WE ARE NATIONWIDE 24 / 7 / 365

TARGET-RICH AND CYBER-POOR: THE IMPACT OF CYBERCRIME ON THE NONPROFIT SECTOR

i4DM
MISSION POSSIBLE

The nonprofit sector, driven by its mission to support communities and advance social causes, is increasingly vulnerable to the impacts of cybercrime. As nonprofits adopt more digital tools to enhance their operations, streamline fundraising, and engage with supporters, they unwittingly become attractive targets for cybercriminals seeking to exploit sensitive data and undermine the ability of organizations to fulfill their missions effectively.

The effects of cybercrime on nonprofits can be profound, ranging from financial losses and reputation damage to disrupting essential services and compromised donor trust. The increasing sophistication of cyber threats magnifies the critical need for robust cybersecurity measures to protect these organizations and ensure they can continue their vital work without interruption.

There is no question that digital threats are evolving at an unprecedented rate. Not only is the frequency of attacks increasing, but the efficacy of cybercriminal attack vectors is continuously improving due to technological advancements, increased sophistication, adaptation to defenses, and collaboration among cybercriminals. Organizations must stay vigilant and proactively update their security measures to counter these evolving threats. As your partner, i4DM makes it our mission to regularly update defenses, conduct threat intelligence, and engage in continuous cybersecurity modeling and training so that we take on the burden of anticipating and preventing these attacks.

In the first half of 2024, the paths that cyber criminals used to gain unauthorized access to a network, computer system, or application were as follows:

	H1 2022		H1 2023		H1 2024
CYBERATTACKS	730	↑ 42%	1,035	↑ 18%	1,226
SYSTEM & HUMAN ERROR	67	↑ 369%	314	↓ 51%	155
PHYSICAL ATTACKS	16	↑ 94%	31	↓ 50%	18
UNKNOWN	4	↓ 50%	2	↑ 8,500%	172

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

WE ARE NATIONWIDE 24 / 7 / 365

TARGET-RICH AND CYBER-POOR | THE IMPACT OF CYBERCRIME ON THE NONPROFIT SECTOR

Disruption of Operations and Essential Services

Cyberattacks can disrupt or disable the systems that manage and deliver essential services, such as food assistance, healthcare, and emergency support. They can cause significant downtime by disrupting access to critical systems, databases, and communication tools needed to carry out daily operations, manage programs, and respond to urgent needs. These disruptions may compromise the quality of critical services and delay their ability to provide services — preventing those in need from accessing the tools used to request service and deliver support. Cyber incidents may also delay the application process, forcing beneficiaries to wait longer for the services or financial assistance support they need.

THE NONPROFIT SECTOR RAISES OVER

$1 TRILLION

annually to deliver programs that bring lifesaving assistance and protection

In today's volatile international environment, nonprofit organizations play a central role in providing humanitarian relief and protecting the human rights of over 1 billion vulnerable individuals worldwide.

Compromised Data and Personal Information

Cybercriminals may steal sensitive personal information from beneficiaries, such as Social Security numbers, addresses, and financial details. This can lead to identity theft, financial fraud, and harmful personal and financial ramifications for those affected. Personal data breaches can result in the unauthorized exposure of beneficiaries' private information, leading to privacy violations and potential data misuse. Beneficiaries who experience financial fraud resulting from a data breach may face additional costs to resolve issues such as credit monitoring or fraud protection services. This adds to their financial burden and can affect their overall well-being.

1.5 M

INDIVIDUALS ARE AFFECTED BY CYBERATTACKS

Erosion of Trust

Beneficiaries may lose trust in the nonprofit organization's ability to safeguard their personal information and manage services. A breach can reduce their willingness to engage with or rely on the organization for support or become anxious or emotionally distressed at the thought of their personal information being stolen or that exposure to sensitive data could lead to stigmatization or discrimination, especially if particularly personal or health-related information is made public. High-profile cyberattacks can attract media attention, resulting in negative publicity that can damage the organization's reputation and affect its ability to attract funding and volunteers.

68%

OF NONPROFITS HAVE EXPERIENCED A DATA BREACH IN THE PAST THREE YEARS

Loss of Volunteer Confidence

Cybercrime incidents can erode volunteer confidence in the nonprofit's ability to protect their personal information. The attacks may also affect systems used to schedule, communicate, and manage volunteers, making it difficult for volunteers to perform their roles effectively. The long-term impact may result in a decrease in volunteer participation and support.

Financial Losses

Cybercriminals may steal funds directly from nonprofit accounts through phishing schemes, ransomware attacks, or unauthorized access to financial systems. This can lead to significant financial losses and disrupt critical operations. In cases of ransomware attacks, nonprofits may be forced to pay ransoms to regain access to their data, which can be financially burdensome and divert resources away from their core missions.

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

WE ARE NATIONWIDE 24 / 7 / 365

TARGET-RICH AND CYBER-POOR | THE IMPACT OF CYBERCRIME ON THE NONPROFIT SECTOR

The costs associated with recovering from a cyberattack, including system repairs, data recovery, and cybersecurity enhancements, can be substantial. These expenses may strain the organization's budget and divert funds away from mission-critical activities. Nonprofits may see increased premiums for cyber insurance as a result of cybercrime incidents, adding to their operational costs and potentially limiting resources available for other areas. Nonprofits may need to divert resources to address legal and compliance issues arising from cyber incidents, which can reduce the resources available for direct beneficiary support.

U.S. Cybercrime Costs Based on the Number of Cybercrime Victims in the Nonprofit Sector in H1 2024

$621,173,635	$51,851,652	$1,700,054	$65,387	$1,177
YEAR	MONTH	DAY	HOUR	MINUTE

Legal and Compliance Risks

Nonprofits may face legal and regulatory consequences obligating them to notify affected individuals and regulatory bodies about data breaches, which can result in legal fees, fines, and additional administrative burdens — or worse, affect their ability to continue offering services.

The breadth of legal and compliance issues extends beyond the nonprofit itself. Vendors often have access to sensitive information, including donor data, financial records, and internal communications. If a vendor's cybersecurity is compromised, it can lead to a breach of your organization's data and systems.

OVER
1,300
NONPROFITS FACED INDIRECT DATA COMPROMISES DUE TO BREACHES FROM SUPPLIERS OR VENDORS

13% of organizations continuously monitor the security risks associated with their external partners.

98% of organizations worldwide are integrated with at least one third-party vendor that has suffered a breach in the past two years.

Failure to protect sensitive data may violate data protection laws and regulations, such as as Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), or California Consumer Privacy Act (CCPA). Affected parties, including donors and beneficiaries, may pursue legal action against the nonprofit for failing to adequately protect their data, leading to potential lawsuits and additional financial liabilities. Your risk management and business continuity plans should address your overall recovery objectives, including IT and data protection, legal and regulatory compliance, cyber insurance, documentation and processes, and coordination with external partners to ensure you can quickly recover and continue your mission.

We can help you fortify your business continuity plan by safeguarding your IT and data systems, ensuring that you meet the requirements to maintain the right level of cybersecurity insurance, and providing the necessary training and resources to internal and external stakeholders to ensure you are technologically sound.

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

TARGET-RICH AND CYBER-POOR | THE IMPACT OF CYBERCRIME ON THE NONPROFIT SECTOR

Cybersecurity Insurance Coverage

First-Party: This type of cyber coverage protects data, including that of your employees and customers. It usually covers business costs that relate to legal counsel; recovery and replacement; customer notifications and help center services; lost income; crisis management; cyber extortion; breach investigation; related fees, fines, and penalties.

Third-Party: This type of cyber coverage generally protects you from liability if claims are made against you by a third party. Coverage can include payments made to affected consumers; claims and settlement expenses; losses related to defamation, copyright or trademark infringement; costs for litigation; accounting costs; and any additional costs related to damages, settlements, and judgments.

Cybercrime can have far-reaching and damaging effects on the nonprofit sector, impacting financial stability, operational efficiency, reputation, and donor trust. To mitigate these risks, nonprofits must prioritize cybersecurity measures and invest in robust data protection strategies.

Let's connect today and explore the ways i4DM can deliver the right-sized solutions designed exclusively to safeguard your organization, offer peace of mind, and support your efforts to fulfill your mission.

Ashley Johnson
Technical Account Manager

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