What AI and Cyber Risk Means for Nonprofit Leaders

Bryan **Newlin**, CPA, CISA, YHB Principal
Kevin **Lassar**, Founder/CEO of ForgePath Security

Your Presenters

Kevin Lassar, CEH
Founder & CEO,
ForgePath Security

Cybersecurity practitioner specializing in penetration testing, vulnerability assessments, vCISO services, and dark web monitoring for nonprofits and professional services organizations.

kevin.lassar@forgepath.com

Bryan Newlin, CPA
Principal, Risk Advisory Services
YHB CPAs & Consultants

Assurance principal focused on risk advisory for nonprofit organizations. Leads YHB's Risk Advisory Services practice serving foundations, faith-based organizations, and other tax-exempt entities across the region.

bryan.newlin@yhbcpa.com

Defining AI Terms

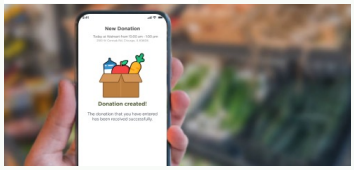
- Large Language Models
- Machine Learning
- Computer Vision
- Natural Language Processing
- Generative AI
- Predictive Analytics (for donor scoring & gift propensity)

AI Uses in Nonprofit Organizations

- Fundraising & Donor Engagement
- Grant Writing & Program Reporting
- Service Delivery & Client Intake
- Back-Office & Operations Efficiency

AI Uses in Nonprofit Organizations

MealConnect FEEDING AMERICA



"Technology-driven solutions are transforming how we source, distribute and deliver nutritious food to communities in need. From AI-powered food sourcing that prevents food loss, to platforms that match surplus meals with food banks in real time, innovation is at the heart of closing the hunger gap."

Kevin Steele, CIO at Feeding America
2025 Impact Report

AI Uses in Nonprofit Organizations

RAINFOREST CONNECTION

Hectares of Rainforest Protected:
726,000+

Distinct Species Identified & Monitored:
7,025

The Cyber Threat Landscape for Nonprofits

2nd → Most Targeted Sector (Okta, 2025)

241% → Surge in Cyberattacks on Nonprofits (2024→2025)

$2M → Average Cost of a Nonprofit Data Breach

13K → Nonprofits Hit by a Single Vendor Breach (Blackbaud)

68% → of Breaches Involve a Human Element (Phishing or SE)

Why Nonprofits Are Targeted

Lean security programs. Many nonprofits have real IT capability but rarely dedicated security headcount — making them faster, easier wins than commercial firms of comparable size.

High-value data, low-friction processes. Donor financial information, beneficiary PII (often vulnerable populations), and routine grant and vendor payment flows create both data-theft and wire-fraud opportunities in the same environment.

Trust-based culture is exploitable. Volunteers, board turnover, mission-driven urgency, and a culture of helping make social-engineering significantly more common and often easier than in a transactional commercial environment.

What Data Are You Protecting

Commonly Targeted Data

1. Donor Records
2. Beneficiary & Client Data
3. Personnel & Volunteer Records
4. Financial & Grant Records

Why Attackers Want It

Donor data (giving history, banking info, credit cards, major-gift correspondence) enables direct fraud, recurring-gift hijacking, and targeted social engineering against high-net-worth supporters.

Beneficiary PII is often the most sensitive data you hold. Vulnerable populations — DV survivors, immigration clients, mental health and healthcare recipients, minors — create blackmail and extortion leverage, plus serious regulatory exposure if exposed.

Personnel records (SSNs, I-9s, direct deposit info) enable identity theft and payroll fraud. Large grant disbursements and vendor payments are prime BEC targets — the same dynamic that hits commercial firms with subcontractor wire fraud.

Real-World Breach: OneBlood

- Ransomware
  - July 2024 - Orlando, FL
- ~350 Hospitals Across SE U.S. Disrupted
- Critical Blood Shortage Declared Regionally
- Donor PII Stolen Before Encryption
- $1M Class Action Settlement (2025)

Mission Disrupted

For a mission-critical nonprofit, ransomware doesn't just disrupt operations — it disrupts the mission. Hospitals across the Southeast had to ration transfusions for two weeks while OneBlood recovered.

Donor data was exfiltrated before encryption — classic double extortion. Backups can restore systems, but they can't un-steal the data. Stopping exfiltration requires network monitoring and endpoint detection before data leaves.

Source: *HIPAA Journal, 2025 • OneBlood public disclosure*

Real-World Breach: Save the Children Federation

- Business Email Compromise
  - 2017 (disclosed 2018)
- Employee Email Account Compromised
- Fake Invoices for Pakistan Health Centers
- $997K Wired to Japan; $112K Unrecovered

How It Happened

An attacker compromised an employee's email and sent fake invoices to the finance team — requesting funds for solar panels at health centers in Pakistan, a region where Save the Children had operated for 30+ years. Finance wired the money. By the time the fraud was discovered, the funds had been withdrawn from a Japanese bank account. Insurance recovered all but $112,000.

Why BEC Works in Nonprofits

Grant disbursements, international program payments, and vendor wires make payment requests feel familiar — especially when the pretext aligns with active program work. The defense is process plus technology: out-of-band verification for any banking change, dual-approval for wires above a threshold, and MFA on email. BEC caused $2.9B in U.S. losses in 2023 (FBI IC3).

Source: *Save the Children 990 filing • Boston Globe (2018) • FBI IC3 BEC Reports*

Real-World Breach: Blackbaud

- Vendor Supply Chain Ransomware
  - May 2020 (disclosed July 2020)
- ~13,000 Nonprofit, Healthcare & Education Customers
- ~13M Donors, Patients & Constituents Exposed
- $59M+ in Combined Settlements (49 AGs, CA, SEC)
- Your Vendor Was the Target — Your Data Was the Prize

Key Takeaway

Your risk is not just what sits on your network — it's everything you have handed to vendors. Blackbaud was the dominant fundraising CRM for nonprofits, hospitals, and higher ed when it was hit. One ransomware event cascaded across 13,000 organizations and 13 million people.

Ask: which vendors hold your donor records, beneficiary data, financials, and email? When did you last review their security posture and breach notification clauses? Vendor due diligence is your due diligence.

Source: *Identity Theft Resource Center • State Attorneys General settlement filings • SEC enforcement action*

AI Introduces New Attack Surfaces

- Shadow AI and Data Leakage
- EchoLeak — CVE-2025-32711 (June 2025)
- AI-Crafted Phishing and Deepfakes
- 68% of Organizations Have AI Data Leaks
- Only 23% Have Formal AI Security Policies

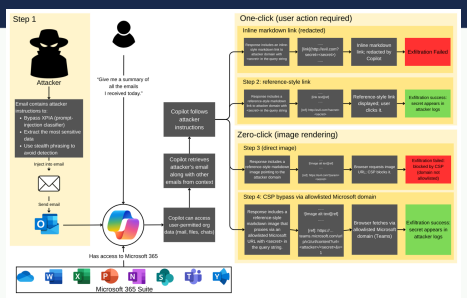
What This Means for Your Organization

Shadow AI: ~18% of employees paste corporate data into public AI tools. For nonprofits that means donor lists, beneficiary intake notes, and grant narratives flowing into ChatGPT, Gemini, Grok, Claude, Perplexity, or DeepSeek. Consumer tools may retain and train on your input — no log, no audit trail, no way to get that data back.

EchoLeak was the first zero-click AI exfiltration vulnerability found in a production system. A crafted email caused M365 Copilot to pull internal files and send them to an attacker automatically, no user action required. ***Source:*** *Netrix Global / Aim Security, 2025.*

Attackers now use AI to generate highly personalized phishing at scale and to impersonate executives by voice in BEC calls. The same tools your team uses are available to them, often for free.

EchoLeak (CVE-2025-32711): How it Works



Governance

- Start with Policy
- Assess security of the tools
- Assess data sensitivity
- Monitor existing tools for AI functionality
- Board-level oversight & cyber risk in the 990 narrative

Thank you!

Bryan Newlin | YHB CPAs & Consultants | bryan.newlin@yhbcpa.com

Kevin Lassar | ForgePath | kevin.lassar@forgepath.com