Safeguarding Nonprofit Data and Employees from Cybersecurity Threats

EXIGENT

Top Cybersecurity Concerns for Nonprofits

1

Data Breaches

Much like many businesses, nonprofits handle sensitive information, including donor details, financial records, and personal information about beneficiaries. Data breaches can lead to severe consequences, including loss of trust and legal repercussions.

2

Phishing Attacks

Cybercriminals target nonprofits with phishing emails to install malware that can often go undetected for months, siphoning off sensitive data the entire time. These attacks exploit the limited cybersecurity awareness among staff and, more often, volunteers.

3

Ransomware

Ransomware attacks, where data is encrypted and held for ransom, can cripple a nonprofit's operations, especially if the organization lacks robust backup and recovery systems.

4

Third-Party Vendor Risks

Nonprofits frequently rely on third-party vendors for payment processing, email marketing, and data storage. These vendors can be a weak link in the cybersecurity chain if they do not have strong security measures.

5

Insider Threats

Human error is the leading cause of data breaches, a challenge that is exacerbated by nonprofits' reliance on volunteers. Nonprofits often struggle with implementing strict access controls and monitoring due to the mix of employees and volunteers needed to operate.

6

Lack of Cybersecurity Policies and Training

Many nonprofits do not have formal cybersecurity policies or regular training programs for their staff and volunteers, making them more vulnerable to cyber threats.

EXIGENT

Safeguarding Nonprofit Data and Employees from Cybersecurity Threats

68%

One of the most immediate and tangible consequences of a cyberattack on nonprofits is the disruption of day-to-day operations. **CyberPeace Institute** research shows that 68% of nonprofits have experienced a data breach in the past three years, making it clear that nonprofits must start to take cybersecurity seriously and invest in the necessary protection to safeguard data. Cybercrime can result in damage and destruction of data, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, and more.

Safeguarding Nonprofit Data and Employees from Cybersecurity Threats

Nonprofits sit in a precarious position when it comes to cybersecurity. Much like law firms and other organizations that store detailed and often confidential information about clients, many nonprofits manage payment portals, keep detailed financial records, and store and transfer data about donors, employees, beneficiaries, and other organizations. However, unlike businesses, nonprofits often operate on limited budgets, have no in-house technology staff, use aging technology, and have a high dependency on volunteers, making policy adherence and enforcement a challenge. What that means is while these entities are prime targets for cybercriminals, they are rarely equipped to protect data from sophisticated hacks or respond quickly to a threat.

While nonprofits may not generate revenue the same way businesses do, they still face financial impact from cyber attacks. Potential losses include direct costs such as paying a ransom or investigating the breach, restoring systems and data, and legal fees or regulatory fines. **The Nonprofit Technology Network (NTEN)** warns nonprofits that donors may be less willing to trust them after a data breach – even though cyber attacks are an increasingly common occurrence with businesses. Because a consumer's relationship with a company is based on the consumer's need, and a donor's relationship with a nonprofit is not need-based, nonprofits may be at greater risk than businesses to suffer reputational and financial damage from a cyber attack.

EXIGENT

Safeguarding Nonprofit Data and Employees from Cybersecurity Threats

Additionally, according to the **Council of Nonprofits**, because many nonprofits collect and store sensitive personal data protected by law as confidential, a breach poses a risk not only for the individuals whose data was disclosed but also for the nonprofit that is potentially liable for the breach. The council's advice: Every nonprofit must, at a minimum, assess its risk of a data security breach and protect its data from unauthorized disclosure.

Nonprofits sit in a precarious position when it comes to cybersecurity

According to Microsoft's 2021 Digital Defense Report, nonprofit organizations are the second most targeted sector by cybercriminals. Adding to that risk, CyberPeace Institute research shows most nonprofit organizations do not have a budget allocated for cybersecurity, and 70% of them do not have the knowledge or skills to respond to a cyberattack. Under those circumstances, how does your nonprofit start to improve? Create and then work through a roadmap to put cybersecurity best practices in place. Here are some key steps for improving your cybersecurity posture:

Audit Your Data

NTEN suggests a nonprofit should start working toward a more secure environment by taking inventory of all the data it collects and recording where it is stored. Understanding what data you have, where it lives, and how it is used helps you plan for its protection, but also serves as a basis for creating a reliable backup and recovery plan. As a starting point, NTEN recommends asking:

- What compliance standards apply to the data we collect and store, and what are they?
- What data does the organization collect from and about people?
- What does the organization do with it?
- Where does the organization store it?
- Who in our organization has access to this data and is responsible for it?
- What is our organization's document retention policy?

You may be surprised by the compliance rules that come into play when it comes to both cybersecurity and business continuity, including General Data Protection Regulations (GDPR) and the **Federal Trade Commission's Disposal Rule**, payment and credit card rules (PCI), healthcare standards (HIPAA), and even state regulations on data protection and breach notifications.

EXIGENT

Safeguarding Nonprofit Data and Employees from Cybersecurity Threats

Complete a Comprehensive Risk Assessment

While it may seem like an expensive endeavor, undergoing a thorough, professional third-party cybersecurity risk assessment is essential to protecting your nonprofit organization. A local, reputable managed services provider (MSP) such as **Exigent**, may offer simple, free or reduced-cost assessments for nonprofits and educational institutions, so ask colleagues for introductions to a trusted MSP to complete this step.

Risk assessments will evaluate your entire environment—from meeting with departmental leaders to conducting penetration and vulnerability testing to evaluating organizational policies and procedures and identifying obsolete technology—and provide a detailed report that includes recommendations for resolving issues. While many nonprofits may not be able to tackle all of those suggestions at once, this assessment can inform and guide a roadmap for improvement that eliminates significant risks first and then builds toward a more robust cybersecurity posture over time.

Build a Business Continuity Strategy

With a firm grasp on a plan for tightening cybersecurity controls, nonprofits should begin to create a strategy for business continuity as well. This plan is a detailed overview that guides your organization through any disruption, such as a natural disaster or data breach. It will cover everything from incident reporting to employee responsibilities, and crisis communication to the essential step of recovering systems and data.

Remember to Secure Your Nonprofit Website

Much like other organizations, nonprofits depend on websites for events and announcements, to share programming information, and to solicit and accept donations. Hackers love the opportunity to disrupt operations, so while your main website will likely remain intact in the background during a website attack, bad actors can create offensive content that damages your reputation. While this type of "attack" doesn't have the far-reaching impact of a data breach, remediating the damage can be time-consuming and expensive. Regular maintenance of your website, along with strong password policies and strict access control, can go a long way in avoiding this type of cyber headache.

Invest in Cyber Insurance

According to the **Nonprofit Risk Management Center,** cyber insurance that provides liability protection for your nonprofit can be well worth the money. They recommend that nonprofits work with a knowledgeable agency to fully explore the types of cyber insurance coverage available and what best fits your needs. As a starting point, nonprofits should understand that cyber insurance can help protect them from expenses such as notifications to impacted parties and regulatory and other legal fines, provide resources and guidance for crisis management, and offer business continuity and/or data loss and system damage coverage.

Need further assistance with cyber insurance? Many **state associations serving nonprofits** offer guidance and detailed resources for their members.

Watch our cyber insurance webinar on-demand, and get our insurance prep checklist as a bonus.

Want to learn more?

Download our business continuity planner

EXIGENT

Safeguarding Nonprofit Data and Employees from Cybersecurity Threats

Other tips:

- Create and adhere to a regular schedule for software updates and security patching, with exceptions for urgent updates from software or hardware vendors warning of potential risk
- Encrypt sensitive data both at rest and in transit, which means solutions for protecting your servers, backup solutions, and email security
- Schedule a cadence of ongoing employee security awareness training to ensure your team is educated and prepared to navigate threats that often slip through via email
- Develop and implement policies that include clear cybersecurity procedures, BYOD usage, acceptable use of nonprofit technology, access control standards, and incident response planning
- Prioritize investments in essential cybersecurity tools such as firewalls, antivirus software, and encryption.
- Implement strict access controls – both physical and digital – and regularly review user access to sensitive information
- Tackle business continuity planning to protect your nonprofit from disruption
- Carefully evaluate third-party vendors' security practices and include security requirements in contracts

How MSPs Can Support Your Nonprofit

While nonprofits are not unique in the impact a cyber attack can have on their operations, they do face challenges that many businesses do not, such as limited budgets, reliance on volunteers, lack of experienced IT staff, and the need for decisions to be vetted and approved by a board of directors, which can limit agility. To combat those issues, many nonprofits elect to partner with a managed services provider (MSP) such as Exigent, with a strong background in cybersecurity and a proven track record with nonprofit clients.

A reputable MSP can guide your organization toward simple, quick fixes that can improve your cybersecurity posture. They will then work with you to identify and deploy right-sized security and business continuity solutions while also creating a long-term roadmap that can be reviewed and plotted out with the board of directors over several years. That approach allows your organization to address unique concerns while also respecting your budgetary and planning limitations.

Read how Exigent partners with one nonprofit to plan its technology roadmap

EXIGENT