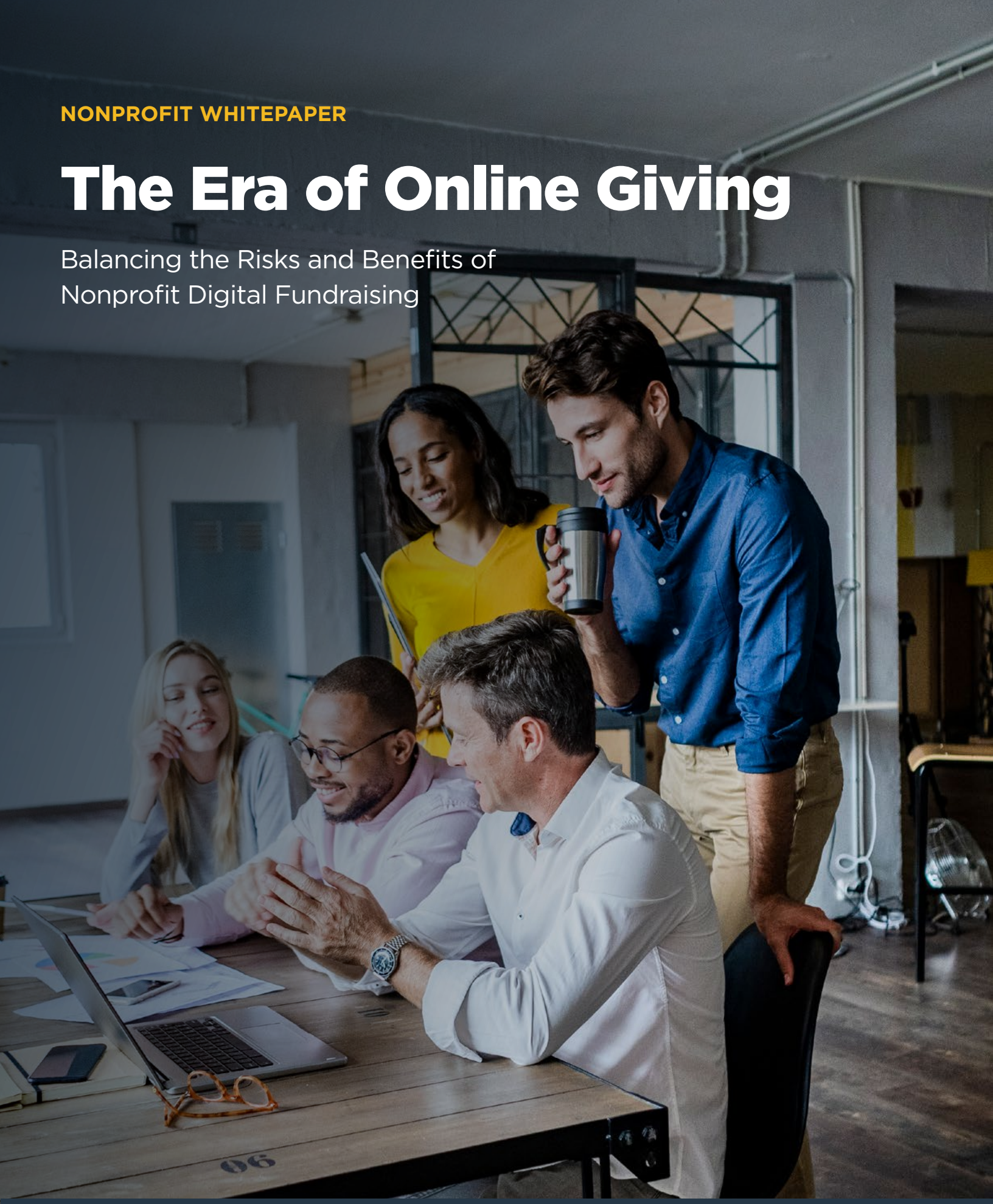
NONPROFIT WHITEPAPER

The Era of Online Giving

Balancing the Risks and Benefits of Nonprofit Digital Fundraising



HUB

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

Online giving is rapidly growing and becoming essential for nonprofit fundraising efforts. Beyond just collecting contributions, organizations are leveraging digital platforms to engage donors and drive support for their causes. This shift has allowed nonprofits to reach more supporters, streamline the giving process and see consistent year-over-year growth in online donations. Online donations have become the preferred method for individual donors — the largest source of giving — with 63% favoring online contributions over traditional methods like direct mail.[1]

As a result, 67% of nonprofits globally now accept online donations.[2] That number will only grow as more nonprofits embrace the digital fundraising trend; however, organizations need to ensure they can provide donors with a safe and efficient experience.

Key Nonprofit Vulnerabilities in Digital Fundraising

Digital fundraising offers many benefits to nonprofit organizations, but it also introduces a variety of risks. These include cybersecurity threats, donor data privacy concerns and legal and financial repercussions related to copyright issues if digital fundraising content is used without proper permissions or licenses.

The impacts of any of these incidents could be devastating to a nonprofit. Aside from the financial cost — averaging nearly $5 million per data breach in 2024[3] — the reputational damage could severely undermine a nonprofit organization's ability to build trust with donors, attract funding and effectively carry out its mission.

Understanding Cyber Risk

One of the biggest risks to nonprofit organizations using digital fundraising methods is a **cyber or data breach**. Nonprofits have become major targets of cybercriminals due to the amount of sensitive donor data they retain and their use of digital channels for processing funds. Additionally, many nonprofits lack the resources to properly protect their technology systems, with 68% reporting they have experienced a data breach in the last three years.[4]

Nonprofits are required by data protection laws, industry regulations and third-party contractual agreements to safeguard any personal data collected, transmitted or stored during transactions. This stored data can leave nonprofits exposed. Even if a nonprofit uses a third-party contractor to process credit card payments and those vendors are responsible for storing the donor information, the nonprofit can still be held liable if personally identifiable information is accessed or stolen.

Nonprofits must carefully evaluate third-party payment vendor security and contracts to ensure they are not taking on undue liability, while also taking steps to properly protect all personally identifiable information that flows through the organization.

Case Study

A nonprofit that specializes in working with at-risk youth reached out to HUB fearing it was under a ransomware attack, exposing vulnerable patient and resident data. HUB immediately put an action plan into place to minimize access to emails and other sensitive information. After bringing in breach counsel and IT forensic investigators, it was determined there was no data stolen during the event.

The client was not only relieved that the impact was minimal and resulted in a total claim under $60,000, but the organization also took the opportunity to train its staff to be better prepared in the future.

[1]DoubletheDonation.com, "Nonprofit Fundraising Statistics to Boost Results in 2025," January 21, 2025.
[2]Nonprofitsource.com, "The Ultimate List Of Charitable Giving Statistics For 2024," accessed January 21, 2025.
[3]IBM, "Escalating Data Breach Disruption Pushes Costs to New Highs," July 30, 2024.
[4]CyberPeaceInstitute.org, "Cyber-poor, target-rich: The crucial role of cybersecurity in nonprofit organizations," March 25, 2024.

Costly Copyright Mistakes

With more nonprofits adopting a digital-first approach to their operations and fundraising activities and younger donors gravitating towards online giving, 91% of nonprofits now have a website and 87% consistently incorporate social media into their digital marketing and fundraising strategies.[5]

While engaging donors through compelling website and social media content is an essential part of digital fundraising, nonprofits must also ensure they are not publishing any copyrighted material or licensed content they do not have proper permission to use. This includes and isn't limited to photographs, music, logos, artwork or any other type of content/information used by other websites or social media platforms.

Copyright infringement penalties can be as high as $150,000 for each work infringed. Nonprofits can also be held liable for attorney fees and court costs related to the infringement claim.[6]

A Cautious Approach to Artificial Intelligence

Nonprofit organizations are increasingly leveraging artificial intelligence (AI) to improve operations and communication with donors. AI can greatly help in improving fundraising efforts. In fact, AI use among nonprofits is outpacing the private sector 58% to 47%.[7] Among nonprofits using AI, 70% believe generative AI will help them achieve their organization's sustainable development goals by enhancing productivity, improving access to information and increasing awareness to drive policy change.[8]

However, nonprofits need to take steps to mitigate **the risks that come with using AI**.

AI-generated materials can also bring legal risk, including claims of personal injury, copyright/trademark infringement and plagiarism, which could lead to costly fines and reputational damage.

From another perspective, nonprofits need to be aware that AI is enabling cybercriminals to carry out more elaborate and sophisticated cybercrime schemes through phishing and ransomware attacks. AI-generated "deepfakes," where AI mimics the voices or faces of real people, are being used to authorize fraudulent wire transfers, spread misinformation, impersonate donors or manipulate employees into divulging sensitive information.

[5]NonprofitTechforGood.com, "2023 Nonprofit Tech for Good Report," February 1, 2023.
[6]Purdue University, University Copyright Office, "Copyright Infringement Penalties," accessed January 27, 2025.
[7]The NonProfit Times, "Nonprofits' Use Of AI Exceeds For-Profit Implementation," September 16, 2024.
[8]McKinsey & Co., "AI for social good: Improving lives and protecting the planet," May 10, 2024.

A Proactive Risk Management Strategy

Given the various risks that come from digital fundraising, having the right insurance and a proven risk management plan is essential to mitigating potential financial and reputational fallout.

Nonprofits can reduce exposure and safeguard their mission and long-term viability by incorporating the following strategies:

- **Be selective about third-party vendors.** Only choose vendors with robust data security controls who understand and are compliant with regulatory requirements regarding the protection of personally sensitive data.
- **Contractually transfer risks that should be covered by outside vendors or relevant parties.** Nonprofits should carefully examine contracts to ensure they are not liable if client data is compromised in a service provider IT breach.
- **Educate and train staff and volunteers.** It's important to provide training for employees to help them identify potential social engineering scams or phishing attempts that could lead to unauthorized access to networks or result in fraudulent activities.
- **Have written policies and procedures in place for staff and donors regarding the transfer of funds.** This should include requiring staff to confirm monetary transfers over a certain amount via a phone call to the requestor.
- **Maintain website and social media protocols.** Nonprofits need to review planned content and media assets to confirm they are properly licensed, as well as regularly monitor online activity to ensure it complies with company policies.

Case Study

An individual posing as a donor attempted to make a $10,000 donation to an organization's fundraising campaign via eCheck through their website. The alleged donor made three separate transactions and then contacted the organization to say the multiple donation attempts were made in error. Because the transactions were made over the weekend, they still showed up as in process and the organization moved ahead in refunding two of the three donations totaling more than $21,000. After the refunds were processed, the original transactions were all rejected by the bank, leaving the organization out $21,000 by the scam. A robust risk management strategy can help organizations evaluate their fund transfer processes and address potential vulnerabilities, so they don't fall prey to fraudulent schemes.

Insurance Coverage Considerations

Standard nonprofit general liability insurance policies may not cover the risks of today's digital landscape. Depending on the scope of their work, nonprofit organizations may want to consider coverages, including:

- **Cyber Insurance:** Covers data breaches, ransom events, extortion events and third-party litigation arising from these types of incidents. Policies can also include coverage for e-crimes, with specific language to protect the nonprofit against social engineering schemes that impact donors.

- **Media Liability Insurance:** Protects against claims related to the use of digital content, such as copyright infringement, unauthorized reproduction or distribution of media. Media and cyber policies may be purchased together or as a standalone option.

- **Commercial Crime Policies:** Covers employee and third-party fraud. It can also include social engineering. It is important that carriers know the insured is a nonprofit organization so donor language can be included.

Key Factors to Consider When Selecting a Broker

A trusted broker offers expertise in insurance products and becomes a valuable partner in navigating complex risks. Nonprofits should look for a broker who can offer customized risk management and product solutions, including crisis response, and provide ongoing advisory services, such as regularly revisiting policies and systems to align with evolving risks. By prioritizing experience, customization and ongoing support, nonprofits can build a resilient foundation to protect their mission, assets and reputation in an ever-changing digital landscape.

To learn more about protecting your nonprofit in this digital world, contact HUB International's nonprofit insurance specialists today.

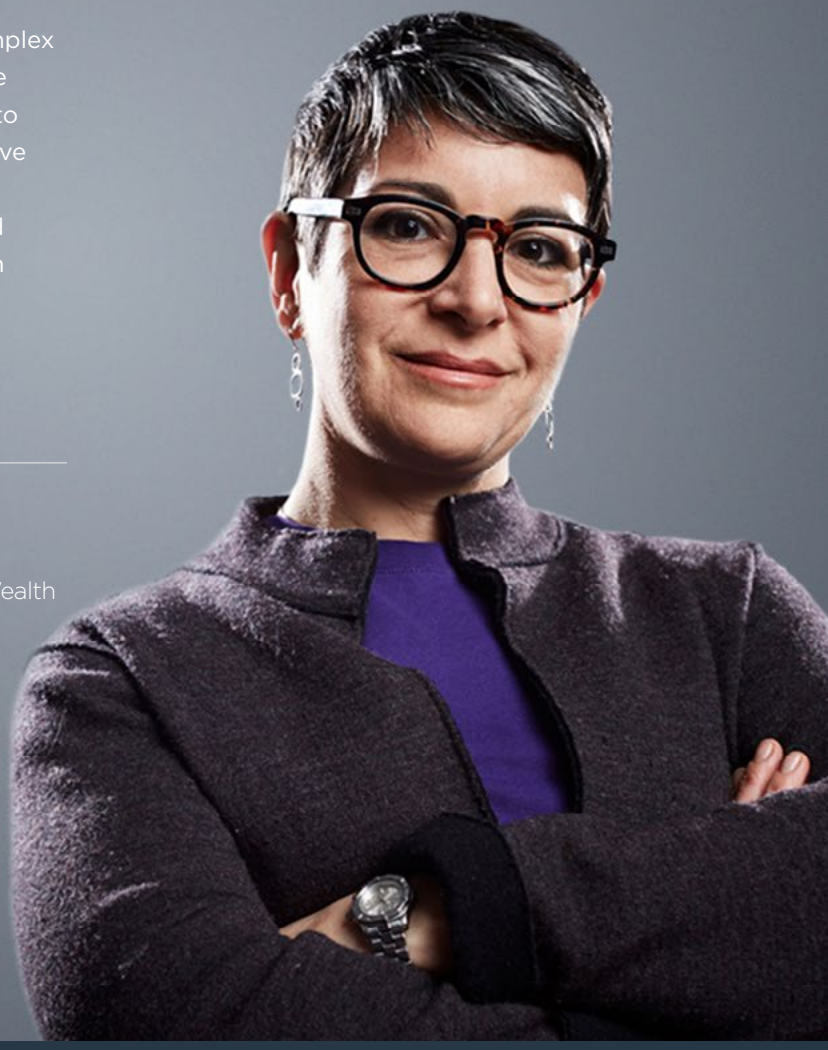
Strategic support that puts you in control.

When you partner with HUB, you're at the center of a vast network of experts who offer creative solutions to the complex challenges you face. We bring a deep understanding of the needs of charitable organizations and a holistic approach to risk, talent and reputation management. With HUB, you have peace of mind knowing that what matters most to you will be protected — through unrelenting advocacy and tailored solutions that support your mission and enable you to plan confidently for the future.

hubinternational.com/nonprofit

Ready for tomorrow.

Risk & Insurance | Employee Benefits | Retirement & Private Wealth



HUB