GOVENDA

Enhancing the Culture of Data and Cybersecurity with Your Directors

Govenda clients hail from industries that span large corporations, to finance, to health care. The need for cybersecurity is critical, and organizations do everything in their power to protect it. But one of the vulnerabilities is the board's own directors, who need to be vigilant of hackers mining for valuable information. Creating a culture of enhanced security is a proactive best practice to keep data secure, as well as to ensure directors comply with expectations for security.

An Enhanced Security Culture Checklist

Most companies ask employees to sign agreements spelling out the expectations to keep data private and secure. Board members have the same responsibility, especially given their access to a company's most sensitive information. Boards need clear expectations and accountability when it comes to information stewardship to encourage participation. And when thoroughly considered and regularly reinforced, this becomes ingrained in the culture of your board membership.

Be sure you've addressed the following topics:

Password Hygiene

Promote basic information stewardship with good "password hygiene." You know the drill on this one: directors should password-protect their devices, use secure, strong passwords for all board- related accounts, and change passwords regularly. This sounds like common sense, but according to the 2019 Data Breach Investigations Report (DBIR) from Verizon, 29% of breaches involved the use of stolen credentials. Two- or multi-factor authentication is a best practice identified to protect accounts against issues.

Enhancing the Culture of Data and Cybersecurity with Your Directors

Defined Cybersecurity Agreement

Define security processes and expectations in a security agreement. How is information accessed? Are there parameters for the device being used for access, such as encryption, anti-virus software, or the ability for a remote wipe should the device be lost? Can board information be accessed from a mobile device, and what are your unique concerns for mobile connectivity? This discussion is most effective when a director joins a board, but should also be revisited over time.

Protected File Storage and Sharing

What about files? This is a big concern for boards. Many of our clients have a “no printing” policy. But for printed or digital files stored locally by directors, it’s important to know how they should be handled, and then destroyed when no longer needed. Given the level of sensitivity of board documents, setting clear expectations takes the guesswork out of processes to protect data.

Policy Adoption to Reduce Liability

Encourage Adoption. Corporate liability is limited for directors, but if data is breached from their accounts, it’s a different story. A data breach stemming from a director’s personal account is double whammy of risk for both the organization and the individual (think Colin Powell’s email hack, which released sensitive information about Salesforce.com). It’s important that directors see security as part of their good governance responsibility, and a source of risk for everyone if not properly executed.

Culture of Security

Keep it top of mind, and topical. With cybersecurity attackers on a relentless war for data, this isn’t a “set it and forget it” business process. And when security becomes part of your board’s culture, it’s baked in to the response when something new arises. For example, during the social distancing mandates related to the COVID-19 shutdowns, meetings migrated to video conferencing. Directors could be creating new accounts to access virtual meetings and need strong passwords and good data protection processes that answer the unique needs of a virtual environment. A strong culture of security drives these activities proactively. And, directors will also benefit from periodic reminders around “general data housekeeping” to update passwords and delete or destroy documents no longer in use.

Enhancing the Culture of Data and Cybersecurity with Your Directors

The Simpler Way

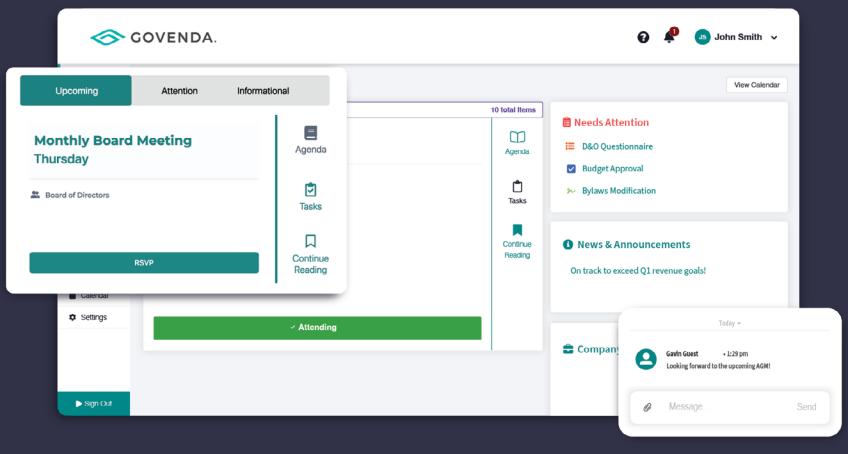
If checklists, emails, passwords, and personal liability seem like a lot of work...well, they are. Here at Govenda, we'll always advocate for board portal software. While we don't replace cyber security agreements, we take the guesswork out! Secure solutions like ours circumvent the need to secure personal emails and lessen risk for directors and their organizations. The annual cost for security and efficiency is a fraction of the cost to mitigate a security breach, making a portal a cost-effective way to address data security.

4.7 Star Rating

Capterra Software Advice GetApp

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

GOVENDA

Fender White Castle lightspeed NYC HEALTH+ HOSPITALS UiPath