INSTITUTE OF COMMUNITY DIRECTORS AUSTRALIA
▸Knowledge ▸Connections ▸Credentials

ourcommunity.com.au
Where not-for-profits go for help

Ten questions every board director needs to ask about cyber security

Not-for-profits collect highly sensitive personal information, including information on people's health, relationships and finances (how does your organisation store donor credit card details, for example?). And their data often includes information about some of society's most vulnerable people, who are the core business of many not-for-profits.

At the same time, the sector has little cash to invest in built-for-purpose secure IT systems, so often this information is collected and stored via online third-party tools and basic apps such as Excel spreadsheets, and many organisations are reliant on off-the-shelf systems designed for the corporate and public sectors. Compounding these challenges, many NFPs find it difficult to recruit people with strong IT skills because they are in high demand and therefore expensive.

With all of these cyber security risks creating potentially rich pickings for cyber criminals – and the potential for serious reputational damage – not-for-profit board directors have a critical role to play in asking the right questions of their organisational leaders.

1. Who's accountable for what?

Whose job is it to look after tech systems and cyber security? In some NFPs, this will be the business manager or the CEO. In organisations without paid staff, it would be appropriate for the "IT person" to have a role on the board. This person's accountabilities might include choosing computers, hardware, software, third-party applications and virus protection, updating systems, and documenting that this has taken place. Clear accountability means that if there is a problem, there is a clear trail of events to show how the organisation can

prevent it from happening again. Remember the story of Everybody, Somebody, Nobody and Anybody and the important job to be done? The punchline is that Everybody blamed Somebody when Nobody did what Anybody could have. Accountability is key.

2. Who has access to what?

Do you have proper systems for managing access to data? What happens when people leave your organisation? What system do you have in place for ensuring they can no longer access private information (including passwords)? Who manages it? What about internally – does every staff, volunteer and board member need access to every piece of information? Do you have a system for ensuring that each person has access to the information they need to do their job but doesn't have access to things they don't need?

3. Are our policies fit for purpose and up to date?

What policies do you have to protect your organisation and the privacy of those who interact with you? How does the organisation ensure that these policies are easy to understand and easy to follow, and that they are updated as often as they need to be? How do you know that the policies are being followed?

4. Is our staff training up to date?

Staff need to know how to prevent data losses and data breaches, so it's important that the organisation has a system for checking that everyone's training is up to date. "Everyone" includes staff, volunteers, board members, and anyone else who has access to the organisation's IT systems.

5. Are our computers and systems fit for purpose?

Old computers tend to be more vulnerable to hackers because hacking and ransomware evolve all the time. Automatic updates offered by manufacturers can be all that is needed to protect your systems, so do you have a system in place for ensuring all staff update their computers as required, or does the organisation have a way to do this automatically? Similarly, are your anti-virus systems up to date?

6. What are our biggest threats?

An organisation that keeps most of its data in the cloud faces different risks from those that store it locally. Those with data in the cloud must consider downtime: how will you access your data if the server is down? How will you prevent your organisation from being hacked, and outsiders accessing your users' private data? Hacking, ransomware and viruses are only three risks to the security of your organisation's data, reputation and finances; others include (but are not limited to) weak passwords, insider threats, social media attacks and mobile phone breaches.

7. Does our culture protect our data?

A psychologically safe culture is one in which staff are more likely to report concerns regarding the safety of the system you use, and mistakes they might make, meaning they will not go unresolved. Similarly, a culture in which people have inherent respect for one another is most likely one which will respect the privacy of others, and take policy adherence seriously.

8. How do we make decisions which could affect cyber security?

The clear communication of organisational expectations regarding accountability, culture, policies and risk appetite will help set the tone for how decisions on cyber security are made. The board should have visibility of the organisation's appetite for risk regarding privacy and cyber safety to ensure that IT purchases are aligned with it.

9. What would we do if a data breach occurred?

Planning for "what if" scenarios is important, partly because it helps ensure sufficient measures are in place to prevent a breach from occurring. In the unfortunate event of a data breach, communication and problem solving are crucial. Does the organisation have a communication plan so that all those affected can be safely informed of the incident? Have you nominated the team of people who will be involved in identifying and containing the problem that caused the breach?

10. Cyber insurance: is it worth it?

Many insurance policies do not cover cyber attacks so an incident can be highly costly in terms of loss of data, loss of community trust and loss of the ability to operate effectively for a period of time. With that in mind, putting preventive systems and policies in place can be low cost and free; investing in up-to-date computers can be expensive but also critical in future proofing the organisation.

More information

Damn Good Advice on Cyber Safety and Fraud Prevention
Privacy Policy template
NFPs must respond to data threats to comply with laws