kyndryl

Managing nonprofit cybersecurity in the AI era

by Kris Lovejoy
Global Head of Strategy

Introduction

The rapid evolution of artificial intelligence (AI) has introduced a profound paradox for nonprofit organizations, a reality reinforced continuously through my discussions with Kyndryl Foundation's global grantees and the developments we see unfolding today. On one hand, generative AI and machine learning tools offer typically lean nonprofit teams new opportunities to scale their missions, improve fundraising, strengthen communications, and streamline administrative workflows. On the other hand, AI has made cybercrime faster, cheaper and more convincing.

Historically, resource-constrained nonprofits often operated under the comforting assumption that they were too small to be targeted, or that basic security instincts — such as spotting a poorly written phishing email — were enough.

Today, AI acts as a major risk multiplier. Bad actors can use advanced tools to craft highly personalized phishing messages, imitate trusted voices, and automate the discovery of software weaknesses much faster than many organizations can respond.

This article is written for anyone who helps lead, govern, advise, fund, volunteer with or support a nonprofit. Whether the organization is a small community-based group, a mid-sized regional nonprofit, or a large international NGO, the same core principle applies: cybersecurity must be treated as mission protection. The scale, staffing, and tools may differ, but every nonprofit needs practical safeguards, clear accountability and a culture of verification.

Why nonprofits are prime targets

The nonprofit sector is actively targeted by cybercriminals for three distinct reasons:

Large collections of donor and beneficiary data: Nonprofits often hold high-value information, including donor records, payment information, corporate philanthropic relationships, volunteer data, and sensitive beneficiary profiles such as health, housing, immigration or financial assistance records.

Limited security capacity: Many nonprofits direct most available funding to programs, not IT infrastructure. Smaller organizations may have no dedicated IT staff, while larger organizations may operate complex systems across multiple geographies, partners and vendors.

A culture of trust: Nonprofits often rely on staff, volunteers, board members, partners and supporters working across many devices and locations. That openness is part of what makes the sector powerful, but it also creates risk if accounts, passwords and data access are not carefully managed.

Ten essential security practices for the AI era

Cybersecurity maturity is a journey. A small nonprofit with no dedicated IT staff will not have the same controls as a global humanitarian organization, but it can still take meaningful steps immediately. The goal is not perfection; it is disciplined progress against the risks most likely to disrupt the mission, expose sensitive data or erode trust.

Regardless of an organization's size, budget, or current technological maturity, nonprofit leaders should embed these foundational practices into daily operations:

1. **Enforce mandatory multi-factor authentication (MFA) while applying strong password hygiene and moving toward passkeys.** MFA remains one of the most effective defenses against identity attacks. It should be required for email, financial systems, donor databases, cloud storage, and other critical accounts used by staff, volunteers and board members. Equally important, require password managers to reduce reuse, prohibit shared accounts where possible, and adopt passkeys when available since they're more resistant to phishing than traditional passwords.

2. **Establish a formal AI governance and data use policy.** Staff and volunteers may use generative AI tools to draft communications, summarize documents or analyze information. Policies should prohibit entering donor, HR, financial, beneficiary, or other sensitive data into unapproved public AI tools; define which tools are approved; require human review of AI outputs; and address vendor AI disclosures.

3. **Keep humans accountable for AI-assisted decisions.** AI tools should not run unsupervised in ways that affect donors, beneficiaries, hiring, grantmaking, service eligibility, code deployment, or public communications. Qualified people should review, validate, and remain accountable for AI-assisted outputs before they affect stakeholders.

4. **Update training for AI-driven social engineering.** Traditional training often focused on broken grammar and obvious suspicious links. AI has made those clues less reliable. Training should help staff, volunteers, and leaders recognize realistic phishing, impersonation, payment diversion, fake invoices, and voice-cloning or urgent-request scams.

5. **Reduce unnecessary data.** Establish data retention and disposal practices so the organization does not keep sensitive information longer than necessary. Reducing stored data reduces harm if a breach occurs.

6. **Apply least privilege.** Limit access to only what people need for their roles. Staff, volunteers, board members, and temporary workers should not have broad access to donor, financial, HR, or beneficiary data unless their work requires it.

7. **Review vendors and supply chain risk.** Nonprofits rely on software providers for donor management, payments, email marketing, case management, payroll, and collaboration. Organizations should understand how vendors protect data, whether AI features are enabled, what data is used for model training, and what contractual protections apply.

8. **Patch quickly and prioritize exposed systems.** Attackers can exploit known software weaknesses rapidly. Enable automatic updates where possible and prioritize internet-facing systems, websites, plugins, email tools, and remote access systems.

9. **Maintain secure, tested backups.** Backups should be separated from day-to-day credentials and tested regularly. A practical approach is the 3-2-1 rule: keep three copies of important data, on two types of storage, with at least one copy offline or otherwise isolated.

10. **Plan for incident response and communications.** Every nonprofit should know who makes decisions during a cyber incident, who contacts technology providers, insurers, counsel, regulators, law enforcement, donors, beneficiaries and the public, and which systems must be restored first to continue mission-critical work.

What this looks like by organization size

Small nonprofits: Focus first on MFA, password managers, secure backups, basic phishing training, limited access to donor and beneficiary data, and simple written policies for data and AI use. If there is no IT staff, assign a responsible owner and use credible free or discounted resources to get started.

Mid-sized nonprofits: Add vendor reviews, incident response planning, cyber insurance review, periodic security assessments, staff and volunteer training, and clearer executive ownership for cybersecurity risk.

Large nonprofits and international NGOs: Implement board-level cyber reporting, security monitoring, tabletop exercises, formal third-party risk management, AI governance, data classification, privacy coordination, and dedicated cyber resilience programs across regions and subsidiaries.

Questions leaders and boards should ask

- Who owns cybersecurity risk at the management level?
- Do we require MFA for staff, volunteers, board members and key vendors?
- What sensitive data do we collect, where is it stored, and how long do we keep it?
- Do we have an incident response plan, and have we tested it?
- Are vendors contractually required to protect our data and disclose security incidents?
- What cyber risks could interrupt fundraising, service delivery, payroll, grantmaking or communications?
- Do funders and partners support the infrastructure needed to protect the mission?

The role of funders, advisors, volunteers and supporters

Cybersecurity is not only an internal operations issue. Funders can include cybersecurity and secure technology in grants rather than treating them as overhead to be minimized. Advisors can help organizations ask better questions about risk, vendor contracts, insurance and privacy. Volunteers can follow security policies, use approved tools, and avoid sharing accounts. Supporters can recognize that resilient infrastructure protects the people and causes they care about.

Free and discounted resources to prepare and protect your organization

Nonprofits can draw on a growing set of free and discounted cybersecurity resources rather than building everything alone.

On the technology side, programs such as TechSoup, Microsoft for Nonprofits, and Google for Nonprofits provide donated or subsidized software and cloud services. For operational guidance, toolkits from the Global Cyber Alliance, CISA's "Secure Our World" initiative, and the Ford Foundation's cybersecurity assessment give structured ways to evaluate risk and implement basic controls. And for situational awareness and crisis support, networks such as NGO-ISAC, NetHope, and Access Now's Digital Security Helpline offer sector-specific threat intelligence and hands-on help during incidents. Because availability and eligibility differ by country, mission, and organizational size, leaders should treat these as examples and confirm the latest program details before acting.

Kyndryl Foundation: Best for organizations aligned with cybersecurity and AI education and skilling, and workforce development and resiliency. Grantmaking is available for eligible U.S. 501(c)(3) and equivalent organizations globally, subject to foundation priorities and program requirements.

Conclusion

AI has changed the economics of cyber risk, but it has not changed the fundamentals of responsible nonprofit leadership. Every nonprofit—large or small, local or global—depends on trust. Protecting that trust requires practical controls, clear ownership, informed board oversight where applicable, and support from funders, advisors, volunteers, staff and partners.

Cybersecurity should not be viewed as a luxury, a purely technical matter, or a distraction from mission. It is part of how the mission is protected. At the next leadership or board discussion, every nonprofit can take immediate steps to identify its most sensitive data, confirm MFA coverage, assign ownership for cyber risk, review one credible resource from this list, and choose one practical improvement to prioritize.

kyndryl