ProWriters
Professional & Management Liability Insurance

Why Nonprofits Need Cyber Insurance

Cyber criminals feel no compunction profiting from nonprofit organizations.

What makes nonprofits tempting targets? They frequently handle large amounts of money. They also collect and store substantial amounts of personal—often sensitive—data from donors, clients, and partner entities, as well as from their own employees and volunteers. Such information includes:

- **Names**
- **Birthdates**
- **Email addresses**
- **Bank account details**
- **Credit card numbers**
- **Social Security numbers**
- **Driver's license numbers**

Cyber criminals sometimes think nonprofits are softer targets because they're often smaller than for-profit businesses, with fewer resources to devote to IT staff and data security. But even large, international nonprofits are at risk.

In the wake of cyber crimes, nonprofits of all sizes can incur major expenses that threaten their revenue, reputation, and resiliency.

Cyber Risks Nonprofits Face

To the extent they use internet-connected devices, nonprofits face the same cyber risks as other businesses and organizations, including but not limited to:

1). Malware and ransomware attacks

Unwanted software installs itself, causing harm. Ransomware is the most common type, encrypting data and threatening to destroy or release it unless the target pays a ransom.

2). Cyber Crime

Threat actors work tirelessly to trick nonprofits into paying fraudulent invoices or transfer funds to the threat actors. This often starts via impersonation or a business email compromise event.

3). Unauthorized logins

Especially when organizations use weak passwords or don't use multifactor authentication (MFA), criminals can infiltrate accounts and systems with credentials stolen through brute force programs or deceit.

Since the information they hold is often extensive and valuable, nonprofits must be on guard against **data breaches** that occur as the result of not only outside cyber attacks but also breaches of third-party vendors and even authorized access by insiders.

Nonprofits also need to be especially vigilant against **social engineering fraud**. In social engineering, criminals impersonate known and trusted individuals or organizations, usually in "phishing" emails. They trick recipients into giving away access credentials, sensitive information, or funds via wire transfer. Also called **business email compromise (BEC)**, such social engineering attacks exploit human error and the person-to-person connections so critical to nonprofits' successful work.

ProWriters
Professional & Management Liability Insurance

Cyber Crime Against Nonprofits: Three Examples

To the extent they use internet-connected devices, nonprofits face the same cyber risks as other businesses and organizations, including but not limited to:

- Philabundance, one of the Philadelphia region's largest hunger relief organizations, paid a fraudulent invoice for more than $923,000. Fraudsters infiltrated Philabundance's systems via phishing emails. They then blocked legitimate emails and sent a spoofing email that looked like an authentic invoice from a construction company.
- One Treasure Island, a San Francisco nonprofit providing affordable housing for low-income and formerly homeless people, lost $650,000 when scammers entered the organization's email via a third-party bookkeeper, added themselves to email chains, impersonated the executive director in email, and altered a legitimate invoice and wire transfer instructions.
- The International Committee of the Red Cross suffered a cyber attack that compromised the personal data and confidential information of more than 515,000 vulnerable people worldwide. Hackers exploited a known but unpatched vulnerability, disrupting the ICRC's humanitarian services and raising the specter of the data being sold or leaked online.

What Should a Nonprofit's Cyber Insurance Policy Cover?

A strong Cyber Insurance policy provides crucial protection against the costly first- and third-party damages incurred during and after a data breach or other cyber incident. Examples include:

First-Party Coverage

- Replacing funds stolen in a cyber crime incident.
- Hiring forensic IT consultants to determine the breach's origin and extent.
- Repairing digital assets and replacing damaged equipment.
- Legal costs in advising how to respond to a breach.
- Notifying individuals whose information was exposed and providing them credit monitoring.
- Managing damage to the nonprofit's reputation through a public relations campaign.
- Lost profits from a Business interruption event.

Third-Party Coverage

- Legal representation in responding to claims or regulatory investigations.
- Document preparation.
- Claims related to negligence, breach of contract, and other issues.
- Payment card industry (PCI) fines, penalties, and assessments.