



2026 SECTOR BRIEFING · NONPROFIT CYBERSECURITY

Navigating the New Threat Landscape

Nonprofit Cyber Trends and How to Respond

Prepared for mission-driven organizations navigating rising cyber risk

Agenda

A grounded look at where nonprofits stand today — and a practical path forward.



Who's a Target, and Why

The structural reasons the sector has become a favored target — and which subsectors carry the most exposure.



The Threats Defining This Moment

Email compromise, ransomware, identity sprawl, vendor risk, legacy tech, and AI-enabled scams.



Where the Sector Can Improve

Thin budgets, underreporting, coverage gaps, and the real cost of getting this wrong.



A Practical Response Plan

A framework, five quick-win spotlights, and a two-phase 90-day roadmap to build lasting maturity.



4

Key Areas to Strengthen Your
Defenses

The Scale of the Problem

Nonprofits are no longer a secondary target — they are squarely in attackers' sights.

85%

of surveyed nonprofits have
experienced
at least one cyberattack

CyberCAN / UC Berkeley CLTC

+35%

year-over-year growth in advanced
email attacks on nonprofits

Abnormal AI, 2025

#2

most-targeted industry in one major
IAM vendor's customer base

Okta, Nonprofits At Work 2025

The Scale of the Problem, Continued

Closer to home: ground-level data from US nonprofits shows the same pattern, in sharper detail.

53%

of nonprofits have no full-time
IT staff of any kind

CyberCAN / UC Berkeley CLTC, survey of Bay Area nonprofits

16%

of nonprofits use no multi-factor
authentication on any system

CyberCAN / UC Berkeley CLTC

500+

suspected account-compromise
incidents
flagged in one year across just ~200
US nonprofit organizations

*Community IT Innovators, 2025 Nonprofit Cybersecurity
Incident Report*

Why Nonprofits Are in the Crosshairs



Sensitive Data at Scale

Donor financials, Social Security numbers, and beneficiary health or identity records — often with light protection.



Resource-Constrained IT

Thin budgets and few (or zero) dedicated security staff, competing against mission-critical program spending.



A High-Trust Culture

Open, helpful communication norms make staff more susceptible to impersonation and social engineering.



Complex Access Needs

Staff, volunteers, part-timers, and board members each need different, frequently-changing levels of access.

Who's Most at Risk Within the Sector

Exposure varies by mission area — but no subsector is exempt.



Human & Social Services

Shelters, food banks, and case-management agencies hold sensitive beneficiary data while running on the sector's thinnest IT budgets.



Healthcare-Adjacent Nonprofits

Organizations handling clinical or health data carry HIPAA-adjacent obligations, and that data commands a premium on the dark web.



Foundations & Grantmakers

Large, recurring wire transfers and high-net-worth donor data make finance teams a favorite target for BEC schemes.



International & Humanitarian NGOs

Cross-border data on refugees and missing persons raises the stakes, drawing interest from sophisticated, sometimes state-linked, actors.

The Budget Reality

Security competes with mission delivery for every dollar.

~5%

of the average nonprofit's operating budget goes to technology overall—
not cybersecurity specifically

NTEN, Nonprofit Technology Staffing & Investments Report

**13.2%
→ 1.5%**

small nonprofits spend a far higher share of budget on tech than large ones — but far fewer absolute dollars

NTEN benchmark

No Line Item

cybersecurity is rarely budgeted or tracked on its own — it's folded into a general “IT” bucket, if funded at all

Sector-wide observation

Business & Vendor Email Compromise

- Attackers impersonate donors, board members, or vendors to redirect payments or harvest credentials.
- Common lures include fake invoices, urgent wire-transfer requests, and gift-card scams targeting staff.
- Finance and development teams are prime targets given their access to payment systems and donor data.



+50%

year-over-year increase in phishing attacks
aimed at nonprofit organizations

Abnormal AI, 2025

Ransomware & Operational Disruption

- Encrypted case-management, donor, and program data can halt service delivery to the people who rely on it.
- Recovery costs and downtime can rival or exceed a nonprofit's entire annual IT budget.
- Underfunded backup and recovery plans leave many organizations choosing between paying or losing data for good.



1 in 3

organizations rank ransomware among the threats they feel least prepared for

Industry benchmarking, 2026

Identity & Access Sprawl

- Full-time staff, part-timers, volunteers, and board members each need different — and frequently changing — access.
- Inconsistent onboarding and offboarding leaves “ghost” accounts active long after people leave.
- Shared logins and reused passwords are common workarounds under time and budget pressure.



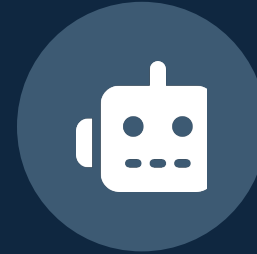
MFA

single-factor logins remain the most exploited weakness across nonprofit systems

Sector security assessments, 2026

AI-Enabled Social Engineering

- Generative AI lets attackers write more convincing, personalized phishing and impersonation content at scale.
- Deepfake audio and video are emerging in executive-impersonation scams requesting urgent wire transfers.
- Traditional “spot the bad grammar” training no longer catches these more polished attacks.



AI

is now cited as a driver of more
sophisticated, harder-to-detect social
engineering

Fortinet 2026 Threat Predictions

Third-Party & Vendor Risk

- Nonprofits often rely on shared SaaS platforms for donor management, payment processing, and case tracking — a single vendor breach can expose many organizations at once.
- Attackers increasingly target the vendor rather than the nonprofit directly, since one successful compromise yields dozens of downstream victims.
- Vendor contracts rarely specify security requirements or audit rights, leaving nonprofits with little visibility into a partner's actual practices.



30%

of all breaches now involve a third party —
double the share reported just a year earlier

Verizon 2025 Data Breach Investigations Report

Legacy Systems & Unpatched Software

- Donor databases, case-management tools, and financial systems often run on unsupported software that no longer receives security patches.
- Attackers rarely need a novel exploit — known, unpatched vulnerabilities remain one of the most common ways in.
- Modernization competes directly with program funding, so aging infrastructure often stays in place long after it should be retired.



99%

of exploited vulnerabilities were already known to IT teams for at least a year before the breach occurred

Gartner, widely cited industry analysis

We Don't Even Know the Full Scope

Unlike healthcare or finance, nonprofits face no consistent breach-reporting requirements — so the true scale of the problem is likely undercounted.



Incidents often surface only as “collateral damage” in third-party or vendor breaches, not as direct nonprofit incidents.



Underreporting weakens the sector's ability to build a case for funding and dedicated cybersecurity resources.



Waiting for perfect data isn't an option — the sector needs support based on what is already known.

The Cost of Inaction

A cyber incident doesn't just cost money — it costs mission capacity.



Program Disruption

Downtime in case-management or donor systems can pause service delivery to the people who need it most.



Donor & Community Trust

A public breach undermines the trust that giving and volunteering depend on — trust that can take years to rebuild.



Financial Strain

Recovery, legal, and notification costs can consume a year's IT budget, with no guarantee of full recovery.



Compliance & Legal Exposure

State breach-notification laws, PCI-DSS, and grant-specific requirements can all apply, regardless of organization size.

The Common Thread

Six different trends. One repeatable pattern.



= Attackers Get In, Stay In, and Cash Out

The good news: closing a small number of foundational gaps disrupts most of these attack paths at once.

A Practical Response Framework

Four pillars, sized for nonprofit budgets and staffing realities.



People

- Role-based security awareness training
- Regular phishing simulations
- Clear reporting path for suspicious activity



Process

- Formal onboarding / offboarding checklist
- Written incident response plan
- Periodic least-privilege access reviews



Technology

- Multi-factor authentication everywhere
- Encrypted, regularly-tested backups
- Email authentication: DMARC, SPF, DKIM



Partnerships

- Nonprofit-focused IT / security vendors
- Peer information-sharing networks
- Grant-funded third-party security assessments

QUICK WIN SPOTLIGHT

Turn On MFA and Email Authentication

- Multi-factor authentication (MFA) stops the vast majority of automated account-takeover attempts, even when a password has been stolen.
- Email authentication (DMARC, SPF, DKIM) makes it far harder for attackers to spoof your own domain in a scam.
- Both are built into Microsoft 365 and Google Workspace at no extra cost — this is a configuration change, not a purchase.



99.9%

of automated account-compromise attacks are blocked by enabling MFA, even with a stolen password

Microsoft Identity Security, widely cited industry benchmark

QUICK WIN SPOTLIGHT

Write (and Rehearse) an Incident Response Plan

- A one-page plan naming who does what — who calls the bank, who notifies leadership, who talks to press or donors — cuts response time dramatically.
- Tabletop exercises (a 60-minute walkthrough of a mock incident) surface gaps before a real attack does.
- You don't need a security team to have a plan — a documented, rehearsed process is what actually reduces damage.



\$1.5M

average breach-cost savings for organizations
with a tested incident response plan versus
none

IBM Cost of a Data Breach Report

QUICK WIN SPOTLIGHT

Test Your Backups Before You Need Them

- A backup you haven't restored from is a hope, not a plan — many organizations only discover a broken backup mid-crisis.
- Schedule a quarterly restoration drill: pick a real file or system and actually bring it back from backup.
- Keep at least one backup copy offline or immutable, since ransomware actively hunts for and encrypts connected backups first.



38%

of organizations that paid a higher ransom said
it was because their backups had failed or were
compromised

Sophos, The State of Ransomware 2025

QUICK WIN SPOTLIGHT

Revoke Access the Day Someone Leaves

- Departing staff, volunteers, and contractors routinely keep access to email, donor systems, and shared drives long after their last day.
- A simple offboarding checklist — disable login, revoke app tokens, reclaim devices — closes this gap in minutes, not months.
- Treat every offboarding the same way regardless of how the departure happened, since access sprawl is the direct fuel for the identity-sprawl trend covered earlier.



89%

of former employees in one workforce study could still access at least one account from a previous employer

Study cited in Beyond Identity / Security Boulevard workforce access research

QUICK WIN SPOTLIGHT

Vet Vendors Before You Trust Them

- Every SaaS platform, payment processor, or contractor with access to donor or client data is a door into your organization.
- A short vendor security questionnaire — how is data encrypted, who can access it, is MFA required — takes an hour and closes most blind spots.
- Put minimum security expectations in the contract itself, so vendor security isn't just a one-time conversation at signup.



64%

of organizations don't evaluate a vendor's security and privacy practices before sharing sensitive data with them

RiskRecon / Ponemon Institute, Data Risk in the Third-Party Ecosystem

A 90-Day Action Plan

You don't need a large budget to make meaningful progress fast.



DAYS 1–30

Foundational

- Enable MFA on email & financial systems
- Inventory who has access to what, and from which devices
- Run a baseline phishing simulation



DAYS 31–60

Harden

- Deploy DMARC, SPF, and DKIM
- Formalize an offboarding checklist
- Test backup restoration end-to-end



DAYS 61–90

Sustain

- Launch ongoing awareness training
- Write & rehearse an incident response plan
- Schedule an outside security assessment

An Advanced 90-Day Roadmap

For organizations that have already covered the foundational basics.



DAYS 1–30

Strengthen

- Move privileged accounts to phishing-resistant MFA (security keys / passkeys)
- Implement device and app management across all devices
- Complete a security review of your top 5 data-sharing vendors



DAYS 31–60

Formalize

- Adopt a written data retention & minimization policy
- Run a tabletop exercise simulating a ransomware incident with leadership
- Segment financial and donor systems from general network traffic



DAYS 61–90

Mature

- Complete a NIST CSF or CISA Cyber Essentials self-assessment
- Establish a standing cybersecurity committee with board-level reporting
- Join a peer information-sharing network for threat intelligence



Key Takeaways

1

Nonprofits are now a top-tier target — this is the norm, not the exception, in the US and internationally.

2

Most successful attacks exploit the same few gaps: weak identity, high trust, and low visibility into vendors and aging systems.

3

MFA, tested backups, fast offboarding, and vendor vetting cover most of what attackers actually rely on.

4

A foundational 90 days plus a follow-on advanced roadmap turns a one-time fix into lasting maturity.



Security Is a Mission Investment, Not a Luxury

Cyber resilience protects the people you serve — donors, beneficiaries, staff, and the community trust your mission depends on.



Questions & Discussion

- Of the Five Quick Wins (MFA, an incident response plan, tested backups, fast offboarding, vendor vetting), which is your organization furthest along on — and which is most exposed?
- What would it take to get MFA turned on every platform and system within 30 days?
- Of the Advanced Roadmap items, which feels furthest out of reach right now, and why?
- A year from now, what would "meaningfully more secure" look like for your organization?



Questions

ASK ME ANYTHING

(Cybersecurity Related)

Thank You!

Francis Johnson
Tech Impact
Chief Technology Officer
francis@techimpact.org