Safeguarding Your Mission

PROTECTING YOUR NONPROFIT FROM CYBER THREATS

filament
ESSENTIAL SERVICES
filamentservices.org

AUGUST 2023

Contents

filament
ESSENTIAL SERVICES

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.

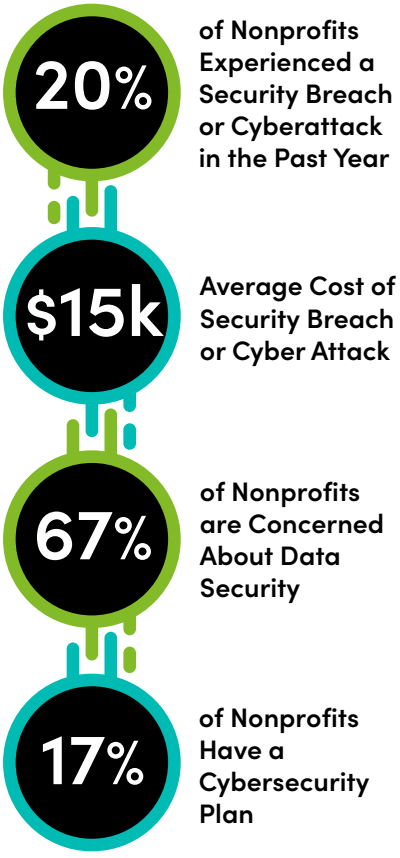
In 2020, the National Board of Medical Examiners (NBME) was targeted in a data breach that exposed the personally identifiable information (PII) and protected health information (PHI) of medical students and professionals. The breach resulted in a settlement of $275,000 with the New Jersey Division of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

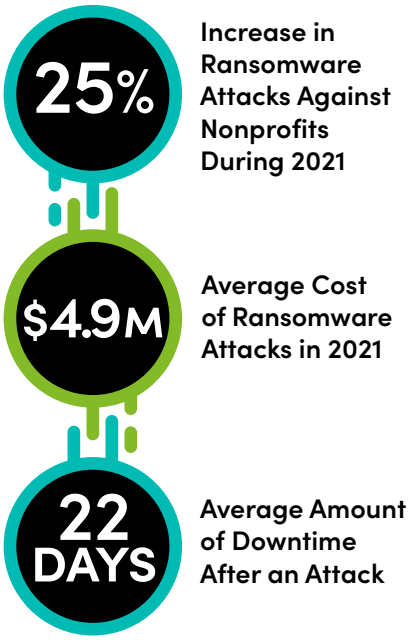
- **General phishing**: In this most common form of phishing, attackers send a large volume of generic emails to a broad audience, hoping that some recipients will fall for the scam. The emails often contain a sense of urgency and request the recipient click on a link or download an attachment.
- **Spear 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.

Assessing and Mitigating Your Data Security Risk

Identify and Inventory Hardware and Software

Inventorying systems and software is essential for nonprofit organizations. It enables effective asset management by providing a clear understanding of hardware and software resources, optimizing their utilization, and minimizing unnecessary costs. Maintaining an inventory helps identify vulnerabilities and risks, allowing organizations to prioritize security measures and protect against potential threats and data breaches. Inventorying systems and software ensures compliance with regulatory requirements such as data protection and licensing regulations.

Furthermore, having a comprehensive inventory supports disaster recovery and business continuity planning, enabling organizations to prioritize critical systems and data for backup and recovery purposes. It also facilitates efficient IT support and troubleshooting by providing necessary information about hardware and software configurations. Overall, an inventory serves as a valuable tool for nonprofit organizations, helping them make informed decisions, optimize costs, maintain security, and ensure the stability of their IT infrastructure.

Hardware Inventory Process

- **Establish a centralized inventory system**: Implement a centralized system to track and manage hardware inventory. This can be a spreadsheet, a dedicated inventory management tool, or a specialized asset management software.
- **Conduct initial inventory audit**: Perform an initial audit to identify and record all hardware assets owned by the nonprofit organization. Include details such as device type, manufacturer, model, serial number, purchase date, and location.
- **Assign unique identifiers**: Assign unique identifiers, such as asset tags or barcodes, to each hardware asset. This makes it easier to track and identify assets throughout their lifecycle.
- **Regular inventory updates**: Maintain an up-to-date inventory by conducting regular updates. This can be done on a quarterly or annual basis, or whenever significant changes occur (e.g., new purchases, retirements, or relocations).
- **Track hardware movements**: Log any hardware movements or transfers within the organization, including changes in location, assignment to different employees or departments, or loaned assets.

Ponemon Institute | NIST | Snyk & F5 Networks

Software Inventory Process

- **Software discovery**: Perform a thorough discovery process to identify and document all software applications used within the nonprofit organization. This includes both commercial software and internally developed applications.
- **License tracking**: Keep track of software licenses and ensure compliance with licensing agreements. Maintain records of license details, such as product keys, purchase dates, license quantities, and renewal dates.
- **Document versions and updates**: Document the software versions and updates installed on each device. This helps to ensure that software is kept up to date with the latest security patches and feature enhancements.
- **Regular software audits**: Conduct periodic software audits to verify that the installed software matches the organization's license agreements and that unauthorized or unlicensed software is not being used.
- **Centralized software repository**: Maintain a centralized repository or documentation system to store software license agreements, installation media, and relevant documentation for easy access and reference.

Identifying and Classifying Sensitive Data

For nonprofits, understanding the types of sensitive data they handle is critical to developing a robust data security strategy. Identifying and classifying sensitive data helps organizations prioritize their cyber security efforts and allocate resources more effectively, while ensuring compliance with applicable data protection regulations.

Identifying Sensitive Data

To identify sensitive data, nonprofits should start by conducting an inventory of all the data they collect, process, store, and transmit. This includes data related to donors, beneficiaries, employees, volunteers, partners, and other stakeholders. Sensitive data can be found across various systems, including databases, file storage, email systems, and cloud-based services. Key types of sensitive data that nonprofits typically handle include:

- **Personal Identifiable Information (PII)**: This includes names, addresses, phone numbers, email addresses, Social Security numbers, and any other information that can be used to identify an individual.
- **Financial Information**: Data related to donations, such as credit card numbers, bank account details, and transaction histories.
- **Health Information**: Medical records, health conditions, treatment information, and other health-related data, particularly relevant for nonprofits in the healthcare sector.
- **Confidential Organizational Information**: Internal documents, strategic plans, financial reports, and other proprietary information that is not meant for public disclosure.

Collectively, these inventories provide a holistic view of the organization's information technology landscape and help establish a strong foundation for information security. They allow organizations to prioritize security measures, address vulnerabilities, enforce access controls, and effectively respond to security incidents. Regularly updating and reviewing these inventories ensures ongoing information security readiness and adherence to best practices and regulatory requirements.

Classifying Sensitive Data

Once sensitive data has been identified, nonprofits should classify it based on its level of sensitivity and the potential impact of unauthorized access, disclosure, or loss. A common approach to data classification involves assigning categories, such as:

- **Public**: Information that is freely available to the public and does not pose a risk if disclosed.
- **Internal**: Information that is intended for use within the organization but is not highly sensitive.
- **Confidential**: Sensitive information that, if disclosed, could harm the organization or individuals involved.
- **Restricted**: Highly sensitive information that requires the highest level of protection and access control, such as financial data or personal health information.

Implementing Sensitive Data Protection Measures

Based on the classification of sensitive data, nonprofits should implement appropriate data protection measures to safeguard the identified information. This may include:

- **Access controls**: Limit access to sensitive data based on the principle of least privilege, ensuring that individuals only have access to the data they need to perform their job duties.
- **Data encryption**: Encrypt sensitive data both at rest and in transit to protect it from unauthorized access or interception.
- **Data retention and disposal policies**: Develop policies for the retention and secure disposal of sensitive data, ensuring that it is not kept for longer than necessary and is properly destroyed when no longer needed.
- **Regular audits and monitoring**: Conduct regular audits and monitoring of sensitive data access and usage to detect and respond to potential security incidents.

Secure Your People, Too

Educate employees on data security awareness and best practices.

Regularly reinforce the importance of data security to foster a security-conscious culture within the organization.

Mapping Data Flows

Understanding how sensitive data flows within a nonprofit organization is an essential component of a comprehensive data security risk assessment. Mapping data flows allows nonprofits to identify potential vulnerabilities and risks within their systems, processes, and third-party relationships, helping them prioritize their cyber security efforts and implement appropriate controls.

Identifying Data Entry Points

The first step in mapping data flows is to identify all the points where sensitive data enters the organization. This may include online donation forms, beneficiary intake forms, volunteer applications, employee records, and partner data sharing. Data entry points can be both digital (e.g., web forms and email) and physical (e.g., paper forms and in-person interactions).

Mapping Data Processing and Storage

Once the data entry points have been identified, nonprofits should map out the processes and systems involved in handling sensitive data. This includes:

- **Data processing**: Identify and document all the processes and systems that manipulate, analyze, or transform the sensitive data. This may involve sorting, filtering, aggregating, or generating reports based on the data.
- **Data storage**: Determine where sensitive data is stored within the organization. This may include databases, file servers, cloud storage services, and physical records.
- **Data access and sharing**: Identify who has access to sensitive data and how it is shared within the organization or with external partners. This includes employees, volunteers, third-party service providers, and other stakeholders.

Why is this important?

Data flow mapping is the process of visualizing and documenting how data moves within your systems, networks, and processes.

It helps identify potential risks, vulnerabilities, and areas for improvement in data security, compliance, and overall data management.

Assessing Data Flow Risks

After mapping the data flows, nonprofits should assess the potential risks associated with each stage of data handling. This may include:

- **Insecure data transmission**: Assess whether sensitive data is transmitted securely, both internally and externally. This may involve checking whether data encryption is used during transmission and whether secure communication channels, such as HTTPS and secure file transfer protocols, are employed.
- **Inadequate access controls**: Evaluate whether access to sensitive data is appropriately restricted based on the principle of least privilege and whether strong authentication mechanisms are in place.
- **Third-party risks**: Assess the security practices of third-party service providers and partners who have access to sensitive data, ensuring they adhere to appropriate security standards and contractual obligations.
- **Compliance requirements**: Identify any regulatory or industry-specific data protection requirements that apply to the organization and ensure that data handling practices meet these standards.

Implementing Data Flow Controls

Based on the identified risks, nonprofits should implement appropriate controls to protect sensitive data throughout its lifecycle. This may include:

- **Data encryption**: Employ encryption for sensitive data both at rest and in transit to protect it from unauthorized access or interception.
- **Secure data storage**: Implement robust security measures for data storage, such as access controls, encryption, and regular backups.
- **Data loss prevention (DLP) tools**: Use DLP tools to monitor and control the movement of sensitive data within the organization and prevent unauthorized data transfers or leaks.
- **Third-party risk management**: Establish processes to assess and manage the risks associated with third-party relationships, including conducting regular security assessments and updating contractual agreements as needed.

Jane's Story

Jane used data flow mapping at her nonprofit to safeguard sensitive donor information.

She discovered an overlooked data transfer with a vendor lacking security controls.

Jane worked with the vendor to implement proper measures and update policies.

Months later, a cyber attack hit a similar organization, but Jane's nonprofit was protected.

Data flow mapping helped identify and mitigate vulnerabilities, protecting donor trust.

Conducting a Risk Assessment

Performing a risk assessment is an essential step for nonprofits to evaluate their data security posture, identify potential vulnerabilities, and prioritize cyber security efforts. A well-executed risk assessment provides a foundation for developing and implementing a comprehensive data security strategy tailored to the organization's needs.

Define the Scope of the Risk Assessment

Start by defining the scope of the risk assessment, including the systems, processes, and data that will be evaluated. This may involve considering the organization's mission, critical business functions, and the types and sensitivity of data handled by the nonprofit.

Assess Vulnerabilities

Evaluate the organization's vulnerabilities by examining existing security controls, processes, and policies. This may involve conducting technical assessments, such as vulnerability scans and penetration tests, as well as reviewing organizational policies and procedures related to data security, employee training, and incident response.

Determine Likelihood and Impact

For each identified threat and vulnerability, assess the likelihood of occurrence and the potential impact on the organization's assets, operations, and reputation. This can help prioritize risks based on their potential consequences and inform decision-making about where to allocate resources and implement controls.

Develop Risk Mitigation Strategies

Develop strategies to mitigate the identified risks, which may include:

- Implementing technical controls (e.g., firewalls, intrusion detection systems, and encryption)
- Strengthening policies and procedures (e.g., access controls, data classification, and incident response plans)
- Providing employee training and awareness programs to reduce the risk of human error
- Establishing a business continuity and disaster recovery plan to ensure the organization can recover from disruptions and resume operations quickly

Monitor and Review

Regularly monitor and review the risk assessment process to ensure it remains up-to-date and reflects any changes in the organization's environment, such as new threats, technologies, or regulatory requirements. This may involve conducting periodic risk assessments, reviewing and updating policies and procedures, and implementing continuous monitoring of security controls and incident detection.

Strengthen Technical Security Measures

Improving technical security measures is a crucial aspect of a nonprofit's cyber security strategy. By implementing robust technical controls, nonprofits can better protect their digital assets, safeguard sensitive data, and reduce the likelihood of security incidents.

Network Security

Implement network security measures to protect the organization's network infrastructure and prevent unauthorized access to sensitive data:

- **Firewalls**: Deploy firewalls to filter incoming and outgoing network traffic, blocking malicious traffic and reducing the risk of cyberattacks.
- **Intrusion Detection and Prevention Systems (IDS/IPS)**: Use IDS/IPS to monitor network traffic for signs of malicious activity and block or alert about potential threats in real-time.
- **Virtual Private Networks (VPNs)**: Encourage the use of VPNs for remote access to the organization's network to ensure secure, encrypted connections.

Endpoint Security

Enhance endpoint security to protect devices such as computers, smartphones, and tablets that connect to the organization's network:

- **Antivirus** and Anti-malware: Install Endpoint Detection and Recovery software on all devices and ensure they are regularly updated to detect and prevent malware infections.
- **Patch Management**: Implement a patch management process to monthly update software, operating systems, and firmware with the latest security patches and fixes.
- **Device Management**: Establish a device management policy that enforces security settings, such as screen locks, encryption, and remote wipe capabilities.

Nonprofit Finance Fund | TechSoup | Nonprofit Tech for Good

Access Controls

Strengthen access controls to limit access to sensitive data and systems:

- **Principle of Least Privilege**: Grant users the minimum level of access required to perform their job functions, reducing the potential impact of unauthorized access or insider threats.
- **Role-Based Access Control (RBAC)**: Implement RBAC to assign permissions based on predefined roles and responsibilities, simplifying the management of user access rights.
- **Multi-Factor Authentication (MFA)**: Require MFA for accessing sensitive systems and data and all administrative use, adding an additional layer of security beyond just a username and password.

Encryption

Employ encryption to protect sensitive data both at rest and in transit:

- **Data Encryption**: Encrypt sensitive data stored on devices, servers, and cloud storage services to protect it from unauthorized access.
- **Secure Communication Channels**: Use secure communication channels, such as HTTPS, SSL/TLS, and secure file transfer protocols, to encrypt data transmitted over the Internet.

Backup and Recovery

Implement a robust backup and recovery strategy to ensure the organization can recover from data loss or system failure:

- **Regular Backups**: Schedule regular backups of critical data, systems, and configurations, and store backup copies offsite or in the cloud.
- **Disaster Recovery Plan**: Develop a disaster recovery plan that outlines the steps and procedures for restoring data, systems, and operations in the event of a disaster or security incident.

Continuous Monitoring

Implement continuous monitoring of security controls and systems to detect and respond to potential security incidents:

- **Security Information and Event Management (SIEM)**: Use SIEM tools to collect, analyze, and correlate security event data from various sources, enabling the organization to detect and respond to incidents more effectively.
- **Vulnerability Scanning and Penetration Testing**: Conduct regular vulnerability scans and penetration tests to identify potential weaknesses in the organization's systems and networks and remediate any identified vulnerabilities.

Developing a Data Security Plan

Developing clear and comprehensive security policies and procedures is an essential step for nonprofits in creating a robust data security plan. These policies and procedures provide a framework for implementing security best practices, ensuring compliance with regulations, and fostering a culture of security awareness within the organization.

Define the Purpose and Scope

Begin by defining the purpose and scope of the security policies and procedures, outlining the specific goals and objectives they aim to achieve. This may include protecting sensitive data, ensuring compliance with data protection regulations, and minimizing the risk of security incidents.

Identify Key Stakeholders

Identify the key stakeholders who will be involved in the development, implementation, and enforcement of the security policies and procedures. This may include IT personnel, executive leadership, and representatives from various departments, such as finance, human resources, and program management.

Develop Written Policies

Create written policies that address various aspects of data security, including:

- **Data classification**: Establish a system for categorizing data based on its sensitivity and the potential impact of unauthorized access or disclosure.
- **Access controls**: Define rules and guidelines for granting and revoking access to sensitive data, ensuring that individuals only have access to the data necessary for their job functions.
- **Authentication and authorization**: Specify the methods and technologies used to authenticate users and authorize access to sensitive data, such as strong passwords, multi-factor authentication, and role-based access controls.
- **Data encryption**: Set requirements for encrypting sensitive data both at rest and in transit to protect it from unauthorized access or interception.
- **Incident response**: Develop a plan for identifying, responding to, and recovering from data security incidents, including roles and responsibilities, communication protocols, and reporting requirements.

Writing Policies

A well-crafted data security policy can provide a critical roadmap for protecting an organization's data assets.

A good policy is clear, concise, and written in language that all employees can understand.

It should be effectively communicated and accessible to everyone in the organization, with regular training provided to ensure everyone understands their responsibilities.

- **Data retention and disposal**: Establish guidelines for retaining and securely disposing of sensitive data, ensuring that it is not kept for longer than necessary and is properly destroyed when no longer needed.
- **Compliance**: Outline the organization's responsibilities and processes for complying with relevant data protection regulations and industry standards.

Establish Standard Operating Procedures (SOPs)

Develop detailed standard operating procedures (SOPs) that provide step-by-step instructions for implementing the security policies. SOPs should be tailored to the specific needs of the nonprofit and its employees, volunteers, and partners, and may cover topics such as:

- Secure data handling and storage practices.
- Use of secure communication channels and file transfer protocols.
- Regular patching and updating of software and systems.
- Security awareness training and education.

Communicate and Train

Ensure that employees, volunteers, and partners are aware of the security policies and procedures, and provide regular training to reinforce best practices and maintain a culture of security awareness. Training topics may include recognizing phishing attacks, creating strong passwords, and reporting suspected security incidents.

Monitor and Review

Regularly monitor compliance with the security policies and procedures, and review and update them as needed to reflect changes in the organization's environment, such as new threats, technologies, or regulatory requirements. This may involve conducting periodic audits, implementing continuous monitoring of security controls, and soliciting feedback from employees and other stakeholders.

Establishing Standard Operating Procedures (SOPs) is crucial for organizations because they provide a framework for consistency, efficiency, and quality control in business operations.

They streamline training and onboarding, ensuring new employees understand their roles and responsibilities effectively. SOPs also foster accountability, enabling easier identification of errors and areas for improvement.

In industries with regulatory requirements, SOPs aid in maintaining compliance and safety standards.

Finally, they offer a contingency plan for personnel absence and a blueprint for scalability during business growth.

Regular reviews and updates of SOPs are necessary to align with evolving business needs and best practices.

Advantages of Partnering with Experts

Collaborating with cybersecurity experts can provide significant benefits to nonprofits, helping them navigate the complex landscape of data protection and strengthening their overall security posture. By leveraging the expertise of these professionals, nonprofits can better protect sensitive data, comply with regulations, and maintain the trust of their stakeholders.

Access to Specialized Expertise

Cybersecurity experts possess in-depth knowledge of the latest threats, technologies, and best practices, enabling nonprofits to benefit from their specialized expertise:

- Stay up-to-date with evolving cybersecurity trends, ensuring that the organization's security measures are current and effective.
- Receive guidance on implementing advanced security controls and technologies tailored to the nonprofit's unique needs and requirements.

Proactive Threat Identification and Management

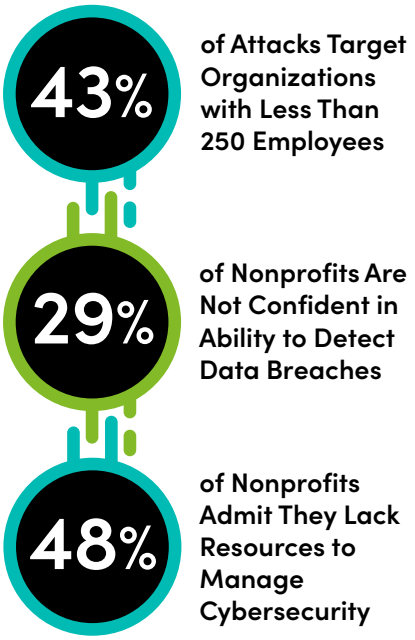
Partnering with cybersecurity experts can help nonprofits proactively identify and manage potential threats before they become security incidents:

- Conduct regular vulnerability assessments and penetration tests to identify weaknesses in the organization's systems and networks.
- Receive real-time threat intelligence and alerts, enabling the nonprofit to take preventive actions and minimize risks.

Improved Incident Response and Recovery

In the event of a security incident, cybersecurity experts can provide invaluable assistance in responding to and recovering from the attack:

- Develop and implement incident response plans, ensuring that the nonprofit is prepared to respond effectively to security incidents.
- Provide support during an incident, helping the organization to contain and remediate the threat, recover lost data, and minimize downtime.



Symantec | Nonprofit Technology Network | Ponemon

Regulatory Compliance and Risk Management

Cybersecurity experts can help nonprofits navigate the complex world of data protection regulations and ensure compliance:

- Provide guidance on complying with relevant regulations, such as the Payment Card Industry Digital Security Standards (PCI DSS) or the Gramm Leach Bliley Act (GLBA).
- Assist in conducting risk assessments and developing risk management strategies, helping the organization prioritize its security efforts and allocate resources effectively.

Employee Training and Security Awareness

Cybersecurity experts can help nonprofits create and deliver effective security awareness training programs for their employees, volunteers, and partners:

- Develop customized training materials that address the specific needs and risks of the nonprofit.
- Offer ongoing training and updates to ensure staff stays informed about emerging threats and best practices.

Cost Savings and Resource Optimization

Working with cybersecurity experts can be more cost-effective than maintaining an in-house security team, especially for smaller nonprofits with limited resources:

- Access specialized expertise without the need to hire, train, and retain a full-time security staff.
- Optimize resource allocation, enabling the nonprofit to focus on its core mission while the cybersecurity experts handle data protection.

Selecting a Data Security Partner

Choosing the right data security partner is crucial for nonprofits looking to enhance their cybersecurity posture. The right partner can help protect sensitive data, maintain regulatory compliance, and ensure the ongoing success of the organization's mission. Consider the following factors when selecting a data security partner for your nonprofit:

Expertise and Experience

Evaluate the expertise and experience of potential data security partners:

- Check for relevant certifications and accreditations, such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), or Certified Information Security Manager (CISM).
- Look for a partner with experience working with nonprofit organizations, as they will understand the unique challenges and requirements of the sector.
- Review case studies and testimonials from previous clients to assess the partner's track record in delivering successful cybersecurity solutions.

Range of Services

Determine if the potential partner offers a comprehensive range of data security services tailored to the needs of your nonprofit:

- Ensure they provide services such as vulnerability assessments, penetration testing, security audits, and risk management.
- Confirm that they offer assistance with regulatory compliance and can help your organization navigate complex data protection regulations.
- Check whether they can develop and deliver customized security awareness training programs for your employees, volunteers, and partners.

Communication and Collaboration

Effective communication and collaboration are essential for a successful partnership:

- Look for a partner who values open communication and is willing to listen to your organization's concerns and requirements.
- Assess their responsiveness and availability, ensuring that they can provide timely support when needed.
- Ensure that the partner is willing to collaborate closely with your organization, integrating their services seamlessly into your existing processes and systems.

Scalability and Flexibility

Choose a data security partner that can scale and adapt to your organization's changing needs:

- Ensure they can accommodate your nonprofit's growth, providing scalable solutions that can evolve alongside your organization.
- Confirm that they can adapt their services to meet the changing needs and requirements of your nonprofit, such as new technologies, emerging threats, or regulatory changes.

Cost and Value

Consider the cost and value of partnering with a data security provider:

- Evaluate the pricing structure of potential partners, ensuring that it aligns with your organization's budget and resource constraints.
- Assess the value of the services provided, considering factors such as the potential cost savings from outsourcing security tasks, reduced risk of security incidents, and improved regulatory compliance.

Cultural Fit

Finally, look for a data security partner that shares your organization's values and mission:

- Choose a partner that understands the unique challenges and goals of nonprofits, demonstrating a genuine commitment to helping your organization succeed.
- Assess the cultural fit between your organization and the potential partner, ensuring that they will be able to work effectively with your team and support your mission.

Summary

Safeguarding your nonprofit's mission from the ever-present risk of cyber threats and data breaches is crucial for maintaining stakeholder trust, ensuring financial stability, and preserving your organization's reputation. As the risks continue to evolve, partnering with a cybersecurity professional to conduct a thorough assessment is a proactive step towards building a robust defense against potential threats.

By leveraging the expertise of professionals, your nonprofit can develop a comprehensive data security plan that effectively mitigates risks, maintains regulatory compliance, and promotes a security-conscious culture. Don't let your organization's mission be jeopardized by inadequate data security measures; reach out to a cybersecurity expert today and secure your nonprofit's digital assets for a safer and more resilient future.