CYBERSECURITY FOR NOT-FOR-PROFITS

a White Paper by eStorm AUSTRALIA

1300 378 676

sales@estorm.com.au

CONTENTS

Introduction

If you're in the not-for-profit business, then odds are you want to help people. Well, what if I told you that your not-for-profit may be endangering every person you come into contact with? Cybersecurity and privacy have not always been a top priority amongst not-for-profits. The bitter truth is that cyber criminals won't think twice about targeting charities, foundations or any organisation trying to make a positive difference in the world.

Your data, applications and information are at the very core of your organisation. Those who have faced cyberattacks will agree that a data breach can potentially bring everything you have built crumbling to the ground.

Don't believe me? Let's take a look at Blackbaud.

In May 2020, the US data services and software company Blackbaud experienced one of the worst data breaches in the history of not-for-profits. Personal information, including social security numbers, driver's licenses, passport details, healthcare records, financial information, email addresses, legal names and birth dates were amongst the data leaked. While the exact number of victims is still unknown, the Identity Theft Resource Center (ITRC) has tracked 536 organisations and nearly 13 million people who were affected by the breach.

The leak was a result of a ransomware attack carried out on February 7th, 2020, which wasn't detected until three months later on May 14th. While the perpetrator was eventually locked out of the system, the damage was done, and a vast amount of information had already been copied. The hackers offered to erase the leaked information in exchange for an undisclosed amount of money. Though Blackbaud has maintained that the data was deleted after the ransom was paid, they have not provided any details of the confirmation.

Since the data breach, Blackbaud has undergone significant damage to their reputation and are still facing an ongoing class action lawsuit. The complaints accuse Blackbaud of, "neglecting to implement security measures to mitigate the risk of unauthorized access, utilizing outdated servers, storing obsolete data, and maintaining unencrypted data fields." The lawsuit also alleges that Blackbaud failed to respond to the threat in a timely manner and neglected their legal obligation to report the incident to data control authorities and customers.

Unfortunately, there is no 100% effective way to prevent your network, web portal or database from falling victim to a cyberattack. However, Blackbaud's data breach could have been prevented had they had the foresight to implement better cybersecurity strategies. We strongly encourage you to follow the strategies outlined in this white paper to protect your own data, as well as the information of donors, volunteers, and clients, against malware and cyber threats.

Why are Not-For-Profits Targeted?

While not-for-profits may not be the obvious choice for cyber criminals, the reality is that 43% of cyberattacks are committed against small businesses, with non-profit and for-profit organisations being equally affected. Let's take a look at some of the reasons not-for-profits are targeted:

FINANCIAL TRANSACTIONS

Chances are your not-for-profit relies strongly on the financial support of the public to keep operating. The bad news is that all online transactions (donations, ecommerce, subscriptions, etc) result in the capturing of personal financial information, such as banking accounts and credit card details. This makes your not-for-profit a prime target for any cyber criminal looking to profit from financial fraud.

INFORMATION COLLECTION

Not-for-profits collect an enormous volume of data relating to their clients, employees, volunteers, and supporters. Email addresses, phone numbers, legal names, health care records, identity documents...not-for-profits are a veritable treasure trove for would-be hackers. Cyber criminals are notorious for stealing personal information to either sell on the dark web, or to commit acts of identity theft, fraud, and extortion. Depending on the reach of your not-for-profit, you could be potentially endangering millions of people.

LACK OF CYBERSECURITY

Unfortunately, most not-for-profits lack the expertise, skill and resources to build a robust cybersecurity framework. According to the Nonprofit Technology Enterprise Network (NTEN), 80% of not-for-profits have not implemented any policies or procedures to address cyberattacks. Furthermore, 70% have never even evaluated their cyber security posture or undergone a vulnerability assessment. If your not-for-profit falls into any of these categories, then it's only a matter of time before you fall prey to a cyber criminal.

Is Your Not-For-Profit at Risk?

Not-For-Profit organisations face unique cyber security risks. While there's a multitude of threats to watch out for, we've put together a list of the most common attack vectors used against not-for-profits.

Online Portals
Not-for-profit websites that include donation or fundraising portals are vulnerable to cyberattacks, especially ones that utilise third-party payment systems. Without adequate security measures to protect sensitive banking and credit card information, these portals may be exploited for financial gain. Cyber criminals may even disguise themselves as potential donors in search of system gaps or loopholes.

Social Engineering
Social engineering attacks such as phishing, pretexting, baiting, and quid pro quo, are often used to scam individuals into revealing confidential information. These attacks use deception and fake communications to trick the receiver into supplying private, commercial, or financial information. Social engineering attacks are also used to compromise an organisation's cybersecurity infrastructure, by duping the victim into installing malware.

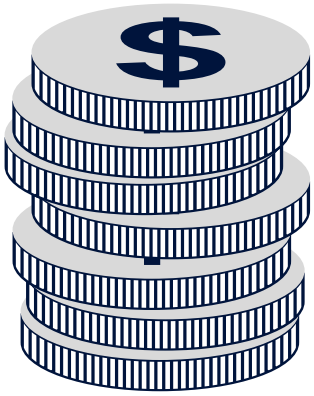
Ransomware and Malware Attacks
Malware is malicious software commonly used by criminals to steal confidential information or to install damaging programs onto devices without the user's knowledge. One of the most popular malwares amongst cyber criminals is ransomware, which is used to render computing devices and/or files unusable until a ransom is paid. Between 2019 and 2020, ransomware attacks increased by 62%. The prevalence, sophistication, and severity of malware-based cyberattacks has impacted all industries, including the not-for-profit sector.

Insider Threats
The State of Nonprofit Cybersecurity Report published in 2018 by NTEN, found a worrying lack of cyber security training amongst not-for-profit organisations. Volunteers, though well-intentioned, are not always the most cautious when it comes to cyber security. This is compounded by the fact they typically aren't as scrutinised as paid employees. Despite this lack of oversight, volunteers still regularly end up with access to digital resources and security clearances.

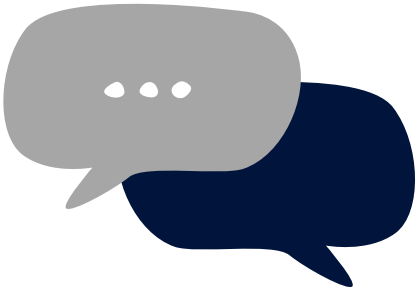
Denial of Service
Denial of Service is a type of attack against a service that allows the attacker to take control of the service that disrupts its normal function and prevent other users from accessing it. Not-for-profits who focus attention on sensitive religious, social, and political issues are often the intended targets of these kinds of cyberattacks. Cyber criminals who disagree with the not-for-profits core mission may attempt to sabotage the organisation's efforts by attempting to crash their online systems, networks, machines, or programs.

How Cyberattacks Can Affect Your Not-For-Profit

Let's take a further look into how your not-for-profit could be affected by a cyberattack:



Financial damages can occur from theft of banking or credit card information, the costs involved with getting your systems running again and clean-up costs. These expenses may include hiring IT professionals, replacing devices, implementing new IT infrastructure, procuring software, etc. Furthermore, disruptions to trading (e.g., the inability to carry out online donations), can also lead to a loss in revenue.



Reputational damages can erode the trust the public has for your not-for-profit. The not-for-profit business model relies on donations to fund the organisation's efforts. Many individuals may hesitate to provide the details necessary to donate after learning of any cybersecurity incidents. Trust is therefore essential to building and maintaining relationships with donors, to lose their confidence would be to lose everything. Furthermore, reputational damage can also negatively impact dealings with other important parties including government and regulatory bodies, media outlets and external partnerships.

Legal consequences are also a potential result of a cyberattack. Data protection and privacy laws require you to maintain and manage the security of all personal data you hold for your employees, volunteers, and donors. In Australia, not-for-profits are governed by The Privacy Act and must follow The Australian Privacy Principles (APPs). The APPs consist of 13 legally binding principles that outline the basic requirements organisations need to follow when collecting, using, disclosing, and storing personal information. If a not-for-profit has failed (accidentally or intentionally) to protect this data, they may face legal and financial penalties.

How to Protect Your Not-For-Profit from Cyberattacks

Here's a few tips to help your not-for-profit improve cybersecurity:

1. Restrict Access
Limiting the number of people who have access to digital tools and sensitive information can greatly reduce the chances of any cybersecurity breaches. Every employee, volunteer, client, and external partner should only need access to the resources pertaining to their individual roles.

2. Protect Devices
Separate devices and online accounts should be allocated for personal and business use. Avoid connecting any untrustworthy hardware (such as USBs, external hard drives, CDs, and DVDs) into computers, mobile devices, or IT networks.

3. Install Cybersecurity Software and Encryption Tools
Antimalware, firewalls, network monitors and intruder detection systems can help stop unauthorised access to networks, as well as alert users of any strange activity.

4. Be Cautious When Using the Internet
Only use a secure browser connection when accessing the internet. The web browser cache, temporary internet files, cookies and internet history should be cleared as often as possible. Never respond to any suspicious pop-up windows and install a pop-up blocker if possible.

5. Use Effective Passwords
All passwords should follow best practice guidelines, this includes:

- Containing at least 8 characters, including upper and lowercase letters, numbers and at least one special character
- Changed every 3 months
- Never reusing old passwords

Employing multi-factor authentication login methods is also recommended, as they require additional tokens to verify user identity and greatly reduce the chance of unauthorised access to accounts and devices.

6. Encourage a Culture of Cybersecurity Awareness

Every member of your team should be educated in cybersecurity best practices and the steps they can take to mitigate the risk of cyberattacks. Ongoing training should be provided to help foster a culture of personal responsibility and cybersecurity awareness.

7. Never Disclose Private Information

All information regarding your not-for-profit's IT environment should be kept on a need-to-know basis within your organisation. Information relating to usernames, passwords, operating systems, firewalls, internet browsers, applications, software, programs, and cybersecurity protocols should never be shared with anyone outside of your not-for-profit, except in the case of outsourcing IT needs to managed service providers and cybersecurity professionals.

8. Have a Reliable Backup System

Having a reliable back up system in place eliminates the danger of losing data, even in a worst-case scenario. It ensures that all organisational information is readily available, even if your not-for-profit suffers a cyberattack, accidental deletion, hardware failure or even a natural disaster.

Cybersecurity Audits

A cybersecurity audit will uncover what you are doing wrong when it comes to your network and systems security. For this reason, conducting a Cybersecurity audit or assessment at least once every year is vitally important.

While there are self-assessment resources available, we suggest employing a cybersecurity expert for your initial audit. An expert will be able to provide unbiased perspective and will create an actionable and airtight approach to mitigating problems identified.

Cybersecurity Self-assessment

The department of Industry, Science, Energy and Resources developed a tool to help you identify your organisation's cyber security strengths and areas where your can improve. It is mainly aimed at small/medium businesses however, any business can utilise the tool.

The tool will go through a series of questions regarding how you currently manage your cyber security risks and then will arm you with a list of recommendations to action based on your answers.

You can access the tool here:
https://digitaltools.business.gov.au/jfe/form/SV_cRMe9MTmaq6QmrA?ref=bga

Implementing an ISMS

To help eliminate or mitigate the risk of an information systems security breach that could have legal or business continuity effects, organisations should implement an Information Security Management System (ISMS).

There are multiple approaches to implementing an ISMS and depending on the level of certification required, the burden of implementation can be high. When in place however, an ISMS provides the following benefits:

- **Information is protected from getting into unauthorised hands**
- **Information is accurate and can only be modified by authorised users**
- **The risks of a breach have been assessed and the impacts mitigated**
- **Improved business reputation and increased confidence in your not-for-profit**

ISO 27001

The gold standard for ISMS is the ISO 27001 certification. This is an internationally recognised accreditation covering 114 controls across 14 sections and is applicable for any sized organisation. This requires external auditing and typically takes an internal team many months to achieve full implementation and certification.

You can read more about ISO 27001 here:
https://www.estorm.com.au/it-support-services/iso-27001-services-consulting/

The DESE and ISMS Scheme

The Department of Education, Skills and Employment's (DESE) Information Security Management Scheme calls for all providers of employment skills, training, and disability employment services to gain ISO27001 and Right Fit for Risk (RFFR) accreditation. Certification allows organisations to tender for deeds and provides assurance that government data and personal information is handled securely.

You can read more about the Information Security Management Scheme here:
https://www.estorm.com.au/news/right-fit-for-risk-and-iso27001-what-is-the-dese-isms-scheme/

Right Fit For Risk

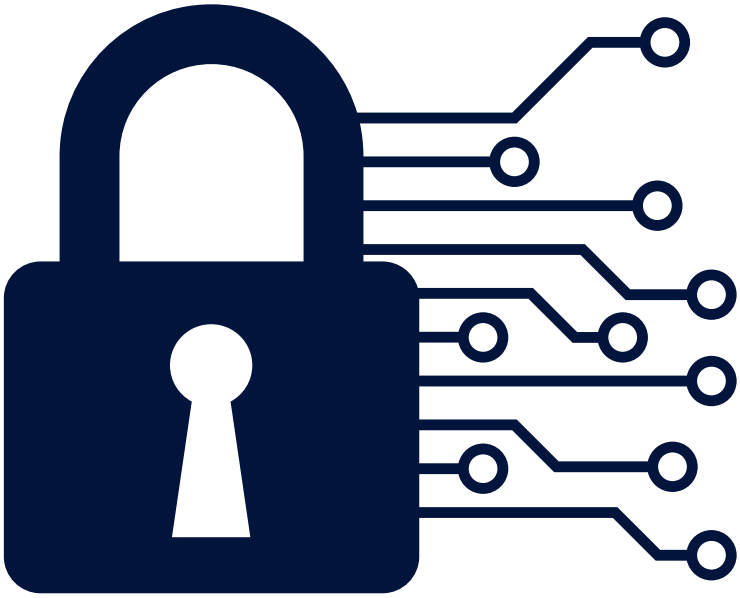
The DESE Information Security Management Scheme customises the baseline requirements of ISO 27001 with additional controls set by the Australian Government's Information Security Manual (ISM). Alongside the baseline requirements of ISO 27001, you must also develop a Statement of Applicability that considers the specific security risks and needs of your organisation, and the applicability of controls outlined in the Australian Information Security Manual. The Statement of Applicability addresses RFFR core expectations, such as the Australian Cyber Security Centre's Essential Eight strategies, personnel security, and data sovereignty.

You can read more about Right Fit For Risk here:
https://www.estorm.com.au/it-support-services/rffr-dese-ism-scheme/

ISMS.online

ISMS.online is an information security management software designed to accelerate and streamline the ISO 27001 process, by supplying all the necessary framework, tools and content required to achieve to meet the ISMS standard. The cloud-based platform provides everything your not-for-profit needs to create or improve your ISMS, privacy information, and business continuity systems.

ISMS.online also supports a host of other standards, policies, and regulations. These include but are not limited to:



- Other ISO certifications
- Cybersecurity Compliance
- Data Protection & Privacy Impact Assessments
- Employee Inductions, Exits & Recruitment
- Business Impact Assessments
- ISMS Audit Frameworks

Not-for-profits are eligible for a 25% discount on ISMS.online's services.

You can read more about ISMS.online here:
https://www.estorm.com.au/it-support-services/information-security-management/