Five Actions To Prevent Cyberattacks

1. **Incident Response Plan**

2. **Prepare an Acceptable Usage Policy for Your Digital Assets**

3. **Review Your Hygiene Factors**

4. **Ensure Backups for All Your Sensitive Data**
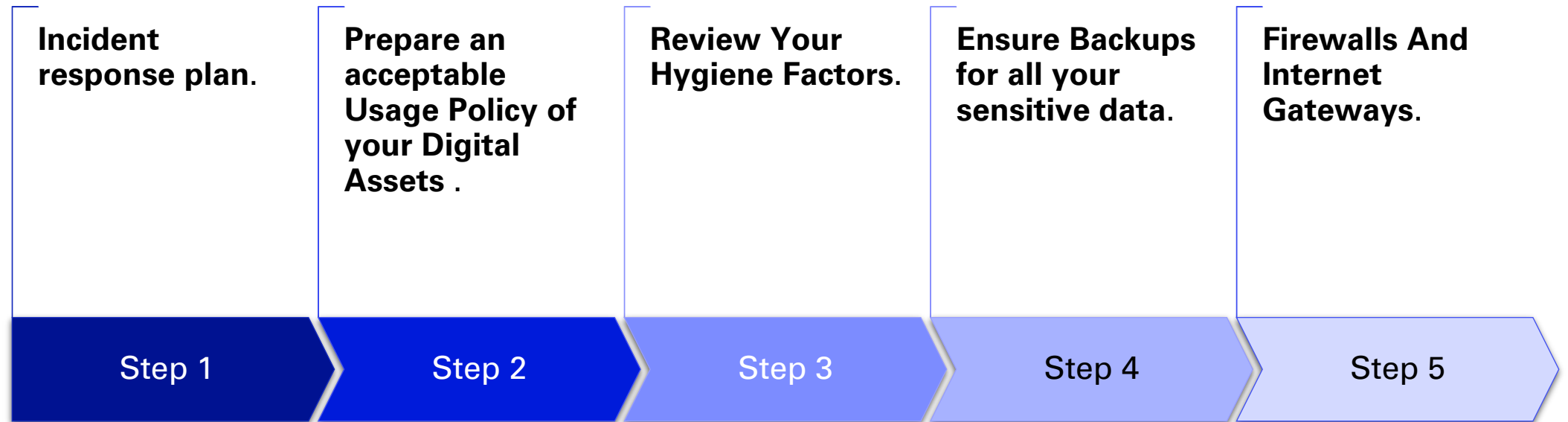
5. **Firewalls & Internet Gateways**

Five Actions to Prevent Cyberattacks

Nonprofit organizations utilize donations, volunteers, and government grants to fulfil their mission. With a tight budget and little funding for cybersecurity, nonprofit organizations cannot implement the latest defensive technology for their future attacks. According to Charity Digital, 98% of charities surveyed recognize cyber security is of paramount importance. Nonprofit organizations have almost no cybersecurity measures to protect their donor's and members' data due to limited budgets. More than 80% of nonprofits don't have a cybersecurity strategy.

Steps To Prevent Cyberattacks

Cybersecurity is essential for nonprofits, and outdated technology and processes impede productivity. The number of cyberattacks against nonprofit organizations has increased dramatically since 2020. Worst of all, most nonprofits have no plans or strategy in place for a cyberattack; therefore, we have listed below the top 5 actions NPOs can take to save their organizations from cyberattacks.

5 Actions

Incident response plan.

Prepare an acceptable Usage Policy of your Digital Assets .

Review Your Hygiene Factors.

Ensure Backups for all your sensitive data.

Firewalls And Internet Gateways.

Step 1

Step 2

Step 3

Step 4

Step 5

Nonprofit.fourdtech.com

Incident response plan

Nonprofits may lead to chaos under a cyberattack without a formal protocol or incident response plan. A robust security policy can enable nonprofit organizations to secure their data, and these response security policies can make it difficult for attackers to infiltrate the organization's resources and cause any damage. According to NTEN, 68% of nonprofits don't have documented policies and procedures in case of a cyberattack. Incident response plans help nonprofits minimize cyber damage and craft plans to respond to cyber incidents.

The incident response plan must include:

- Plan and roles of team members during cyberattacks

- Follow communication protocols for a smooth and efficient workplace.

- Working through containment and mitigation strategies in the event of an incident.

- Include any external assistance required during an attack

Nonprofit.fourdtech.com

Prepare an acceptable Usage Policy of your Digital Assets

It's imperative to outline the acceptable usage of the Internet, intranet including but not limited to computer equipment, application software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, Access to Social Media Platforms. These rules are framed to protect the employees working in Nonprofits to use the Digital Assets for proper and legal use of resources. Inappropriate use of resources exposes the Nonprofits to virus attacks, security threats/vulnerabilities and legal issues.

Review Your Hygiene Factors

Cybersecurity hygiene means practices conducive to maintaining an organization's systems health. It is the way of developing and implementing a set of tools, policies, and practices to maintain cyberhealth. Following these hygiene factors will keep any sensitive data organized and secure from theft or attacks.

Research has shown that more than 50% of cyber-attacks happen due to employees' negligence or intent. Creating a routine around cyber hygiene helps NPOs enable practices that continually help prevent cybercriminals from causing security breaches or stealing personal information. A comprehensive cybersecurity strategy must include:

- Use a strong password and change them often.
- Use multi-factor authentication to build an additional layer of security.
- Regular update of hardware and software.
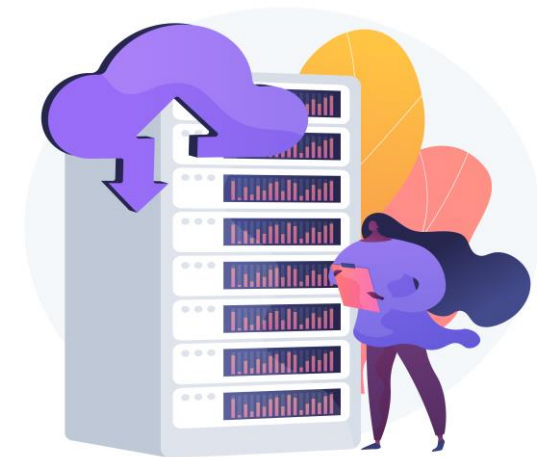
Ensure Backups for all your sensitive data

A data back is a copy or archive of the organization's critical information stored on the devices. It is essential to create multiple copies of the essential data so that NPOs can restore it quickly in the event of data loss or cyberattack.

The data nonprofits collect on donors, corporate contributors, partners, vendors, and charities are critical to their operations. Loss of essential data would disrupt operations, create compliance risks, and cause a significant breach of trust among donors. More than 80% of nonprofits don't even have a strategy to deal with cyberattacks. Below are the actions NPOs can take:

- Using removable media can enable NPOs to store files in smaller quantities

- Using External hard drives for ample storage of data

- Using Cloud backup for flexible storage

- Using other backup services such as tablets, computers, laptops.

Nonprofit.fourdtech.com
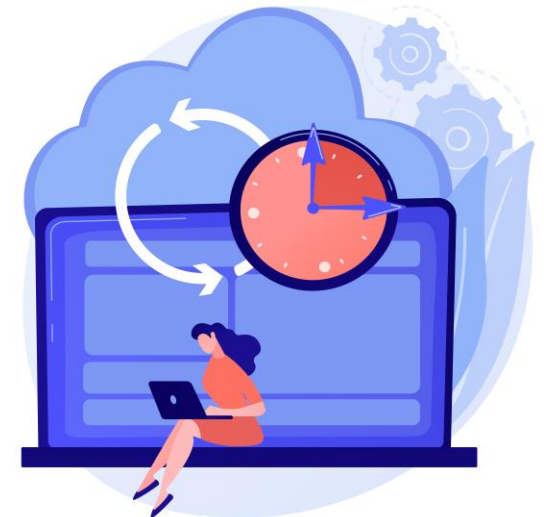
Firewalls And Internet Gateways

Firewalls and internet gateways are the first line of defense for keeping the donors and members safe. It blocks unauthorized users from gaining access to the organization's data, checks and monitors the data through the network, and blocks unwanted data according to pre-defined firewall rules. Nonprofit organizations aren't aware of these IT facilities. They can make the firewalls more secure by only allowing traffic from trusted web addresses listed in a safe list. The amount of spam nonprofits receive has increased by 170%, and spear-phishing attacks by 321% in 2021. Securing the organization's data has become challenging for nonprofit organizations.

Below are a few actions NPOs can take:

- Change of default administrative password to an alternative

- Prevent access to any administrative interface from the Internet unless needed

- Block unauthenticated inbound connections

- Ensure inbound firewall rules are approved and documented by an authorized individual

- Remove or disable permissive firewall rules as soon as they are not needed

Nonprofit.fourdtech.com

Conclusion

Nonprofit organizations have considerable responsibilities to support their mission and community. Your mission is what drives your organization forward. At the same time, taking care of donors' and members' data is of paramount importance. Also, security updates are essential. In conclusion, this guide will help NPOs understand some basic steps to take when planning to prevent cyberattacks.

Fourth Dimension Technologies empowers communities and nonprofits to use technology to serve the world better. We create custom IT solutions tailored to your organization's needs using our "**Proprietary transformation model**." Being a leading provider of technology and solutions for nonprofits and their communities, we design budget-friendly technology services that maximize your nonprofit's return on investment, so you can better serve the community.

Nonprofit.fourdtech.com