Safeguarding Your Mission

PROTECTING YOUR NONPROFIT FROM CYBER THREATS

PART 3 OF 3

filament
ESSENTIAL SERVICES
filamentservices.org

AUGUST 2023

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.

43% **of Attacks Target Organizations with Less Than 250 Employees**

29% **of Nonprofits Are Not Confident in Ability to Detect Data Breaches**

48% **of Nonprofits Admit They Lack Resources to Manage Cybersecurity**

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.