Safeguarding Your Mission

PROTECTING YOUR NONPROFIT FROM CYBER THREATS

PART 1 OF 3

filament
ESSENTIAL SERVICES
filamentservices.org

JUNE 2023

Introduction

In today's digital age, the nonprofit sector faces a myriad of cyber security challenges that threaten the integrity of their organizations and their missions. With an increasing reliance on technology for daily operations, data management, and fundraising efforts, nonprofits must prioritize data security to safeguard their stakeholders and maintain trust.

Risk Pretest

Before we get started, honestly answer the following questions about your organization and consider the risks:

Question	Risks
Does your organization have sufficient cyber security and awareness training for staff and volunteers?	Vulnerability to social engineering attacks and other threats.
Does your organization have dedicated IT personnel or do you rely on volunteers or generalists to manage your technology needs?	Gaps in the organization's cyber security defenses and vulnerability management.
Does your organization have difficulty keeping up with evolving cyber threats?	Exposure to new and emerging risks.
Does your organization mistakenly assume that they are not an attractive target for cybercriminals?	False sense of security that can lead to inadequate investment in cyber security measures.
Does your organization struggle to foster a strong cyber security culture?	Staff and volunteers unaware of the risks or not prioritizing cyber security in their daily activities.
Does your organization hold sensitive and valuable data related to their donors and beneficiaries including personal information, financial details, and contact information?	The high value of this data makes it an attractive target for cybercriminals, who may use it for identity theft, financial fraud, or other malicious purposes.

The Perils of Ignoring Data Security

Ignoring data security can have severe consequences for nonprofits, exposing them to various risks that can compromise their mission, undermine stakeholder trust, and result in financial and reputational damage.

Financial Losses

Data breaches can lead to significant financial losses for nonprofits:

- **Direct costs**: Expenses related to incident response, forensic investigations, legal fees, public relations efforts, and credit monitoring services for affected stakeholders.
- **Indirect costs**: Loss of donations and grants due to decreased donor trust, as well as potential fines and penalties for non-compliance with data protection regulations.

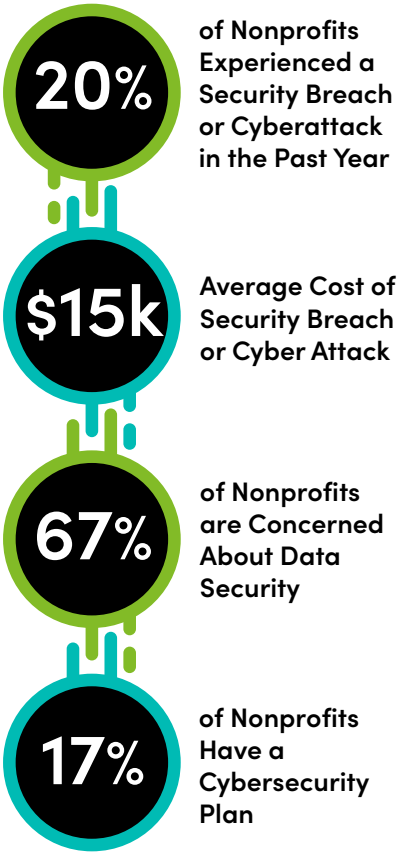
In 2020, the National Board of Medical Examiners (NBME) was targeted in a data breach that exposed the personally identifiable information (PII) and protected health information (PHI) of medical students and professionals. The breach resulted in a settlement of $275,000 with the New Jersey Division of Consumer Affairs, which was responsible for investigating the incident.

Reputation Damage

A data breach can severely damage a nonprofit's reputation, undermining public trust in the organization and its mission:

- **Negative media coverage**: Data breaches often attract media attention, which can lead to negative publicity and lasting reputational harm.
- **Stakeholder trust erosion**: Donors, beneficiaries, volunteers, and partners may lose trust in the organization's ability to protect their sensitive information, jeopardizing future support and collaboration.

In 2019, the American Medical Collection Agency suffered a data breach that exposed the personal and financial information of millions of patients from various medical testing laboratories. The breach caused significant reputational damage for both the AMCA and the affected laboratories, resulting in multiple lawsuits and the bankruptcy of the AMCA.



Loss of Stakeholder Trust

Stakeholders expect nonprofits to protect their sensitive data, such as personal information, financial records, and confidential documents:

- **Donor attrition**: Donors may be less likely to contribute funds or support an organization that has experienced a data breach, impacting the nonprofit's financial stability.
- **Volunteer and partner disengagement**: Volunteers and partners may be hesitant to work with an organization that cannot adequately protect their data, limiting the nonprofit's capacity to carry out its mission.

In 2021, the National Business Aviation Association (NBAA) suffered a data breach that resulted in the compromise of employee and member information, including email addresses and physical addresses. The breach led to a loss of stakeholder trust from members who were concerned about the security of their personal information.

Legal and Regulatory Penalties

Nonprofits are subject to various data protection regulations, and failure to comply can result in penalties and legal consequences:

- **Fines**: Nonprofits that fail to comply with regulations, such as GDPR or HIPAA, may face significant fines and penalties.
- **Legal actions**: Affected stakeholders may initiate lawsuits against the nonprofit, resulting in legal expenses and potential damages.

The National Board for Certification in Occupational Therapy (NBCOT) is another example of a nonprofit in the U.S. that suffered legal and regulatory penalties due to a data breach. In 2020, NBCOT agreed to pay $100,000 to the New York Attorney General's office to settle allegations that it failed to provide notice of a data breach affecting approximately 61,000 individuals in a timely manner, as required by New York's data breach notification law.

Operational Disruptions

Data breaches can disrupt a nonprofit's operations, diverting resources from mission-critical activities and hindering the organization's ability to achieve its goals:

- **Diverted resources**: Responding to a data breach requires time, effort, and financial resources, which can strain an organization's limited resources and impede its ability to carry out its mission.
- **Lost productivity**: Recovering from a data breach often involves downtime and lost productivity, as staff members must focus on addressing the security incident rather than their regular duties.

The Lupus Foundation of America (LFA) suffered a data breach in 2020 that resulted in the unauthorized access to employee email accounts, leading to operational disruptions. As a result of the breach, LFA reset email passwords, implemented additional security measures, and provided employees with cyber security training.

Increased Vulnerability to Future Attacks

Ignoring data security can leave a nonprofit more vulnerable to future cyberattacks, as attackers may perceive the organization as an easy target:

- **Repeat attacks**: Cybercriminals may target a nonprofit that has experienced a data breach in the past, believing that the organization's security measures remain inadequate.
- **Widespread targeting**: News of a successful attack against a nonprofit can encourage other cybercriminals to target similar organizations, putting the entire sector at increased risk.

The Partnership HealthPlan of California, a nonprofit organization that manages health care for counties in California, experienced a ransomware attack that led to the ransomware group stealing private data from roughly 850,000 members, including social security numbers.

Understanding the Cyber Threat Landscape

Phishing Attacks

Phishing attacks are a prevalent form of cybercrime that target nonprofits and other organizations by attempting to obtain sensitive information, such as login credentials, financial data, or personal details, through deceptive means. Typically, cybercriminals employ social engineering tactics to manipulate individuals into divulging sensitive information or performing actions that compromise the security of the organization.

Types of Phishing Attacks

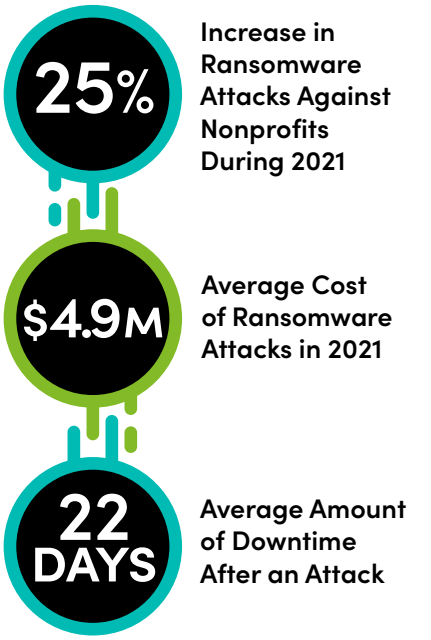
- **General phishing**: In this most common form of phishing, attackers send a large volume of generic emails to a broad audience, hoping that some recipients will fall for the scam. The emails often contain a sense of urgency and request the recipient click on a link or download an attachment.
- **Spear phishing**: Spear phishing is a targeted form of phishing attack where the cybercriminals research their intended victims, often focusing on specific individuals or organizations. By customizing the email content to appear more relevant and credible, attackers increase their chances of success.
- **Whaling**: This type of phishing attack targets high-level executives and decision-makers within an organization. Whaling emails are highly personalized and often appear to be from a trusted source, such as a business partner or a senior executive within the company.
- **Clone phishing**: Clone phishing involves replicating a legitimate email and altering the content slightly to include malicious links or attachments. Recipients may believe the email is a follow-up or an update to a previous message they received.
- **Smishing and vishing**: These forms of phishing use text messages (SMS) or voice calls instead of emails to trick victims into providing sensitive information or performing a harmful action.

Most Common Types of Attacks on Small Businesses & Nonprofits

Ponemon Institute

Ransomware

Ransomware is a type of malicious software that encrypts an organization's data, rendering it inaccessible until a ransom is paid to the attackers in exchange for a decryption key. Nonprofits are particularly vulnerable to ransomware attacks due to their limited resources, reliance on technology, and valuable data. A successful ransomware attack can have severe consequences for a nonprofit, including financial losses, operational disruptions, and reputational damage.



Cybersecurity Tech Accord | Accenture | Statista

How Ransomware Attacks Occur

- **Phishing emails**: Ransomware is often distributed through phishing emails containing malicious attachments or links, which, when opened or clicked, infect the recipient's computer and spread throughout the network.
- **Exploit kits**: Cybercriminals use exploit kits to take advantage of software vulnerabilities in web browsers, plugins, or operating systems, allowing them to deliver ransomware to a victim's device without any user interaction.
- **Remote desktop protocol (RDP) attacks**: Cybercriminals target organizations with weak or compromised RDP credentials, gaining access to their systems and deploying ransomware.
- **Malvertising**: This method involves injecting malicious code into legitimate online advertisements, which can redirect users to a site hosting ransomware or automatically download the ransomware payload onto their devices.

Malware

Malware, short for malicious software, refers to a range of software programs designed to infiltrate, damage, or otherwise compromise computer systems, networks, or devices without the owner's consent. Nonprofits, like any other organization, are at risk of malware attacks due to their reliance on technology for operations, fundraising, and communication. Understanding the various types of malware and implementing effective strategies to mitigate the associated risks is critical for safeguarding a nonprofit's digital assets and reputation.

IBM 2020

Types of Malware

- **Viruses**: Malicious programs that attach themselves to legitimate files and replicate, spreading from one device to another through file sharing, email attachments, or infected software downloads.
- **Worms**: Self-replicating malware that spreads rapidly across networks, often exploiting system vulnerabilities or using social engineering tactics, causing damage by consuming bandwidth and overloading servers.
- **Trojans**: Malware disguised as legitimate software, which, when downloaded and installed, provides a backdoor for cybercriminals to access the infected system, steal sensitive data, or install additional malware.
- **Adware**: Unwanted software that displays intrusive advertisements on a user's device, potentially redirecting them to malicious websites or tracking their online activity.
- **Spyware**: Covert software that monitors and collects information about a user's activities, such as keystrokes, browsing history, or login credentials, without their knowledge or consent.
- **Ransomware**: As previously discussed, ransomware is a type of malware that encrypts an organization's data, demanding payment in exchange for decryption.
- **Fileless malware**: This type of malware resides in a computer's memory instead of the hard drive, making it more challenging to detect and remove. It often leverages legitimate system tools and processes to carry out malicious activities.

Insider Threats

Insider threats are security risks that originate from within an organization, involving individuals with authorized access to its systems, data, or facilities. Nonprofits, like any other organization, must be vigilant against insider threats, as they can have severe consequences on the organization's operations, reputation, and stakeholder trust. The individuals involved in insider threats can be employees, volunteers, board members, or third-party contractors.

Verizon | Bitglass | Cybersecurity Insiders

Types of Insider Threats

- **Malicious insiders**: individuals who intentionally cause harm to the organization, either for personal gain, revenge, or ideological reasons. Malicious insiders may steal sensitive data, sabotage systems, or facilitate unauthorized access for external threat actors.
- **Unintentional insiders**: individuals who unknowingly expose the organization to security risks through negligence, lack of training, or failure to follow security policies. Unintentional insider threats may involve accidentally sharing sensitive information, falling for phishing scams, or using weak passwords.
- **Compromised insiders**: individuals whose accounts or devices have been compromised by external threat actors, allowing unauthorized access to the organization's systems and data. Compromised insiders may not be aware that their credentials or devices are being used for malicious purposes.

Distributed Denial of Service (DDoS) Attacks

Distributed Denial of Service (DDoS) attacks are a type of cyber threat that aims to overwhelm an organization's network, website, or online services with an excessive volume of traffic, rendering them inaccessible to legitimate users. Nonprofits, like any other organization, may be targeted by DDoS attacks, resulting in disruptions to their online presence, communication channels, and digital services. Understanding the nature of DDoS attacks and implementing effective mitigation strategies is essential for maintaining a nonprofit's digital resilience and fulfilling its mission.

Types of DDoS Attacks

- **Volume-based attacks**: These attacks aim to consume an organization's bandwidth by flooding the target with massive amounts of data. Common examples include User Datagram Protocol floods and Internet Control Message Protocol floods.
- **Protocol-based attacks**: These attacks exploit vulnerabilities in network protocols to exhaust resources or create bottlenecks. Examples include synchronization floods, Ping of Death, and Smurf attacks.
- **Application-layer attacks**: Also known as Layer 7 attacks, these target specific applications or services at the application layer of the Open Systems Interconnection Model, often appearing as legitimate traffic. Examples include HTTP floods and Slowloris attacks.

Building a Security-Conscious Culture

Creating a security-conscious culture within a nonprofit organization is essential for maintaining a strong cyber security posture. By fostering an environment where employees, volunteers, and partners prioritize security, nonprofits can more effectively mitigate risks and protect sensitive information.

Leadership Commitment

Executive leadership plays a critical role in promoting a security-conscious culture. Leaders should:

- Demonstrate a commitment to cyber security by actively participating in security initiatives and supporting investments in security measures.
- Communicate the importance of cyber security to the organization's mission, emphasizing the potential consequences of security incidents.

Security Awareness Training

Regular security awareness training helps employees, volunteers, and partners understand their role in protecting sensitive data and reducing security risks:

- Provide training on various cyber security topics, such as phishing attacks, social engineering, password security, and secure data handling.
- Offer ongoing training and updates to ensure that staff stays informed about emerging threats and best practices.

Clear Policies and Procedures

Develop and communicate clear security policies and procedures that outline expectations and responsibilities for maintaining a secure environment:

- Make security policies easily accessible and ensure they are written in plain language.
- Provide guidance on how to report suspected security incidents and encourage open communication.

Employee Recognition and Accountability

Encourage a sense of responsibility for security by recognizing employees who demonstrate a strong commitment to cyber security and holding staff accountable for security lapses:

- Recognize and reward employees who proactively identify and report potential security issues or demonstrate exceptional security practices.
- Address security violations or negligence with appropriate disciplinary actions and use them as learning opportunities for the entire organization.

IBM 2020

Collaboration and Information Sharing

Promote collaboration and information sharing among different departments and teams to ensure a holistic approach to security:

- Encourage cross-departmental collaboration on security initiatives, fostering a shared understanding of security risks and responsibilities.
- Share information about potential threats, security incidents, and best practices to raise awareness and improve the organization's overall security posture.

Regular Evaluation and Improvement

Continuously evaluate and improve the organization's security culture to adapt to changing threats and technologies:

- Conduct periodic assessments of the organization's security culture, using surveys, focus groups, or interviews to gauge employee attitudes and behaviors.
- Identify areas for improvement and develop strategies to address weaknesses, such as targeted training, updated policies, or increased communication efforts.

Summary

Ignoring data security can lead to severe consequences. To mitigate these risks, nonprofits must focus on building a security-conscious culture, with leadership commitment, security awareness training, clear policies and procedures, employee accountability, and regular evaluation. By prioritizing data security, nonprofits can safeguard their mission, protect stakeholder trust, and ensure the longevity of their operations in an increasingly digital world.

Parts 2 and 3 Coming Soon

Keep a lookout in your email for Part 2, set to be available for download in two weeks. This installment will guide you through assessing your data security risk and suggest ways to bolster your security measures. Two weeks later, expect a link to Part 3 in your inbox. This section will detail how to create a data security plan and why it's beneficial to work with experts, along with advice on how to pick a trustworthy one.