



**BoardEffect**  
a Diligent brand



# Board Management Solutions: How Secure Is Secure?

# Introduction

---

A data breach would send your volunteer board into crisis, especially if you weren't prepared to handle it. To avoid such a tragedy, it's crucial for organisations to hold security and confidentiality of communications high.

Your board management solution is a tool you rely on regularly to manage board and committee activities. Since your board members use it so often, you need peace of mind in knowing that the data you collect and share is secure. While software vendors make big promises about how secure their products are, it's prudent to question the validity of their claims and really understand what protection you're getting. To accomplish that, you'll need to ask the right questions.

Has your board considered the risks of cybersecurity in relation to the security of your board management solution? Your board needs assurance that you have full control over your data, and you also need to have control over who can access it. This type of security is a critical factor when choosing the best board management solution.

## Table of Contents

[Volunteer Board Management Solution Vendors: Are Platforms as Secure as They Claim?](#)

[Why Security Is Critical in a Volunteer Board Management Solution](#)

[Questions Your Volunteer Board Needs to Ask About Security in a Board Management Solution](#)

[Substantiating a Board Management Solution Vendor's Claims About Security](#)

# Volunteer Board Management Solution Vendors: Are Platforms as Secure as They Claim?

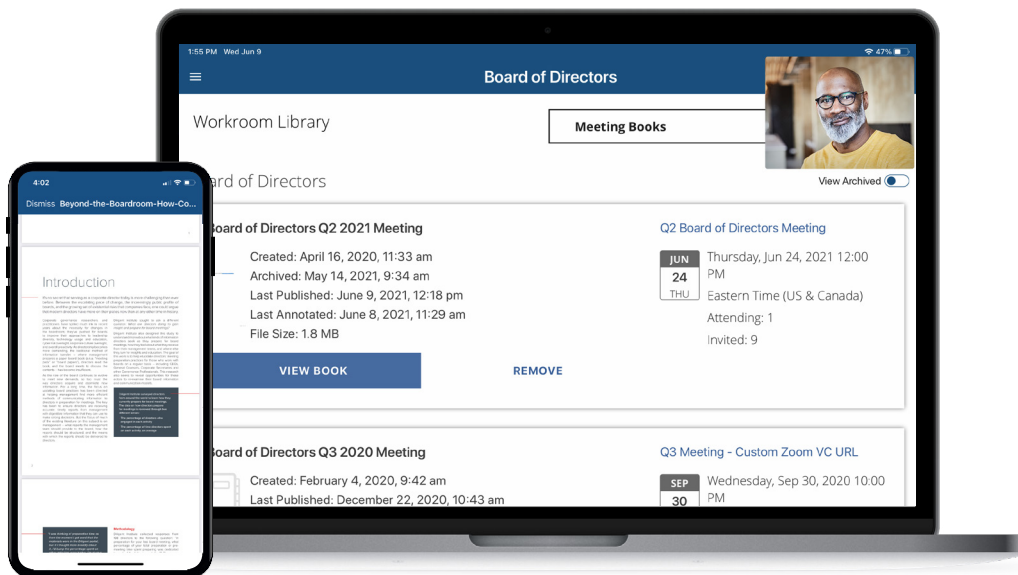
Information technology governance is the process of creating and maintaining a framework for information security strategies that align with the following three things:

1. Aligns with your organisation's mission
2. Enables your organisation to be compliant with laws and regulations
3. Assigns responsibility in an effort to mitigate risks

A key responsibility of a volunteer board is managing risk, and for that reason, cybersecurity must be one of their primary focuses. A board management solution is the key to managing your board duties with efficiency, transparency, and security.

The marketplace offers a wide variety of board management solutions. Considering paramount focus on cybersecurity and the sensitivity of information your organisation collects and stores, board management solution vendors attract your attention by claiming their platforms are highly secure. Words are meaningless if they're not backed by solid data and information to support them.

How can you be sure that a board management solution lives up to your board's needs and expectations? It takes asking the right questions and having a better understanding of how to assess board management solution security with accuracy.



# Why Security Is Critical in a Mission-Driven Organisation's Board Management Solution

A security vulnerability is a flaw or weakness that malicious actors tap into to perform nefarious actions within a computer system. Weak security can have a serious negative impact on everyone connected with your organisation including your board, donors, volunteers, other vendors, and the community at large.

80% organisations do not have any cybersecurity plan

CyberPeace Institute<sup>1</sup>

**Here are 3 situations where charities and not-for-profit organizations need to make cybersecurity a high priority:**

1. Your organisation processes e-commerce transactions on an e-commerce site (donations, event registrations, product sales, etc.)
2. Your organisation stores or transfers sensitive, confidential, or personally identifiable information (employee records, driver's license numbers, contact information, national insurance numbers, etc.)
3. Your organisation collects information from donors, patrons, members, volunteers, or subscribers related to their habits or preferences.

The United Kingdom's Information Commissioner notes that the severity of GDPR fines relates to having adequate, reasonable, consistent, and effective controls.

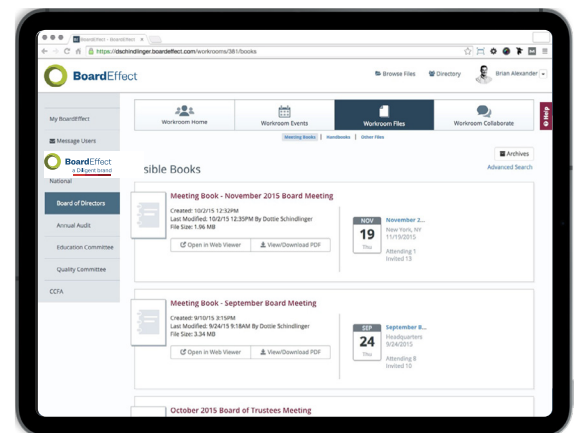
"Cybersecurity for nonprofits is critical—these organisations provide essential services to their communities. In the event of a cyberattack that exposes the personal data of clients, the consequences are particularly significant."

**John Giordani**





"Staying ahead of [cyber risk] really comes down to you as a board members knowing the right questions to ask."

**Brian Stafford**

President and CEO Diligent.



**Gartner has come up with the following Care Standard for Cybersecurity based on that principle:**

-  **Consistent:** Do your controls work the same way over time?
-  **Adequate:** Do you have satisfactory and acceptable controls in line with business need?
-  **Reasonable:** Do you have appropriate, fair and moderate controls?
-  **Effective:** Are your controls successful in producing the desired or intended results?

Source: Gartner<sup>4</sup>

Ultimately, in protecting your organisation, your board is also protecting many other groups and individuals.

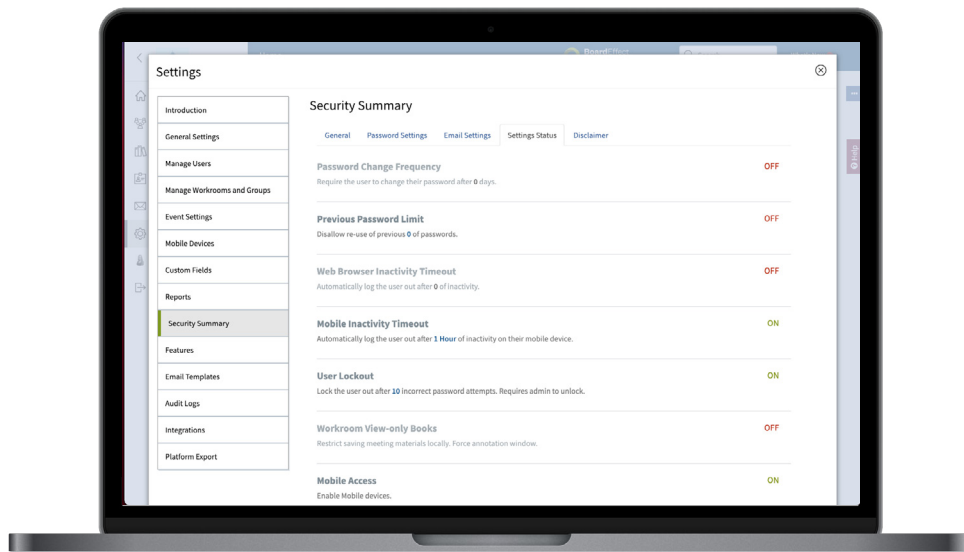


# 7 out of 10

charities do not have board members or trustees explicitly responsible for cyber security<sup>3</sup>.

“Cybersecurity readiness is a choice. Create adequate, reasonable, consistent, and effective controls that are credible and defensible with your key stakeholders.”

**Paul Proctor**  
Gartner<sup>5</sup>



# Questions Your Volunteer Board Needs to Ask About Security in a Board Management Solution

If you ask a board management solution provider about the strength of their platform's security, they're bound to play up their product's benefits and advantages. The challenge for volunteer boards is knowing which questions to ask to get at the heart of whether a claim of security is valid.

A good rule of thumb for your board to rely on is "trust but verify." Many Software as a Service (SaaS) providers claim to be certified, yet they haven't gone through the official process.

Gartner suggests that boards and senior executives are making poor investment decisions in board management solutions because they're asking the wrong questions.<sup>5</sup>

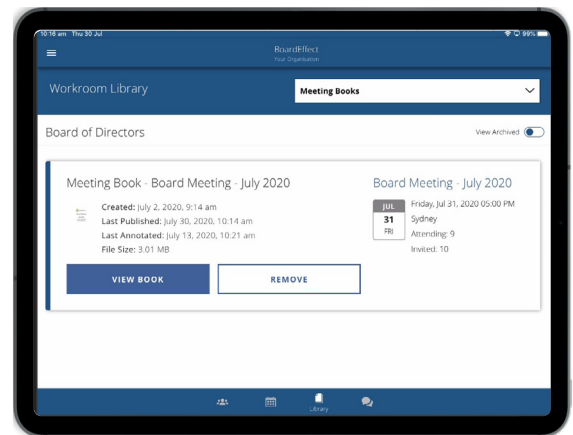
As you perform due diligence in assessing board management solutions, be aware that a hosted data center (AWS, for example) may be ISO 27001 certified but the nonprofit that uses the data center as Infrastructure as a Service (IaaS) may lack internal controls. As a result, the nonprofit believes its system is secure when it isn't.

AWS's "shared responsibility model" clearly states, "AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services." Customers are responsible for "security in the cloud".<sup>6</sup>

It's essential to understand that by accepting claims about security in volunteer board management systems without evaluating end-to-end security, your board is not appropriately addressing cybersecurity risks, and that could have a serious negative impact on your organisation in the future.

## What are the right questions?

- What security certifications does your nonprofit board management solution have?
- Who holds the security attestations? The hosting provider? Platform provider?
- Does the solution store data in the cloud and is it a shared cloud environment?
- Are your servers located in various geographical locations?
- Are servers stored in locked rooms and facilities?
- Can the vendor provide documentation from an independent source to verify their certifications?



# Substantiating a Board Management Solution Vendor's Claims About Security

To help your board make sense of the technical jargon, the two main certification programs for software programs are ISO and SOC. Both certifications require a third-party independent auditor to conduct a rigorous review of the controls, and both standards focus on information controls that involve people, processes, and technology.

What separates them is SOC 2 is an attestation process and ISO 27001 is an accredited certification program. With that in mind, it's possible for a data center to be ISO 27001 certified but not be SOC 2 certified. The SOC 2 Type II report is more in-depth and includes auditor opinions.

BoardEffect, a Diligent brand, has a continuous certification process that's updated annually.

BoardEffect ensures security around the platform. To provide even greater security, our data is hosted in a private cloud in a multi-tenant environment, and our equipment is housed in secure, locked storage rooms and facilities. With BoardEffect, your board gets cybersecurity control down to the document level within the platform.

“Ransomware continues to be a successful cyberattack and although the extent of the harm is underreported by most victims, ransomware remains hugely profitable for individuals and group offenders and equally disruptive for victims.”

**National Fraud Intelligence Bureau (NFIB)**  
Action Fraud <sup>7</sup>

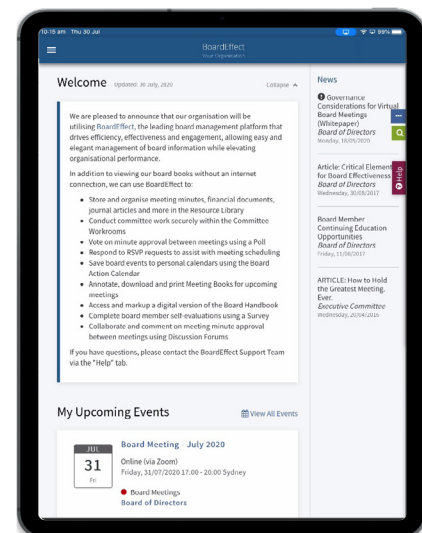
Beyond managing security issues, the pressure is on for nonprofit boards to work efficiently and transparently. BoardEffect provides your board with an all-in-one board management system that ensures efficiency, transparency, and efficiency in one valuable program.



The following certifications for the BoardEffect platform are a key differentiator that sets our products apart from competitors:

- ISO 27001 (2013)
- ISO 27017 (2015)
- ISO 27018 (2019)
- SOC 2 Type I
- SOC 2 Type II
- SOC 1 Type II
- HIPAA.HITECH Act

In 2021, we added 2 Diligent modules (Minutes, and Messenger to ISO 27001, SOC 2, and HIPAA certifications).



## References

- [1] <https://cyberpeaceinstitute.org/news/the-dark-side-of-cyberspace-the-threat-to-ngos-and-nonprofits-2/>
- [2] <https://www.forbes.com/sites/forbestechcouncil/2022/11/08/the-necessity-of-cybersecurity-in-the-non-profit-sector/>
- [3] <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>
- [4] <https://www.gartner.com/en/documents/3980890>
- [5] <https://www.gartner.com/en/experts/paul-proctor>
- [6] <https://aws.amazon.com/compliance/shared-responsibility-model/>
- [7] [https://www.ncsc.gov.uk/files/Cyber\\_threat\\_report-UK-charity-sector.pdf](https://www.ncsc.gov.uk/files/Cyber_threat_report-UK-charity-sector.pdf)

## About BoardEffect

---

**We're passionate about the work of boards, which drives how we develop the BoardEffect solution.**

Boards operate in a series of overlapping cycles: a regularly scheduled meeting cycle, an annual operating cycle, and the cycle of longer-term board development and engagement. BoardEffect's solution supports a modern approach to governance, powering boards' interdependent responsibilities across these ongoing cycles.

**BoardEffect Global 24/7 Support**  
support@boardeffect.com

**United States**  
+1 800 961 6429

**United Kingdom**  
+44 208 819 7320

**Australia**  
+61 1300 731 253

**South Africa**  
+27 21 205 1491