Grassroots IT

THE NON-PROFIT GUIDE TO CYBER SECURITY

www.grassrootsit.com.au

CONTENTS

Dear Reader

Non-profit organisations face many unique challenges, not least of all around data security & privacy. While focused on the crucial mission of creating social impact, many non-profits find themselves increasingly vulnerable to cyber threats. This ebook is designed to equip you with the knowledge and strategies necessary to protect your organisation from escalating cyber-attacks.

As a non-profit leader, you may feel overwhelmed by the complexities of cybersecurity, especially when juggling numerous responsibilities and limited resources. However, the importance of safeguarding your digital assets cannot be overstated. Effective cybersecurity measures protect not just your data, but your reputation, donor information, and most importantly, the people you serve.

This comprehensive guide will walk you through:

- **The unique cybersecurity challenges facing non-profits**
- **Common cyber threats and how to recognise them**
- **Dispelling myths about cybersecurity in the non-profit sector**
- **Practical, low-cost strategies to enhance your cybersecurity**
- **Advanced measures for those able to invest more in security**
- **Building a cyber-resilient organisation**
- **Compliance and legal considerations**

Whether you're new to cybersecurity or looking to strengthen your existing measures, this guide provides actionable insights tailored to the non-profit sector. Remember, the biggest threat to your organisation's cybersecurity is complacency. By engaging with this material, you've already taken the crucial first step towards protecting your non-profit.
Let's embark on this journey to secure your mission, protect your stakeholders, and build a resilient future for your non-profit organisation.

Ben Love
Founder & Managing Director

Introduction

Non-profit organisations face unique challenges in cybersecurity. Committed to their missions of creating social impact, they must navigate the expanding array of cyber threats. Technology has improved the efficiency and effectiveness of tasks, from aiding in fundraising to communicating with donors and volunteers. However, the increased use of technology also leads to greater risks of cybersecurity threats.

According to statistics from the 2023 Global Risks Report the World Economic Forum, cyberattacks are among the top 5 global risks in terms of likelihood. This means that organisations, including non-profits, need to take cybersecurity seriously to protect their assets and data.

Staying informed and proactive is crucial for non-profits to safeguard their operational integrity and focus on their core missions.

The Unique Cybersecurity Challenges for Non-profits

Non-profit organisations operate with limited resources, which unfortunately makes them appealing targets for cybercriminals. They are also entrusted with the management of sensitive information, encompassing details about both donors and beneficiaries, and are frequently in charge of substantial financial resources.

Given the challenges posed by limited staffing and budgetary constraints, non-profits encounter unique hurdles in the realm of cybersecurity. This vulnerability underscores the pressing need for comprehensive security measures. It is crucial to safeguard sensitive data and uphold the operational integrity of these organisations. This not only protects the organisation but also the individuals and communities they serve.

Unfortunately, many non-profit organisations are ill-prepared to handle cyber threats, leaving them vulnerable to attacks with potentially devastating consequences, such as:

› **Budget Constraints:** Limited funding can restrict access to advanced cybersecurity tools and expertise.

› **Awareness and Training:** Staff may lack cybersecurity awareness, leading to vulnerabilities.

› **Data Sensitivity:** Non-profits handle sensitive information, including donor details and beneficiary data, making data breaches particularly damaging.

› **Legacy Systems:** Many non-profits rely on outdated software and systems due to budget constraints, which can have unpatched vulnerabilities.

› **Financial Loss:** A successful cyberattack on a non-profit can result in direct financial losses from stolen funds or ransomware, not to mention costs involved in recovering from the incident and returning operations to normal. For smaller non-profits with limited resources or lacking cyber-insurance, the consequences can be catastrophic.

› **Third-Party Relationships:** Non-profits often collaborate with various third parties, which can introduce additional cybersecurity risks, particularly if those partners lack robust security measures.

› **Volunteer Workforce:** A significant portion of the non-profit workforce may consist of volunteers who have not received comprehensive cybersecurity training.

Understanding the Threats

Non-profit organisations need to stay vigilant and up to date about the various cybersecurity threats they may encounter. Here are common threats:

› **Social Engineering:** This is a broad term that encompasses various tactics used by hackers to manipulate people into giving away sensitive information or taking certain actions. Social engineering can be difficult to defend against using only technology which is why complementary methods such as cybersecurity awareness training is important.

› **Phishing Attacks:** These are deceptive emails sent by cybercriminals to trick individuals into revealing sensitive information or installing malware. They can be highly targeted, using personal information to increase their success rate.

› **Ransomware:** This is a type of malicious software that encrypts an organisation's data and demands a ransom for its release. The impact on non-profits can be severe, disrupting operations and potentially leading to substantial financial losses.

› **Distributed Denial of Service (DDoS) Attacks:** These attacks overload an organisation's servers with traffic, making their online services unavailable. Non-profits that rely on online donations or services are particularly vulnerable.

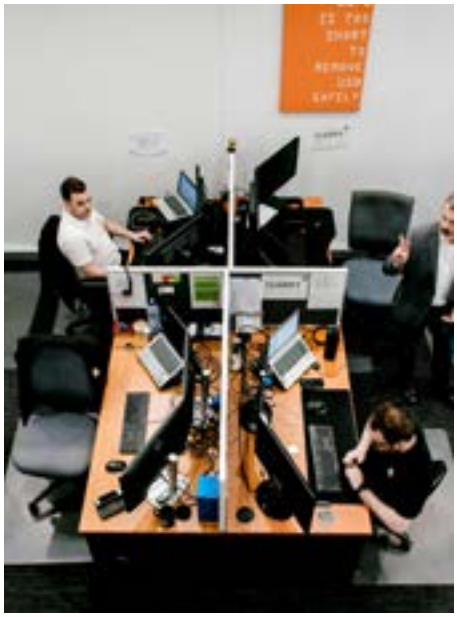
› **Business Email Compromise:** This is a type of fraud where hackers gain access to your email system and use social engineering tactics to trick employees into transferring money or sensitive data to them.

› **Supply Chain Attack:** This is an attack where hackers target a company's suppliers or partners to gain access to their systems, and then use that access to compromise the main target. Recent high-profile examples include the SolarWinds and 3CX supply chain attacks.

› **Data Breaches:** Unauthorised access to sensitive data, such as donor details or beneficiary records, can lead to serious repercussions. These can include damage to the non-profit organisation's reputation and potential legal consequences.

› **Insider Threats:** These threats can come from insiders, whether malicious or accidental, who have access to the organisation's systems and data. This includes volunteers or employees who may unintentionally expose vulnerabilities or intentionally misuse their access. By understanding these threats, non-profits can better prepare and implement strategies to mitigate their risks.

Busting the Myths



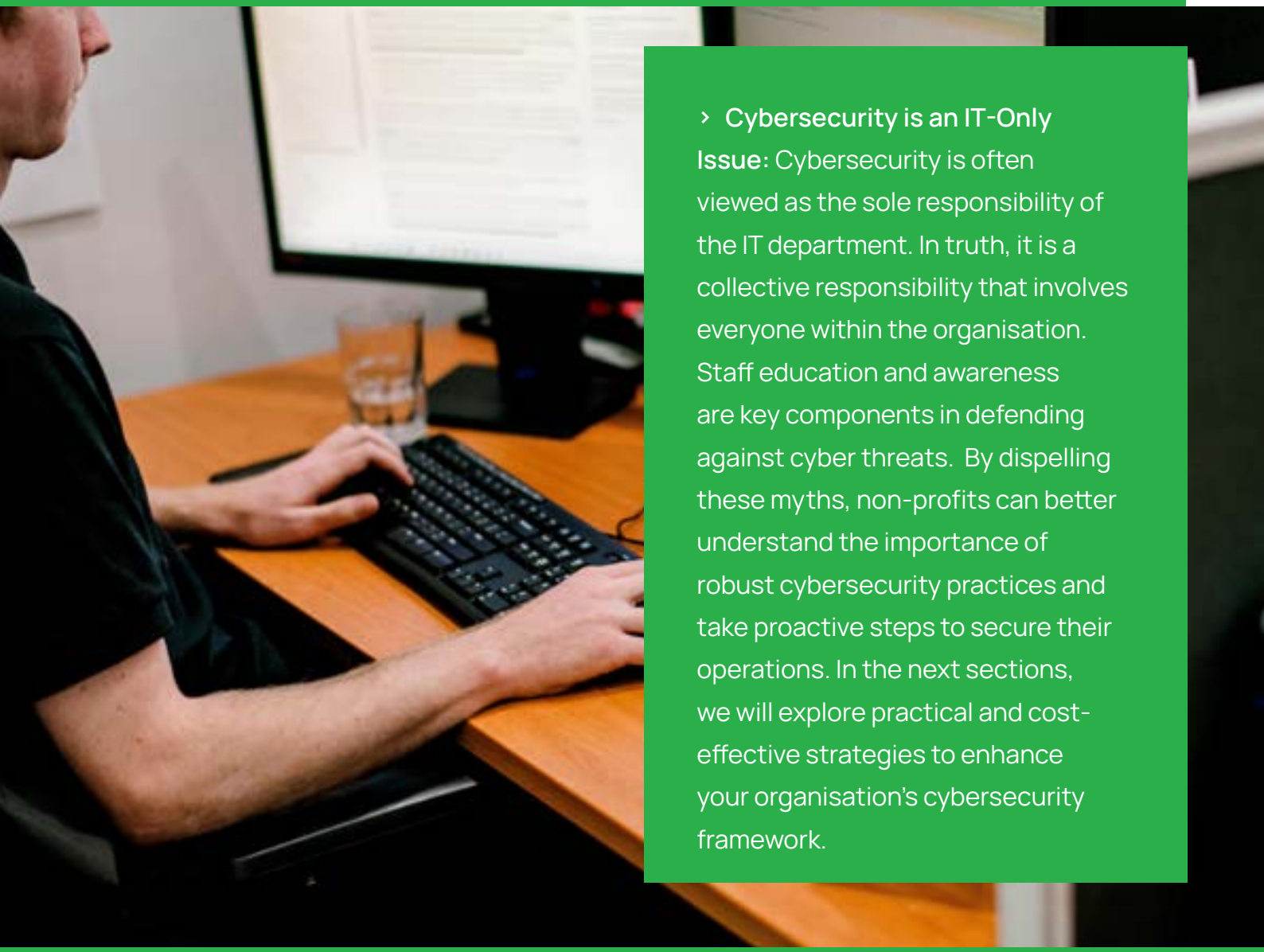
Several misconceptions hinder effective cybersecurity practices for non-profit organisations. Dispelling these myths is essential for cultivating a culture of security awareness and proactive defence mechanisms. It is important to debunk these myths to have a clear understanding of what you need to do to protect your non-profit organisation.

› **Our Organisation is Too Small to be Targeted:** Many non-profits believe that their limited size and scope make them unattractive to cybercriminals. However, this misconception couldn't be further from the truth. Cyberattacks can target any organisation, regardless of size, and smaller entities are seen as easier targets due to potentially weaker security measures.

› **We Don't Have Valuable Data:** Some non-profits might underestimate the value of their data, but cybercriminals do not. All data holds significant worth, especially donor details, financial records, and sensitive beneficiary information. Even seemingly insignificant information can be exploited for identity theft or financial fraud, presenting substantial risks.

› **Cybersecurity is Too Expensive:** Advanced cybersecurity solutions can be costly however, there are often affordable or even free resources available to non-profits. Implementing basic security measures can significantly reduce cyber risks without breaking the bank.

› **We Have Antivirus Software, That's Enough:** Antivirus software is a key component of your cybersecurity defences; however, relying solely on this measure falls short. Achieving comprehensive security necessitates a multi-layered approach. This includes the deployment of firewalls, encryption, regular backups, and continuous monitoring of systems and networks.



› **Cybersecurity is an IT-Only Issue:** Cybersecurity is often viewed as the sole responsibility of the IT department. In truth, it is a collective responsibility that involves everyone within the organisation. Staff education and awareness are key components in defending against cyber threats. By dispelling these myths, non-profits can better understand the importance of robust cybersecurity practices and take proactive steps to secure their operations. In the next sections, we will explore practical and cost-effective strategies to enhance your organisation's cybersecurity framework.

Low-Cost Cybersecurity Strategies for Non-profits

Given that non-profits manage sensitive donor information, financial records, and beneficiary data, it is crucial to employ budget-friendly yet secure solutions. Robust cybersecurity measures are essential to prevent significant reputational and operational harm. Here are low-cost strategies that non-profits can implement to strengthen their cybersecurity posture.

- **Employee training & awareness:**

  One of the most vulnerable areas of non-profit organisation's cybersecurity is its employees. It is crucial for non-profits to provide cybersecurity awareness training to all staff members, including volunteers, on safe internet practices and how to identify potential threats.

  As well as commercially available cybersecurity awareness training offerings, there are plenty of free resources available online, such as on YouTube. Running internal training sessions and information sharing workshops is also free and easy, and an excellent way of building cybersecurity awareness amongst staff and volunteers.

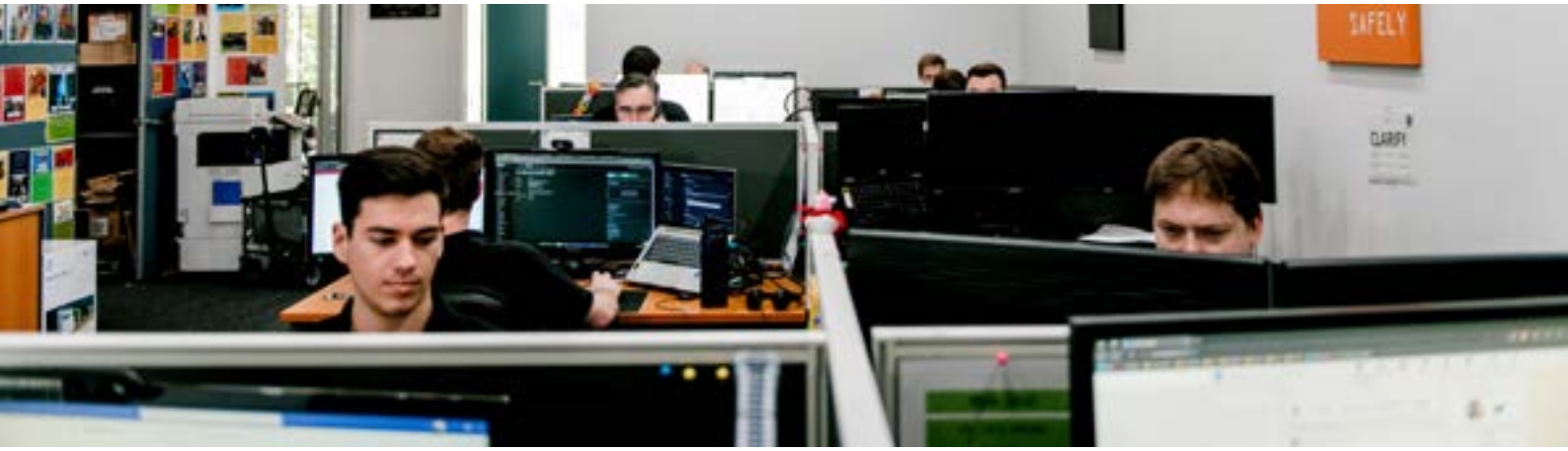
› **Vendor donations & discounted software:** Non-profits can leverage vendor donation programs to access a variety of technology solutions, including cybersecurity software and tools, either at a reduced cost or for free. Numerous tech companies, such as Microsoft, Canva, and Xero, offer specialised programs for non-profits, providing discounted or donated products and services. As an example of what's available, Microsoft offers up to 10 free licenses of Microsoft 365 Business Premium to qualifying non-profit organisations in Australia, with deep discounts for additional licensing over the initial 10.

How can this help non-profit cybersecurity? Microsoft 365 Business Premium includes many advanced cybersecurity features that other plans do not. Without these discounts many non-profits would be forced to rely on cheaper alternatives, missing important security & data protection benefits.

› **Partners that understand non-profits:** When selecting a non-profit technology partner, decision-makers should prioritise companies with a working knowledge of the unique challenges and needs of non-profit organisations. IT partners well-versed in the non-profit sector act as collaborators who align closely with the mission and values of the non-profit organisation.

This alignment is crucial, as it translates into more than just technical support – it is about providing cost-effective and mission-driven solutions. The right IT partner is not just a service provider but a strategic ally – one that empowers the non-profit to focus on their core mission, knowing that their technology needs are in capable and understanding hands.

It is important to ensure that non-profit cybersecurity solutions are carefully considered and right sized for the needs of the organisation, taking into consideration the organisational strategy, key risk areas and various constraints.



Cybersecurity Basics

While it may appear that advanced technology is key for robust cybersecurity, it is important for non-profit organisations not to overlook the fundamentals.

At a minimum, every non-profit should implement basic cybersecurity measures: these are essential steps that can significantly enhance your defence against cyber threats: The measures outlined below are either low-cost or free, ensuring they are readily accessible to non-profits operating on limited budgets.

› **Executive Support:**
Understanding and prioritising cybersecurity is non-negotiable for today's leadership. They must acknowledge the significance of protecting data and systems. Implementing cybersecurity practices is essential for non-profit organisations to defend against potential threats and preserve their operational integrity.

› **Develop a Cybersecurity Policy:**
Establish clear guidelines and procedures for staff and volunteers to follow. This includes data handling practices, access controls, and incident response protocols.

› **Use Strong Passwords and Multi-Factor Authentication (MFA):** Ensure that all accounts use strong, complex passwords and enable multi-factor authentication (MFA) wherever possible. MFA adds an extra layer of security by requiring a second form of verification beyond just a password.

› **Backup Data Frequently:** Implement a robust data backup strategy to ensure that all critical data is regularly backed up and stored securely. This can help in quick recovery in case of ransomware attacks or data loss incidents.

› **Regular Software Updates & Patching:** Keep all software, including operating systems, antivirus programs, and other applications, up to date. Regular updates often include patches for security vulnerabilities that cybercriminals could exploit.

› **Implement Access Controls:** Limit access to sensitive information based on role and necessity. Use the principle of least privilege to ensure that individuals have access only to the information they need to perform their duties. By integrating these basic cybersecurity practices, non-profits can build a more resilient defence against cyber threats.

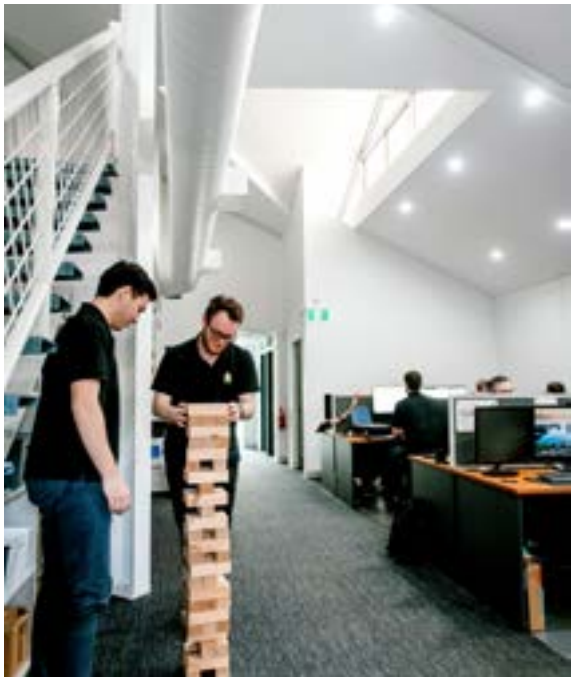
Advanced Cybersecurity Strategies

If your non-profit organisation can invest more in safety, consider the following advanced strategies:

› **Deploy Advanced Threat Detection Systems:** Invest in sophisticated threat detection systems like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). These tools continuously monitor network traffic for suspicious activities and can automatically block potential threats. Advanced detection systems use machine learning and artificial intelligence to adapt to new attack vectors, providing an added layer of defence.

› **Implement Endpoint Detection and Response (EDR):** Endpoint Detection and Response (EDR) solutions provide real-time monitoring and response capabilities for endpoints such as laptops, desktops, and mobile devices. EDR tools can detect, investigate, and mitigate suspicious activities quickly, reducing the risk of a successful cyber-attack. They also provide insights into potential vulnerabilities and help in maintaining comprehensive security across all devices.

› **Use Advanced Encryption Techniques:** Employ advanced encryption techniques to protect sensitive data both in transit and at rest. Implementing encryption protocols like Advanced Encryption Standard (AES) ensures that data remains secure even if intercepted by cybercriminals. Encrypting data at the file system level and using secure communication channels such as Virtual Private Networks (VPNs) can further enhance security.



› **Conduct Penetration Testing & Regular Audits:** Regular penetration testing involves simulating cyber-attacks to identify and address vulnerabilities in your systems. Engaging professional penetration testers or 'ethical hackers' to perform these tests helps uncover weaknesses before malicious actors can exploit them. These simulations provide a realistic view of your cybersecurity posture and guide necessary improvements.

› **Implement Zero Trust Architecture:** Adopting a Zero Trust architecture means that no one, inside or outside the network, is trusted by default. This approach ensures strict identity verification for every person and device attempting to access resources within the network. By continuously verifying users and monitoring for anomalous behaviour, Zero Trust mitigates the risk of insider threats and lateral movement by attackers.

› **Foster a Security-First Culture:** Creating a security-first culture involves integrating cybersecurity into every aspect of your non-profit organisation. Encourage all employees and volunteers to prioritise security in their daily activities and decision-making processes. Offer ongoing education, promote best practices, and recognise and reward security-conscious behaviour

to establish a collective commitment to cybersecurity.Incorporating these advanced strategies will significantly enhance the security posture of your non-profit organisation. By staying ahead of evolving threats and continuously improving your defences, you can protect your operations, data, and stakeholders from cyber risks.

Building a Cyber-resilient Non-Profit Organisation

The ongoing safety & stability of your non-profit necessitates the building of a cyber-resilient infrastructure. Cyber-resilient non-profit organisations are not only more capable of maintaining a secure stance long term, but they are also better equipped to withstand and recover swiftly from cyber-attacks. Key components of a cyber-resilient non-profit organisation can include:

› **Cybersecurity Policy:** Having a solid cybersecurity policy in place is crucial for setting expectations and guidelines for all employees and volunteers. This should outline best practices, procedures for handling sensitive data, and disciplinary measures for non-compliance. When compiling your cybersecurity policy pay particular attention to addressing requirements for remote workers.

› **Cybersecurity Awareness:** Educating your employees and volunteers on best practices for cybersecurity is crucial for maintaining a strong defence. This includes regular training sessions on topics such as social engineering, password security, and data protection. As with any cultural change, to be effective, a culture of cybersecurity awareness must be driven from the very top of the non-profit organisation.

› **Incident Response Plan:** In the event of a cyber-attack, having a well-defined incident response plan can help minimise damage and facilitate a quicker recovery for your non-profit organisation. This should include steps for containing the attack, notifying relevant parties, and restoring systems. Your Incident Response Plan should also work closely with your Non-profit Business Continuity Plan, given the high potential for a security breach to interrupt operations.

› **Cyber-Insurance:** Cyber-insurance can help mitigate the financial impact of a cyber-attack by not only facilitating recovery, but also covering costs such as data recovery, legal fees, and regulatory fines. The cyber-insurance industry is evolving at a breakneck pace as it scrambles to keep up with the evolving threat landscape, so it is advisable to speak with a cyber-insurance specialist, rather than a general insurance provider or broker.

The Value of Cybersecurity Frameworks

Adopting recognised cybersecurity frameworks can guide your efforts and demonstrate due diligence.

Varied frameworks are applicable to certain

situations, ranging from non-profits with immature cybersecurity through to organisations with extensive cybersecurity capabilities.

ACSC Essential Eight

Developed by the Australian Cyber Security Centre, this framework provides eight basic strategies for mitigating cyber threats. These include things like patching applications, restricting administrative privileges, and using multi-factor authentication. The Essential Eight is widely recognised and used across Australian business and government and is the ideal place to start for non-profit organisations of all sizes that have no previous framework in place.

NIST Cybersecurity Framework

Developed by the National Institute of Standards and Technology, this framework provides a comprehensive approach to managing and reducing cybersecurity risks. The NIST framework is comprehensive and best suited to non-profit organisations with more complex security needs.

ISO 27001

This international standard outlines the requirements for creating an Information Security Management System (ISMS). It provides a framework for identifying and addressing potential security risks.

Compliance & Legal Considerations

Non-profits must be mindful of legal requirements and compliance regulations. Adhering to data privacy laws is as essential for non-profits as it is for any other organisation. Regulations like the Australian Privacy Act set stringent rules for handling personal data.

Non-profits need to comprehend and follow these laws to prevent hefty fines and preserve their stakeholders' trust. Moreover, establishing robust data privacy measures can bolster non-profits organisations credibility and show dedication to protecting the privacy of donors and beneficiaries.

Privacy Act 1988

This act regulates how organisations handle and protect personal information. It includes requirements for data breach notification and imposes heavy penalties for non-compliance.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) applies to businesses that handle credit card information. It outlines security standards for protecting this sensitive data and ensuring secure transactions.

If you operate in international jurisdictions, other considerations may apply, such as:

GDPR:

The General Data Protection Regulation (GDPR) is a set of rules designed to protect the personal data of individuals in the European Union. Any business that collects or processes personal data from EU citizens must comply with GDPR standards.

HIPAA:

The Health Insurance Portability and Accountability Act (HIPAA) requires healthcare organisations to implement safeguards to protect patient information. This includes requirements for secure storage, transmission, and access control of electronic health records.

Notifiable Data Breaches (NDB) scheme

Under this scheme, if your non-profit organisation experiences a data breach that is likely to result in serious harm to individuals whose personal information is involved, you are legally obligated to notify both the affected individuals and the Office of the Australian Information Commissioner.

Importance of Regular Security Audits

Conducting regular security audits is a best practice for maintaining a strong cybersecurity posture. Security audits involve a comprehensive evaluation of an organisation's information systems, policies, and procedures to identify potential vulnerabilities and areas for improvement.

These audits can uncover gaps in security that might have been overlooked and provide actionable recommendations to enhance defences. Ensuring that security audits are performed periodically—and acting on the results—is vital for staying ahead of emerging threats and maintaining a resilient cybersecurity framework.

By incorporating these practices, non-profit organisations can build a secure environment that not only protects their data but also fosters trust and confidence among their stakeholders.

› **Data Protection Laws:** Understand and comply with relevant data protection regulations (e.g., GDPR, CCPA).

› **Reporting Requirements:** Know the mandatory reporting obligations in case of a data breach.

› **Third-party Agreements:** Ensure vendors and partners also adhere to strong cybersecurity practices.

Conclusion

As a Non-profit leader you don't need to be a cybersecurity expert, but you do need to have a clear understanding of the potential risks to your business, and the steps you can take to mitigate them. A good place to start is by having a security audit conducted to assess your current security posture and identify any vulnerabilities.

Cybersecurity is a critical aspect of running a successful non-profit organisation. By understanding the unique challenges, implementing basic and advanced strategies, and leveraging available frameworks, non-profits can significantly enhance their security posture. The journey toward robust cybersecurity may seem daunting, but with informed steps, it is achievable.

Secure your mission, protect your stakeholders, and build a resilient future. For more insights and resources, consider partnering with experts in the field and investing in continuous learning and improvement.

Grassroots IT

Take the Next Step in
Your IT Transformation Journey
Contact Grassroots IT today.

www.grassrootsit.com.au