Security Guide for Boards

Overcoming common cyber threats.

aprio

> **Cybersecurity has always been top-of-mind for IT departments, and these days, it's an increasingly important issue for boards as well.**

Gartner estimates that by 2020, virtually all large enterprises will need to report annually to their board of directors on cybersecurity and technology risk, and this timeline seems conservative. It will likely be a standard requirement much sooner.

With this increased focus on security, what about security of board information itself? Board communications bring challenges above and beyond internal company data

Part of a board administrator's job is to coach and oversee how directors communicate, to ensure that they don't unintentionally leave company data unsecured. Directors are busy, mobile, and sometimes less-than-tech savvy. How many of them right now are saving documents outside your safety protections and onto their desktops? How many are conducting board decision debates over email?

While IT often laments human behavior, the fact is that administrators need to safeguard against those things we all know "people shouldn't do" – but do.

Whether you're using board portal software or board meeting management tools like email, Dropbox, SharePoint or an in-house system, there are three key threats to watch.

Data can be downloaded.

When you send information electronically to your board members, they need to review it and depending on how data is sent, directors can put data at risk when accessing documents.

Email is notoriously insecure and will require directors to download material outside of their email. Dropbox may seem secure due to its AES 256-bit encryption, but similar to email, your data will not stay within Dropbox. It will be opened by directors and potentially saved elsewhere (e.g., their desktop).

With SharePoint, as well, the documents are only secure when they reside within the system. As soon as they're saved elsewhere, you've lost control – and you don't even know the data has been removed.

SOLUTION

Board management software can provide administrators control of whether documents may be printed or downloaded and can track who has accessed documents – all to protect sensitive material.

2

Decisions and communications are data.

When you use Dropbox, SharePoint or another in-house system for board communications, you need to put in place a separate platform for discussion and decisions to prevent director temptation to discuss decisions over email, which is generally unsecure.

SOLUTION

Beyond being a one-stop source for board materials, a board portal provides instant tools for directors to annotate documents and discuss board decisions. Whether these discussions are across the whole board or with select directors, it's all kept secure. Administrators can also post questions to the board through surveys. These features help keep sensitive topics out of everyone's inbox.

3

Lost data doesn't disappear.

No one intends to lose their tablet, phone or laptop, but mistakes happen to the best of us. The key issue for board administrators is whether you can remove data from a lost or stolen device if you need to. Email, documents and even potential Dropbox access are instantly at risk.

The ability to purge data is essential for confidential company material. Board portals allow for rapid response if a device or laptop is lost, with instant, remote data-wiping.

Safeguarding your board – key things to consider

The challenge with security is the complexity of board communication. When choosing board collaboration tools, you need to consider the end-to-end activities of board members, as they access, review, and communicate.

These five security-focused features will help keep your data safe:

- Encryption during transit and at rest

- Ability to restrict downloads if required

- Easy, secure forum for shared notes (e.g., annotations within a portal)

- Easy, secure way to record decisions (e.g., survey tool)

- Ability to wipe data remotely, upon a lost or stolen device

Last year, the cost of cyber security to companies rose 22.7 per cent to an average of US$11.7 million, primarily due to security breaches. Protecting your board will help ensure that you don't become part of this statistic.

KEEPING DATA SECURE WITH YOUR BOARD OF DIRECTORS

UNSAFE

SAFE

ADMIN

Unsafe:
- Sends files via Dropbox or email

Safe:
- Shares board book via board portal (encrypted files, restrictions on downloads)

DIRECTOR

Unsafe:
- Downloads sensitive document to desktop
- Sends document with comments via email
- Loses tablet holding company information
- Fails to purge Dropbox contents

Safe:
- Reviews document in board portal
- Adds annotation to document in board portal
- Shares discussion with other directors via board portal
- Loses tablet but advises admin, so they can wipe data remotely from the board portal

BOARD CHAIR

Unsafe:
- Sends question to directors via email
- Loses access to company-built interface in a disaster or crisis situation

Safe:
- Polls directors via board portal
- Accesses company information in a crisis, through a board portal that ensures business continuity

EFFICIENT BOARD MEETINGS & EASIER BOARD COMMUNICATION

Discover why hundreds of admins and board members love Aprio. We make good governance simple and affordable.

The Aprio board portal helps organizations large and small to efficiently run board meetings, keep directors up to date, and keep information secure. Aprio provides premium features without premium pricing, all delivered with unmatched service.

GET IN TOUCH

Get a free 30-minute needs assessment on improving your security with Aprio.

Visit **aprio.net/demo**

1-855-55-APRIO (1-855-552-7746)
aprio.net