501Secure.org

Cybersecurity Assistance for Nonprofits

Ten Questions to Ask About Your Nonprofit's Cybersecurity

August 2025

501Secure is a Mabel G. Ragland Institute program.

Connect with the program at info@501secure.org.

Contact:
Kai Dailey, Executive Director
Mabel G. Ragland Institute
kai@501secure.org

10 Questions to Ask About Your Nonprofit's Cybersecurity

Introduction

Everyday cybercriminals target nonprofits and succeed in compromising email and cloud accounts, launching ransomware, and receiving payment on fraudulent invoices and bank transfers. The impact of an incident at one organization can rapidly expand outward, compromising other nonprofits and government partners. Often, one organization is targeted to gain access to another. Every nonprofit, no matter its size, has a responsibility to protect not only itself but also the community it works with.

If you've recognized the urgent need to secure your organization, you're not alone. The challenges of cybersecurity can feel overwhelming, from gaining buy-in from leadership to motivating staff to adopt new practices. National and local organizations are stepping up to provide support, but navigating the landscape of available resources, training, and services can be difficult.

Ultimately, the responsibility for putting effective security measures in place rests with each nonprofit team. While a third-party consultant can help validate your concerns and explain the risks, true motivation for change must come from leadership. Nonprofit leaders must educate themselves, set clear goals, hold people accountable, and consistently show that cybersecurity is a top priority.

The Path Forward: More Than Just Technology
Effective cybersecurity is about more than just technical controls like passkeys and conditional access to accounts and data. It requires a fundamental shift in mindset. You need to gain a green light from leadership and inspire (and require) every staff member to participate.

Bringing up cybersecurity can be tough. Your colleagues might see it as an extra burden, and leadership may view it as an unnecessary expense. You might feel like you're nagging people, but don't give up. Protecting your organization demands persistence, constant learning, and a commitment to teaching others. Every organization needs a champion to lead these efforts.

If that person is you, this handout contains ten questions designed to help you think critically about your nonprofit's cybersecurity. Use them to identify risks, start a conversation, and begin the process of building a plan to create a more resilient organization and a culture of security awareness.

Table of Contents

Ten Questions

1. **What are our most valuable assets? (And who has access to them?)**

   This question gets to the heart of what your organization needs to protect, shifting the conversation from a general "security" issue to a specific "mission protection" issue. Go beyond just identifying IT systems and hardware. Consider what data, applications, or processes are absolutely essential for getting the most important work done. Is it donor data, client records, program management systems, or your website?

   Informally rank assets based on their value to the organization and the potential impact of their loss. This will help identify areas of concern.

2. **How do we currently handle sensitive data? (What systems, devices, and platforms does it live on?)**

   This helps identify the scope of your data protection needs without a technical inventory. Initially, start with a conversation, rather than a database.

   - What data do you store? The more sensitive the data, the greater the target.
   - How do you accept payments? Online transactions require extra security measures.
   - What devices do your employees use? Organization-owned? Personal? Mobile devices? Each has its own set of risks.
   - Do you use cloud services? (MS 365, Google Workspace, Dropbox, Salesforce, etc.) Cloud security is essential if you store data or use applications in the cloud or have a remote working environment.

3. **What policies do we have in place to protect data? (And are they understood and followed by everyone?)**

   This addresses the human element and potential for policy gaps.

   - Are the data protection regulations that apply to your organization, such as GDPR, HIPAA, PCI, or state-specific laws Identified, researched, and understood?
   - Are policies and procedures in place to ensure compliance with relevant regulations?
   - Do you monitor regularly for changes in regulations and update your compliance efforts accordingly?

- Do you conduct regular data audits and report incidents promptly? If a breach occurs, do you have a procedure in place to report it to affected individuals and relevant authorities as required by law?

4. **How do we handle new staff, departing staff, and changes in roles?**

   This focuses on a major attack method that's often overlooked. Flaws in how user access is managed create easy entry points for attackers.

   - Do staff members or volunteers have too much access to accounts, admin permissions, and data? When users have more permissions than their job requires, it creates greater attack opportunities to gain immediate access to a wider range of sensitive resources.
   - Do you adjust access when a staff member changes roles within the organization? Without a formal process, it is common that an employee's permissions may accumulate over time as they change roles or take on new responsibilities, without their old permissions being revoked. Attackers can exploit this to access old data or systems the staff member no longer needs.
   - Lingering access after employee separation? When a staff member leaves an organization, a failure to promptly and completely revoke their access can allow a former employee or an attacker to use their account to gain unauthorized access to a network or cloud accounts.

5. **What would we do if a key employee's email was compromised (or if we lose email access altogether)?**
   This is a simple question that can reveal major gaps in incident response planning.

   Do we have an incident response plan and was it tested in the last 12 Months? Who will we call in an emergency for IT assistance?

6. **Who is responsible for security? (Is it just IT, or is it everyone?)**

   This question prompts a discussion about shared responsibility and the need for a security culture. It is reasonable to expect that anyone with access to your systems and data should be responsible stewards of your organization's information assets. But is this made explicit through policy, training, and frequent reinforcement? If you are using cloud services, what responsibilities for data protection belong to your organization and which ones belong to the cloud vendor?

7. **What's our biggest fear? (Losing a funder? A data breach? Being locked out of our systems?)**

   This gets to the emotional core of why security matters. While our biggest fears are not necessarily our biggest cyber risks, taking the time to discuss worst case scenarios is an important first step in preparing for the worst. It also frames planning efforts to put security measures in place to reduce the risk of a potentially organization-ending incident.

8. **What's our plan for backing up critical data?**

   This addresses a fundamental step in resilience. If you lose access to your primary client database, do you have a back up? Have you tested it? What steps are involved to access it? How long would it take to restore your database or locate the data? How current is the data in the backup?

9. **Do we have baseline security controls like MFA and email security in place?**

   What blocks are there to implementing multi-factor authentication or adding additional email security? Multi-factor authentication (MFA) on all accounts, especially for those with access to sensitive data or systems dramatically reduces your risk of data loss and unauthorized account access. Don't make exceptions!

   Adding email filtering effectively blocks a greater percentage of phishing attempts, spam, and malware.

10. **How can we make security an easy, regular part of our work?**

    This question shifts the focus from “burden” to “best practice” and sets the stage for a sustainable program. For example, adding cybersecurity/data security to the regular meeting agenda keeps safety top of mind and signals to staff its importance. If you currently have no training in place, begin by training staff to recognize and report suspicious emails.

Additional Resources

Nonprofit
501Secure [Website]

Fair Institute Cybersecurity Risk Measurement Framework [Website]

NTEN Cybersecurity HUB [Website]

NTEN Cybersecurity Readiness 3-Month Cohort Program [Website]

Cybersecurity strategies for nonprofit websites [Blog]

Government

CISA Cyber Hygiene Vulnerability Scanning – A free service by the federal agency responsible for national internet security to identify vulnerabilities in your internet-facing systems. [Service]

Cyber Guidance for Small Business [Services and Info]

Government Alerts and CISA Alerts and Advisories [Newsletters]

CISA Assistance for Small and Medium Sized Businesses [Services and Info]

Commercial

Treat Cybersecurity as a Business Investment for Better Outcomes by Paul Proctor [Webinar]

Complimentary Business and IT Webinars by Gartner [Webinar Library]

Tech Target Security [Article Library]