling access quickly can make all the difference.

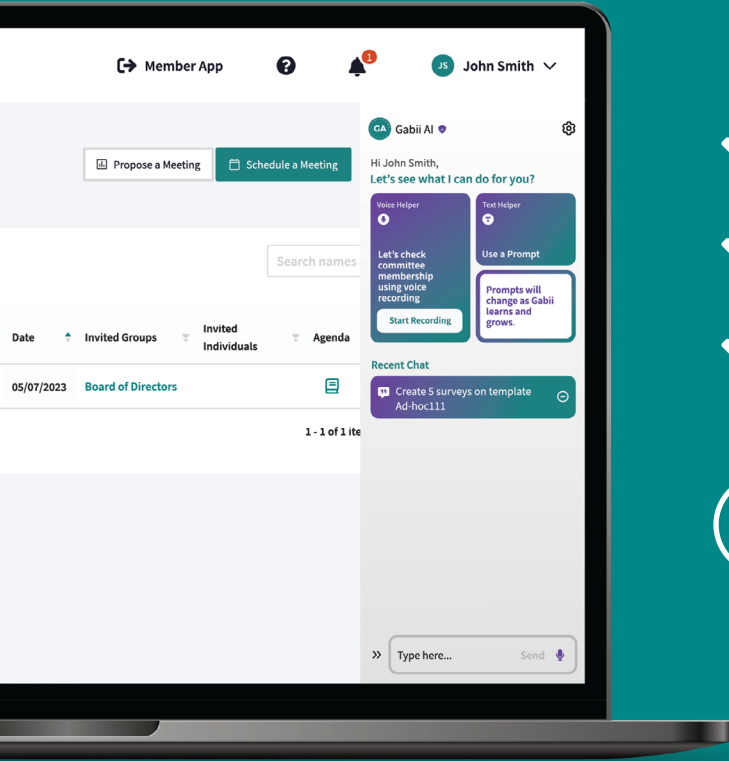
5. Commit to Cybersecurity

- According to a recently released IBM Security Services Cyber Security Intelligence Index report, 95 percent of all investigated cybersecurity incidents involved human error. Your board members should welcome the opportunity to protect any information your company shares.
- Educating and reviewing security best practices is a great start. Take it one step further by asking your board members to commit to the goal of minimizing risk as much as possible by signing a Cybersecurity Agreement.



The innovation leader in board management platforms

See what our platform can do for you!



- ✓ Improve Decision-Making
- ✓ Accomplish More in Less Time
- ✓ Mitigate Compliance Risk

[Schedule a Demo](#)

Trusted By



Call: 1.412.436.5180 x322

Email: info@govenda.com

Web: Govenda.com

