Safeguarding Your Mission

PROTECTING YOUR NONPROFIT FROM CYBER THREATS

PART 2 OF 3

filament
ESSENTIAL SERVICES
filamentservices.org

JULY 2023

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.

54% of Organizations Experienced a Breach Due to Unsecure Hardware

90% of Incidents are Caused by Hardware and Software Vulnerabilities

76% of Organizations Experienced an Incident Due to Unesecure Software

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

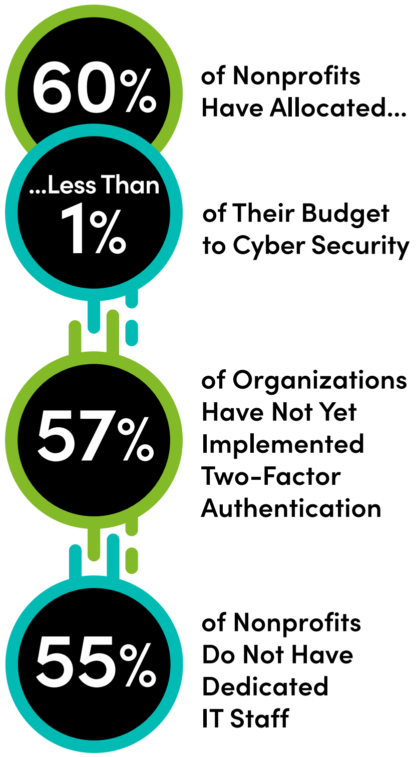
Implement network security measures to protect the organization's network infrastructure and prevent unauthorized access to sensitive data:

- **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.



60% of Nonprofits Have Allocated...

...Less Than 1% of Their Budget to Cyber Security

57% of Organizations Have Not Yet Implemented Two-Factor Authentication

55% of Nonprofits Do Not Have Dedicated IT Staff

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.

Summary

In today’s digital landscape, ensuring data security is crucial for all organizations, including nonprofits. By assessing and mitigating data security risks, nonprofits can protect sensitive information, comply with regulations, and maintain the stability of their IT infrastructure. By prioritizing data security and implementing these measures, nonprofits can safeguard their valuable data, make informed decisions, and mitigate potential cybersecurity risks.