CARE
MANAGED IT

The Non-Profit's Guide to Cybersecurity:

Investing in your Future by protecting Your Mission

Free downloads – https://www.caremit.com.au/freebees

By Roger Smith
Director of client security for CareMIT
CareMIT Mini Guide Downloads
LinkedIn profile: http:// au.linkedin.com/in/smesecurity

<u>PLEASE FORWARD TO OTHERS</u>

This is a FREE Guide. You are welcome to forward this guide or the webpage link https:// caremit.com.au/mini-guides to your clients and contacts.

For Publishers: Please feel free to use the content in this guide for publishing in magazines, newsletters, etc. Please do not change the substance of the content. Simply cite the author, publication title and website.
The abbreviated content in this document is taken in part from several publications by this author including his book "The CEO's Guide to Cyber Security".

Free downloads – https://www.caremit.com.au/mini-guides

Care Managed IT Pty Ltd
Unit 3, 116 – 118 Wollongong Street
Fyshwick, ACT 2609

Keep in touch! For new articles and guides
Email: sales@caremit.com.au
Downloads: https://www. Caremit.com.au/freebees
Twitter: @smesecurity
Linkedin: https:// au.linkedin.com/in/smesecurity
FaceBook: /better business security

Subscribe: Free subscription at www.caremit.com.au/newsletter

NOTE: The information in this guide is of a general nature only. When making decisions about your business it is strongly recommended that you seek qualified advice tailored to your needs and business situation.

The Importance of Cybersecurity for Non-Profits and Associations

In today's digital age, organizations of all sizes and types, including non-profits and associations, face an increasing threat of cyber-attacks.

These attacks can come in many forms, from phishing scams to data breaches, and can have devastating consequences for organizations that rely on sensitive data and intellectual property.

In the case of non-profits and associations, a successful cyber-attack can not only lead to the loss of important information, but also damage the organization's reputation and erode public trust.

The non-profit and association sectors are particularly vulnerable to cyber-attacks due to a number of factors, including limited resources, a lack of technical expertise, and a general assumption that they are not prime targets for cyber criminals.

However, non-profits and associations often hold a wealth of sensitive information, including donor data, financial information, and confidential information about their clients and members.

This information is valuable to cyber criminals, who can use it for financial gain or to cause harm to the organization and its stakeholders.

Despite the increasing threat, many non-profits and associations are still not taking adequate steps to protect their data and IP.

This is largely due to a lack of understanding of the risks and the steps that need to be taken to prevent cyber-attacks.

This guide is designed to help non-profits and associations understand the importance of cybersecurity, the threats they face, and the steps they can take to secure their data and IP against cyber-attacks.

In today's digital age, organizations of all sizes and types, including non-profits and associations, face an increasing threat of cyber-attacks.

The Importance of Cybersecurity for Non-Profits and Associations

This guide will serve as a valuable resource for organizations looking to protect themselves in today's digital landscape.

This guide is organized into five chapters, each focusing on a specific aspect of cybersecurity for non-profits and associations.

Chapter 1, we will provide an overview of why non-profits and associations are vulnerable to cyber-attacks and the impact a successful attack can have.

Chapter 2 will explore the current threat landscape, including common types of cyber-attacks and their methods.

Chapter 3 will discuss the development of a cybersecurity plan, including assessing the organization's current security posture and creating a policy.

Chapter 4, we will focus on employee awareness and training, including the role of employees in protecting the organization and best practices for training.

Finally, in Chapter 5, we will discuss incident response and recovery, including preparing for a cyber-attack, responding to an attack, and disaster recovery planning.

By the end of this guide, non-profits and associations will have a better understanding of the risks they face and the steps they can take to secure their data and IP against cyber-attacks.

We hope that this guide will serve as a valuable resource for organizations looking to protect themselves in today's digital landscape.

Introduction to Cybersecurity for Non-Profits and Associations

Non-profits and associations are facing an increasing threat of cyber-attacks, which can have devastating consequences for organizations that rely on sensitive data and intellectual property.

Despite the growing threat, many non-profits and associations are still not taking adequate steps to protect their data and IP, largely due to a lack of understanding of the risks and the steps that need to be taken to prevent cyber-attacks.

Why Non-Profits and Associations are Vulnerable to Cyber-attacks

Non-profits and associations are vulnerable to cyber-attacks for several reasons, including:

Limited resources:

Many non-profits and associations have limited resources, including budget and staff, which makes it difficult for them to invest in cybersecurity measures.

This can lead to a lack of investment in technical controls, such as firewalls and antivirus software, as well as training for employees.

Lack of technical expertise:

Many non-profits and associations do not have a dedicated IT staff, which means they may not have the technical expertise to properly secure their systems and data.

This can lead to vulnerabilities in the organization's security posture, making it easier for cyber criminals to penetrate the network.

Many non-profits and associations have limited resources, including budget and staff, which makes it difficult for them to invest in cybersecurity measures.

Introduction to Cybersecurity for Non-Profits and Associations

***Assumption of low risk*:**
Many non-profits and associations believe that they are not prime targets for cyber criminals, and therefore do not take cybersecurity seriously.

This assumption can lead to a false sense of security and a lack of investment in security measures.

Handling of sensitive information:
Non-profits and associations often hold a wealth of sensitive information, including donor data, financial information, and confidential information about their clients and members.

Many non-profits and associations believe that they are not prime targets for cyber criminals, and therefore do not take cybersecurity seriously.

This information is valuable to cyber criminals, who can use it for financial gain or to cause harm to the organization and its stakeholders.

The Impact of a Successful Cyber-attack on a Non-Profit or Association

A successful cyber-attack can have several devastating consequences for non-profits and associations, including:

Loss of sensitive information:
A cyber-attack can result in the loss or theft of sensitive information, including donor data, financial information, and confidential information about clients and members.

This information is valuable to cyber criminals, who can use it for financial gain or to cause harm to the organization and its stakeholders.

Financial losses:

A successful cyber-attack can result in significant financial losses for non-profits and associations, including the cost of repairing damaged systems, restoring lost data, and investigating the attack.

Introduction to Cybersecurity for Non-Profits and Associations

Reputational damage:

A cyber-attack can cause significant damage to the reputation of a non-profit or association.

The loss or theft of sensitive information can erode public trust and damage the organization's reputation, making it harder to attract donors and clients in the future.

Legal and regulatory implications:

Non-profits and associations that handle sensitive information, such as financial data and personal information, may be subject to legal and regulatory requirements.

A successful cyber-attack can result in legal and regulatory penalties, as well as reputational damage.

Non-profits and associations are vulnerable to cyber-attacks due to several factors, including limited resources, a lack of technical expertise, and a general assumption of low risk.

A successful cyber-attack can have devastating consequences, including the loss of sensitive information, financial losses, reputational damage, and legal and regulatory implications.

A successful cyber-attack can have devastating consequences, including the loss of sensitive information, financial losses, reputational damage, and legal and regulatory implications.

It is important for non-profits and associations to understand the risks and take steps to protect their data and IP against cyber-attacks.

Understanding the Threat Landscape

To effectively protect against cyber-attacks, it is important to understand the types of attacks that are most commonly used and the methods that cyber criminals use to carry out these attacks.

To effectively protect against cyber-attacks, it is important to understand the types of attacks that are most commonly used and the methods that cyber criminals use to carry out these attacks.

This chapter provides an overview of the most common types of cyber-attacks and discusses the current trends in cyber-attacks targeting non-profits and associations.

Common Types of Cyber-attacks

Phishing:

Phishing is a type of social engineering attack that is designed to trick individuals into revealing sensitive information, such as login credentials and financial information.

Phishing attacks are often carried out through emails that appear to be from a trusted source, such as a bank or a well-known company, and contain a malicious link or attachment.

Ransomware:

Ransomware is a type of malware that encrypts the victim's files, making them inaccessible.

The attacker then demands a ransom payment in exchange for the decryption key.

Ransomware attacks are particularly dangerous because they can result in the permanent loss of data if the ransom is not paid.

Malware:

Malware is a type of malicious software that is designed to cause harm to the victim's computer or network.

Malware can take many forms, including viruses, worms, and trojans, and can be spread through email attachments, malicious websites, or infected software.

DDoS:

DDoS, or Distributed Denial of Service, is a type of attack that is designed to overload a website or network with traffic, making it unavailable to users.

DDoS attacks can be used to disrupt the operations of non-profits and associations and can also be used as a smokescreen for other types of cyber-attacks.

SQL Injection:

SQL Injection is a type of attack that targets the databases of websites and applications.

The attacker injects malicious code into the database, which can then be used to steal sensitive information, manipulate the website, or carry out other types of attacks.

Understanding the Threat Landscape

Current Trends in Cyber-attacks Targeting Non-Profits and Associations

Cyber criminals are increasingly targeting non-profits and associations due to the valuable information that these organizations often hold.

The following are some of the current trends in cyber-attacks targeting non-profits and associations:

Targeted attacks:

Non-profits and associations are often targeted by cyber criminals who have specific motivations, such as stealing sensitive information or disrupting the organization's operations.

Targeted attacks are often more sophisticated than mass attacks and can be more difficult to detect and prevent.

Increased use of ransomware:

Ransomware attacks are becoming more common, and non-profits and associations are particularly vulnerable due to their limited resources and lack of technical expertise.

Cyber criminals are taking advantage of this vulnerability by targeting non-profits and associations with ransomware attacks.

Increased use of cloud services:

Non-profits and associations are increasingly using cloud services to store and manage their data.

While cloud services can offer many benefits, they can also create new security risks, as cyber criminals may target these services to steal sensitive information.

Social engineering attacks:

Social engineering attacks, such as phishing and vishing, are becoming more sophisticated, and non-profits and associations are particularly vulnerable to these types of attacks due to the trust they have built with their stakeholders.

It is important for non-profits and associations to understand the types of cyber-attacks that are most used and the methods that cyber criminals use to carry out these attacks.

By understanding the threat landscape, non-profits and associations can take steps to protect their data and IP against cyber-attacks.

Cyber criminals are increasingly targeting non-profits and associations due to the valuable information that these organizations often hold.

Developing a Cybersecurity Plan

To effectively protect against cyber-attacks, non-profits and associations must develop a comprehensive cybersecurity plan. This chapter outlines the steps necessary to assess the organization's current security posture, explains the importance of creating a cybersecurity policy, and discusses the implementation of technical controls, such as firewalls, antivirus software, and encryption.

Steps to Assess the Organization's Current Security Posture

Perform a security audit:

A security audit is a comprehensive assessment of an organization's security posture.

This can be done internally by the organization's IT staff or by an outside security consultant.

The security audit should include a review of the organization's current security policies and procedures, as well as an assessment of the technical security measures that are in place.

Identify potential threats:

The security audit should also identify potential threats to the organization's data and IP, such as unauthorized access to sensitive information, data breaches, and cyber-attacks.

This will help the organization prioritize its cybersecurity efforts and allocate resources where they are needed most.

Assess the organization's vulnerabilities:

The security audit should assess the organization's vulnerabilities, such as weak passwords, unpatched software, and outdated security measures.

This information will be used to determine which areas of the organization's security posture need to be strengthened.

To effectively protect against cyber-attacks, non-profits and associations must develop a comprehensive cybersecurity plan.

Developing a Cybersecurity Plan

A cybersecurity policy is a written document that outlines an organization's security posture and provides guidance to employees

Importance of Creating a Cybersecurity Policy

A cybersecurity policy is a written document that outlines an organization's security posture and provides guidance to employees on how to handle sensitive information and respond to security incidents.

The following are the key benefits of creating a cybersecurity policy:

Provides clear guidelines:

A cybersecurity policy provides clear guidelines for employees on how to handle sensitive information, such as passwords and personal data, and how to respond to security incidents, such as a data breach.

This helps ensure that employees are taking the necessary precautions to protect the organization's data and IP.

Enhances accountability:

A cybersecurity policy helps to ensure that everyone in the organization is aware of their responsibilities when it comes to security.

This enhances accountability, as employees are aware of the consequences of not following security procedures.

Helps prevent security incidents:

A well-crafted cybersecurity policy can help prevent security incidents by providing clear guidance to employees on how to handle sensitive information and respond to security incidents.

Demonstrates commitment to security:

Having a cybersecurity policy demonstrates to stakeholders, such as members, donors, and partners, that the organization is committed to protecting its data and IP.

Developing a Cybersecurity Plan

Technical controls are security measures that are designed to protect an organization's data and IP.

Implementing Technical Controls

Technical controls are security measures that are designed to protect an organization's data and IP.

The following are some of the technical controls that non-profits and associations should consider implementing:

Firewalls:

Firewalls are devices that act as a barrier between a network and the Internet and are designed to block unauthorized access.

Firewalls can be used to prevent cyber-attacks and to restrict access to sensitive information.

Antivirus software:

Antivirus software is designed to detect and prevent malware from infecting an organization's computers and network.

Antivirus software should be updated regularly to ensure that it is effective against the latest threats.

Encryption:

Encryption is the process of converting plain text into ciphertext, making it unreadable to unauthorized individuals.

Encryption should be used to protect sensitive information, such as financial information, personal data, and login credentials.

Access controls:

Access controls are security measures that are used to control who has access to sensitive information and resources.

Access controls should be based on the principle of least privilege, meaning that individuals should only have access to the information and resources that they need to perform their job duties.

Access controls can include user authentication, password policies, and multi-factor authentication.

Developing a Cybersecurity Plan

Data backup and disaster recovery:

Data backup and disaster recovery are critical components of an organization's cybersecurity plan.

Data backup ensures that the organization's data can be restored in the event of a disaster, while disaster recovery outlines the steps that the organization will take to restore normal operations in the event of a security breach.

Network segmentation:

Network segmentation is the process of dividing a network into smaller segments, or subnets, to help limit the spread of malware and to restrict access to sensitive information.

Network segmentation can help prevent unauthorized access to sensitive information and reduce the impact of a security breach.

Regular software updates:

Regular software updates help to ensure that the organization's software is up to date and protected against the latest security threats.

This includes updating operating systems, applications, and firmware.

By implementing these technical controls, non-profits and associations can significantly improve their security posture and reduce the risk of a successful cyber-attack.

However, it is important to remember that cybersecurity is an ongoing process and that security measures must be regularly reviewed and updated to ensure that they are effective against the latest threats.

In conclusion, developing a comprehensive cybersecurity plan is essential for non-profits and associations to protect their data and IP against cyber-attacks.

The plan should include a security audit, a cybersecurity policy, and the implementation of technical controls, such as firewalls, antivirus software, and encryption.

By following these steps, non-profits and associations can significantly improve their security posture and reduce the risk of a successful cyber-attack.

Data backup ensures that the organization's data can be restored in the event of a disaster, while disaster recovery outlines the steps that the organization will take to restore normal operations in the event of a security breach.

Employee Awareness and Training

Employees play a critical role in protecting an organization from cyber-attacks.

Employees play a critical role in protecting an organization from cyber-attacks. It is important for non-profits and associations to educate their employees about the latest cyber threats and to empower them to take proactive measures to protect the organization's data and IP.

Creating a Culture of Cybersecurity

To create a culture of cybersecurity within the organization, non-profits and associations must educate their employees about the importance of cybersecurity and how they can contribute to the organization's security posture.

This can be done through regular training sessions, posters, and regular communication from senior management.

It is important to emphasize that cybersecurity is everyone's responsibility and that employees should report any suspicious activity to the appropriate personnel.

Best Practices for Employee Training

Regular training:

Regular training is essential to keep employees up to date on the latest cyber threats and best practices for protecting the organization's data and IP.

This can include online courses, in-person training sessions, or a combination of both.

Phishing simulation:

Phishing simulation is a great way to educate employees about the dangers of phishing and to train them to recognize and respond to phishing attacks.

This can be done by sending simulated phishing emails to employees and monitoring their responses.

Employee Awareness and Training

Password management:

Employees should be trained on best practices for password management, including the use of strong passwords and the importance of regularly changing passwords.

Mobile device security:

With the increasing use of mobile devices for work, it is important to educate employees on how to protect their devices and the data stored on them.

This can include using a password or pin, enabling remote wipe, and using encryption.

Social media and internet use:

Employees should be trained on how to use social media and the internet safely, including avoiding suspicious links and avoiding sharing sensitive information online.

By providing regular training and creating a culture of cybersecurity within the organization, non-profits and associations can empower their employees to take proactive measures to protect the organization's data and IP.

Employee awareness and training are critical components of a comprehensive cybersecurity plan for non-profits and associations.

By educating employees about the latest cyber threats and best practices for protecting the organization's data and IP, non-profits and associations can reduce the risk of a successful cyber-attack and create a culture of cybersecurity within the organization.

Employee awareness and training are critical components of a comprehensive cybersecurity plan for non-profits and associations.

Incident Response and Recovery

Cyberattacks can have devastating consequences for non-profits and associations. It is therefore essential that organizations have a plan in place to respond to an attack, mitigate its impact, and recover from it.

In this chapter, we will discuss the steps for preparing for a cyber-attack, responding to it, and recovering from it.

Steps for Preparing for a Cyber-attack:

Develop an incident response plan: A comprehensive incident response plan outlines the steps to be taken in the event of a cyber-attack.

It should include the roles and responsibilities of each member of the organization, the steps to be taken to contain the attack, and the process for reporting the attack to the relevant authorities.

Test the plan regularly:

Regular testing of the incident response plan is critical to ensure that it is effective and that all members of the organization understand their roles and responsibilities.

Assign a designated incident response team:

A designated incident response team should be assigned to respond to cyberattacks.

This team should be trained in the incident response plan and have the necessary technical skills to contain and mitigate the attack.

Cyberattacks can have devastating consequences for non-profits and associations. It is therefore essential that organizations have a plan in place to respond to an attack, mitigate its impact, and recover from it.

Incident Response and Recovery

Responding to a Cyber-attack:

Contain the attack:

The first step in responding to a cyber-attack is to contain it.

This involves disconnecting the affected systems from the network and isolating them to prevent the attack from spreading.

Investigate the attack:

The incident response team should work with a forensic specialist to investigate the attack and determine the extent of the damage.

This information is critical in determining the next steps to be taken to recover from the attack.

Report the attack:

The attack should be reported to the relevant authorities, such as law enforcement and regulatory bodies, as soon as possible.

Notify affected individuals:

If sensitive information, such as personal data, has been compromised, the affected individuals should be notified as soon as possible.

Recovering from a Cyber-attack:

Develop a disaster recovery plan:

A disaster recovery plan outlines the steps to be taken to recover from a cyber-attack.

This plan should include the processes for restoring data, rebuilding systems, and ensuring that the organization can continue to operate.

Rebuild systems:

The incident response team should work with IT to rebuild the affected systems and restore data.

Review and improve:

After the attack has been contained and recovery has been completed, the organization should review the incident and identify areas for improvement.

> ***Preparing for a cyber-attack is critical for non-profits and associations.***

This information should be used to update the incident response plan and improve the organization's overall security posture.

Preparing for a cyber-attack is critical for non-profits and associations.

A comprehensive incident response plan, regular testing, and employee training are essential in ensuring that the organization is prepared to respond to an attack and recover from it.

By taking these steps, non-profits and associations can protect themselves from the devastating consequences of a successful cyber-attack.

Conclusion:

Throughout this book, we have discussed the importance of cybersecurity for non-profits and associations and provided an overview of the threat landscape, as well as steps for developing a cybersecurity plan and protecting against cyber threats through employee awareness and training, and incident response and recovery.

It is important for non-profits and associations to take action and implement the steps discussed in this book to secure their data and IP against cyber-attacks.

A proactive approach to cybersecurity can help organizations minimize the risk of a successful cyber-attack and protect sensitive information.

We encourage all non-profits and associations to conduct a cybersecurity audit to assess their current security posture.

> ***Cybersecurity is a critical issue for non-profits and associations, and it is essential that organizations take steps to secure their data and IP against cyber-attacks.***

An audit can help identify any vulnerabilities and weaknesses in the organization's cybersecurity defences and provide a roadmap for improving security.

In addition, we invite all non-profits and associations to attend a 60-minute webinar on cybersecurity.

During the webinar, we will provide practical tips and best practices for securing data and IP against cyber-attacks, as well as a Q&A session where attendees can ask questions and get advice on their specific security concerns.

Cybersecurity is an essential issue for non-profits and associations, and it is crucial to take action to protect against cyber-attacks.

By conducting a cybersecurity audit and/or attending a 60-minute webinar, organizations can secure their data and IP and minimize the risk of a successful cyber-attack.

Don't wait, act today and secure your organization's future!