WE ARE NATIONWIDE 24 / 7 / 365

CYBERSECURITY: UNIQUE NEEDS OF THE NONPROFIT SECTOR AND HOW i4DM CAN HELP

Over the past few years, nonprofits have begun adopting digital strategies to gain efficiencies and make a greater impact in the communities they serve by leveraging information technology (IT) tools and resources to manage operations through digital systems, accept donations, run events, and coordinate efforts across their increasingly remote or hybrid workforce and volunteer teams. The benefit of digital connectivity comes with heightened vulnerability to cyberattacks. For nonprofits cybersecurity is no longer an option – it's a priority.

Nonprofit organizations have become the second most targeted sector by cybercriminals

31% of all notifications of attacks were against nonprofit organizations, as detected by Microsoft.[1]

And that's where i4DM can help. We work with you to define a strategy that aligns with your goals and budget. We prioritize the security of your client data and donor management systems, while reinforcing the essential technologies you need to make a lasting impact. Defining and managing a cybersecurity strategy can be intimidating and overwhelming, and there is no one-size-fits-all solution. We take the guesswork out of IT by implementing strategies that meet the organization's needs so you can energize your teams to advance your mission.

Beyond the Basics – i4DM's Cybersecurity Guide for Nonprofits

People and Culture

- Entrust your managed service provider (MSP) to complement your digital onboarding process by streamlining asset procurement, setup, delivery, and monitoring, while providing your new team members with the necessary resources and information they need for a smooth transition to the team.
- Empower your staff and volunteers by helping them understand their role in protecting the organization's infrastructure and data. Ensure that the right people have appropriate access to the right data at the right time.
- Provide ongoing cybersecurity training and build awareness by showing them how to recognize and avoid phishing scams.
- Leverage technology to improve the volunteer experience and value they bring to your organization through vetted volunteer management systems, screening, learning management systems, video conferencing tools, encryption protocols and secure storage, and role-based access control.

Technology and Tools

- Create a multilayer defense strategy by deploying a combination of security technologies such as firewalls, intrusion detection/prevention systems (IDS/IPS), antivirus software, and encryption.
- Enforce robust access controls and identity management systems, including multifactor authentication (MFA), password policies, single sign-on solutions, least privilege access, and maintain visibility through regular access audits.
- Secure the network perimeter and internal networks through endpoint protection, virtual private networks, segmentation, monitoring, and intrusion detection systems.
- Secure online donations with a payment card industry data security standard (PCI) compliant payment processor, while ensuring the platform provides encryption or other protections for donor data.

Ashley Johnson | M: 410.846.9138 | E: amjohnson@i4DM.com

CYBERSECURITY: UNIQUE NEEDS OF THE NONPROFIT SECTOR & HOW i4DM CAN HELP

Risk Management and Governance

- Conduct regular vulnerability scans and risk assessments to identify potential threats and weaknesses that could put your organization's assets at risk.
- Implement an incident response plan that outlines the process and procedures for detecting, responding to, and recovering from cybersecurity events.
- Ensure that your organization maintains the compliance requirements set by government regulations like HIPAA, key vendor and partner relationships, and grant-based restrictions. These requirements may include cybersecurity insurance coverage, third-party risk management, backup, recovery, and incident response plans.
- Implement measures to ensure your external partners adhere to security standards that align with your overall strategy.

Processes and Procedures

- Ensure coordination between IT, security, legal, and other relevant departments to address cybersecurity issues comprehensively. Foster a culture of collaboration to enhance overall security posture.
- Implement a formal change management process to evaluate the security implications of changes to systems, applications, and configurations.
- Deploy security information and event management (SIEM) systems penetration testing and assessments and security audits to continuously track and analyze network traffic, system activities, and user behaviors.

Are you ready to maximize the benefits of IT? We'll work with you and your teams to ensure the tools, resources, training, and processes are in place to enhance organizational effectiveness, mitigate risks, and foster a culture that encourages continuous improvement while adopting a security-first mindset.

Let's put technology to work – *for good*. Contact Ashley to get the conversation started.

Ashley Johnson
Technical Account Manager

M: 410.846.9138 | E: amjohnson@i4DM.com | i4DM.com

[1]Cyberpeaceinstitute.org, 2024. Cyber-poor, target-rich: The Crucial Role of Cybersecurity in Nonprofit Organizations