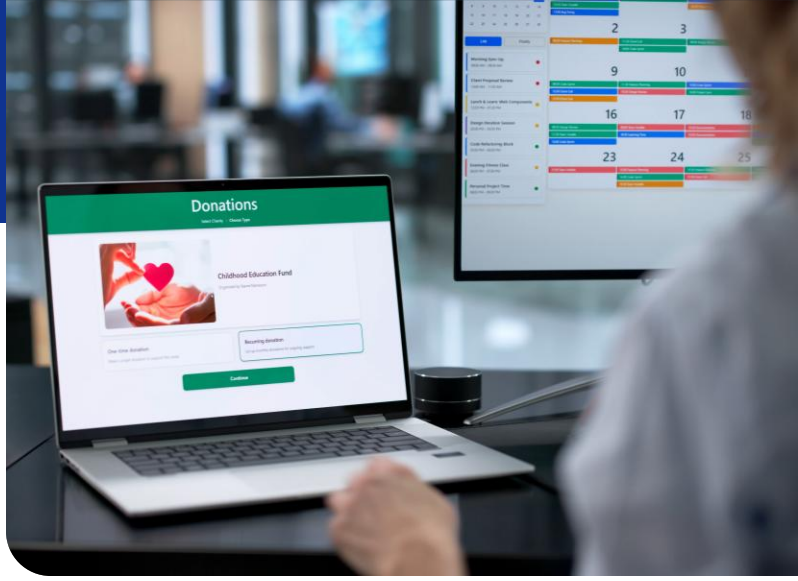
EPIC
Insurance Brokers & Consultants



CLIENT ALERT

When Fundraising Stops: What Recent Cyber Incidents Mean for Nonprofits

Two recent cyber incidents involving leading nonprofit fundraising platforms serve as a reminder that organizations face cyber risk not only from attacks on their own systems, but also from disruptions and breaches affecting third-party service providers.

Recent events involving DonorPerfect and GoFundMe Pro demonstrate how both cyberattacks and data breaches can create significant challenges for nonprofits, particularly during critical fundraising periods. While the nature of each incident differed, both underscore the importance of understanding and managing third-party cyber risk.

DonorPerfect AI-Driven Cyberattack Causes Operational Disruption

DonorPerfect, a fundraising platform serving nonprofit organizations, recently experienced a cyberattack involving adaptive AI-driven bots. After initially identifying what appeared to be multiple isolated issues, the company later determined the activity was part of a singular coordinated attack attributed to an AI agent known as "ZHA," which was actively targeting several DonorPerfect systems.

DonorPerfect began a phased restoration of services on November 14, 2026, with approximately 99% of systems restored by November 16, 2026. While recovery was relatively swift, the outage created operational challenges for nonprofit organizations during the critical year-end fundraising season, limiting access to donor records, reporting tools, and certain online forms. Although some third-party donation platforms remained operational, synchronization with DonorPerfect was delayed until secure connections could be restored.

GoFundMe Pro Data Breach Exposes Donor Information

In a separate incident, GoFundMe recently disclosed a security breach affecting its GoFundMe Pro fundraising platform. According to the company, an unauthorized third party accessed donor and supporter information between October 14, 2026, and October 18, 2026, and again on November 8, 2026.

Potentially impacted information includes names, mailing addresses, email addresses, phone numbers, and, for some individuals, dates of birth and the last four digits of payment card numbers. GoFundMe has stated that it secured the platform, engaged third-party cybersecurity experts, disabled unauthorized accounts, and notified law enforcement.

Why These Incidents Matter

Many nonprofit organizations depend on third-party vendors for services such as fundraising, payment processing, cloud storage, employee benefits administration, and other essential services. As a result, a cyber incident involving a vendor can have significant downstream impacts, including:

- Reputational damage and loss of stakeholder trust.
- Regulatory inquiries and potential notification obligations.
- Increased costs associated with incident response and remediation.

© 2026 Edgewood Partners Insurance Center. All rights reserved. CA License: 0B29370

Even when a nonprofit organization's own systems remain secure, donors, customers, employees, and other stakeholders often associate a breach or outage with the nonprofit organization they entrusted with their information. Importantly, outsourcing data processing does not necessarily transfer liability. Nonprofit organizations may retain statutory and contractual obligations related to breach notification and may face class action litigation, regulatory investigations, and reputational harm resulting from the unauthorized disclosure of their data by a third-party service provider.

Insurance Implications

These incidents also highlight the importance of reviewing insurance risk transfer mechanisms in the context of management liability, security breaches, and technology outages involving third-party service providers.

Nonprofit organizations should work with their brokers and insurers to understand how their policies may respond to:

- Director and Officer liability
- Business interruption losses.
- Contingent business interruption arising from vendor outages.
- Privacy liability claims.
- Regulatory investigations and defense costs.
- Breach response expenses, including forensic investigations and notification costs.
- Crisis management and public relations expenses.
- Data restoration and system recovery costs.
- Losses arising from security failures involving third-party service providers.

Nonprofit organizations should also be mindful of policy reporting requirements and involve their insurance advisors early when assessing potential exposures.

Key Takeaway

The DonorPerfect and GoFundMe Pro incidents demonstrate that cyber risk extends well beyond a nonprofit organization's own network. Whether through an AI-enabled attack that disrupts operations or a data breach affecting a trusted service provider, nonprofit organizations can face significant operational, financial, legal, and reputational consequences.

As threat actors increasingly leverage artificial intelligence to automate and scale attacks, nonprofit organizations should evaluate vendor management practices, incident response preparedness, business continuity planning, and cyber insurance protections to ensure they remain aligned with evolving cyber threats and third-party risk exposures.

Ready to be EPIC***?***

For more information about how EPIC can help your business, visit us at **epicbrokers.com**.

© 2026 Edgewood Partners Insurance Center. All rights reserved. CA License: 0B29370

EPICBROKERS.COM