Nonprofit Guide to Cybersecurity

Version 1.0

The Nonprofit Executive's Guide to Cyber Risk Management and the NIST Cybersecurity Framework

This guide was designed to help executive directors, board members, and senior staff manage cyber risk within nonprofit organizations. The introduction helps nonprofit leaders understand the risk landscape and their role in managing cyber risk, part one explains how to lead the organization toward an improved cybersecurity posture, and part two introduces The National Institute of Standards and Technology's Cybersecurity Framework[1], which is a widely used, free methodology for managing cybersecurity.

threat SKETCH®

Part of the *Cyber Risk Management Toolkit for Nonprofits*

https://threatsketch.com/cyber-risk-management-tools-nonprofits/

Funding and support provided by the U. S. Department of Homeland Security, National Protection and Programs Directorate, Office of Infrastructure Protection, through the National Infrastructure Protection Program Security & Resilience Challenge which is implemented by The National Institute For Hometown Security (NIHS).

Disclaimer: This guide is for informational purposes only and does not contain or convey legal, financial, or insurance advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer, financial adviser, insurance adviser, or other professional adviser.

[1] The official title is *Framework for Improving Critical Infrastructure Cybersecurity*, but it is commonly referred to as the NIST Cybersecurity Framework.

Why Care About Cybersecurity?

When you are fueled by passion, good intention, and a desire to improve the community, it is often hard to believe that anyone would want to harm your organization or disrupt your mission. Unfortunately, there are plenty of bad actors in the world who are indifferent to your good intentions. There are hacktivists (activist hackers) who may oppose your mission. There are thrill-seekers who hack for sport. There are nation-state espionage campaigns whose goal is to spread disinformation and use nonprofits as a conduit to other targets. And there are the insiders (staff or volunteers) who can make innocent mistakes or maliciously abuse their privilege. All of these people have different motivations, but the end result is the same — cyber attacks that put your organization and its stakeholders at risk.

The motives driving cybersecurity attacks include:

MONEY – Nonprofits are ripe targets for extortion, scams, and digital theft.

DATA – Information about board members, staff, volunteers, donors, and beneficiaries.

ACCESS – Impersonating you, or using your login credentials, gives hackers a platform from which to attack bank accounts, funding sources, partners, service providers, and other stakeholders.

REPUTATION – Nonprofits are extremely sensitive to reputational damage across many stakeholders. A damaged reputation can undermine funding, volunteers, staff, beneficiaries and community support.

You might think your organization's budget is too small for anyone to bother targeting you for money. However, automated phishing and extortion (ransom) attacks do not care about a large amount of money per attack. They simply rely on mass attacks to yield lots of little "successes," and the best targets are small organizations that haven't addressed the basics of cybersecurity.

You might also think that no one cares about your organization's data, but personal and operational information has plenty of black market value. Hackers can get a few dollars for each volunteer's information, which is incentive enough. Then the organization is left holding the bag for legal and regulatory penalties that can sink the organization. The reputational damage alone can be catastrophic.[2]

A nonprofit organization's reputation is a double-edged sword. One edge serves hackers, the other serves hacktivists. Hackers seek to exploit your good reputation by taking over your digital presence (email, website, social media) so that victims will let down their guard. By compromising board members, staff, and volunteers, hackers can easily infiltrate other organizations. On the other side are hacktivists that want to destroy your reputation. Defacing websites is one thing, but imagine the harm done from exposure of confidential information like the personal information of employees, donors, or people receiving services from your organization.

Who wants to steal from nonprofits?

HACKERS that have automated phishing and extortion attacks and do not care if nonprofits are part of the harvest.

CRIMINALS, in the aftermath of a crisis, want to divert donations by compromising your website or by creating a look-alike presence.

HACKTIVISTS, driven by political or ideological beliefs, will target nonprofits to destroy its reputation in the name of their own cause.

BAD ACTORS want to gain access to your funding partners, board members, and community partners. They do that by taking over your email and social media accounts, or to steal login information to someone else's system.

Your Role

This guide is written for nonprofit leaders who are charged with overseeing the mission success of the organization. Throughout this guide we use the term leadership to include board members and executive directors who may or may not be paid staff. In larger, more complex organizations, leadership might include senior staff, program managers, and other senior executives. The leadership team may not have technical skills, but that does not absolve them of the **fiduciary duty** to address the threat that cybersecurity presents to the organization and the mission they are charged with governing.

It is tempting to believe that cybersecurity is just an Information Technology (IT) problem, or that moving everything to "the cloud" means everyone is free to focus on more important matters. But the digital economy has changed the landscape. Today, a few errant clicks can lead to legal, regulatory, and reputational nightmares. A host of new threats to your organization's mission now exist, and leaders have a moral and legal obligation to the organization and its stakeholders to manage the emerging cyber risk. Cloud solutions can improve operational security, but the liability when someone gains access to the data and the reputational damage that follows can be catastrophic. Outsourcing to cloud-based solutions can be helpful, but it is not a cure all. You may have trusted your organization's information to a cloud-based host, but reading through the privacy policies and terms and conditions
is often an eye-opener. In fact, when it comes to cybersecurity, there is no magic bullet.

[2] Arnold, Rob (2017). *Cybersecurity: A Business Solution.* P. 5 ISBN 978-0692944158. https://threatsketch.com/book

Background

In the commercial sector, the main goal of an organization is *profit*[3], which is easy to measure in monetary terms. For nonprofits the goal is *mission continuity*, which is the flow of resources from donors, volunteers, staff, board members, and the community to produce a consistent supply of service to the nonprofit's beneficiaries. Through one or more programs, each representing a unique combination of these resources, a nonprofit organization fulfills its mission. Together the resources and beneficiaries make up the organization's *stakeholders*.

Nonprofit Stakeholders

Funding Resources including donations, grants, contracts, fundraisers, etc.

Volunteers and Staff representing the human effort.

Board Members providing oversight, fiscal transparency, and key relationships.

Community Resources such as reputation, IRS nonprofit status, loaned space for operations, etc.

Beneficiaries, who may be members, clients, citizens, etc.

Some stakeholders are more sensitive than others to disruptions to the mission and programs. Down time, diverted dollars, reduced service hours, unmet payroll, and unserved beneficiaries are some examples of how disruption and its impact might be measured. If the organization has multiple programs, these measures and the sensitivity to disruption may vary from one program to the next. Across organizations, strategic differences such as variations in funding models can influence which measures of impact matter the most.

Maintaining mission continuity includes managing cybersecurity issues that can disrupt programs and impact stakeholders. Throughout an organization, cyber risk is more than just IT solutions like firewalls and antivirus software. It also includes managing:

- Legal and regulatory exposure
- Financial resilience
- Public relations
- Vendor/supplier relationships
- Confidentiality
- Internal culture and training
- A balance between prevention and preparedness

Part One of this guide gives nonprofit leaders an overview of their role in managing cyber risk. Part Two introduces the National Institute of Standards and Technology (NIST) Cybersecurity Framework[4]. The NIST Cybersecurity Framework is the federal government's standard for addressing cybersecurity. In 2017, all federal agencies were directed to align with this de facto standard. This is relevant to nonprofits because any organization that interfaces contractually with a federal agency is part of that agency's supply chain, and therefore may become subject to the NIST Cybersecurity Framework. As a result, federal grants will eventually reference these requirements. Adopting the NIST Cybersecurity Framework is the most universal solution to demonstrate a commitment to good cybersecurity stewardship. Having a solid understanding of the terminology and the concepts will improve communication with donors, staff, volunteers, vendors, and other partner organizations when aligning with the NIST Cybersecurity Framework.

The full guide is available as part of the Threat Sketch Cyber Risk Management Toolkit for Nonprofits that helps board members, directors, and senior staff plan for, communicate, and manage the big picture of cybersecurity. You can request a free copy of the guide and learn more about the toolkit by visiting https://threatsketch.com/

GET THE TOOLKIT

https://threatsketch.com/cyber-risk-management-tools-nonprofits/

[3] Cyber Resilience White Paper: An Information Technology Sector Perspective. March 2017. http://www.it-scc.org/uploads/4/7/2/3/47232717/it_sector_cyber_resilience_white_paper.pdf

[4] NIST Cybersecurity Framework. https://www.nist.gov/framework