2026 Edition | Enterprise Risk & Compliance Series
For Executive Directors · Board Members · CFOs · IT Directors · Development Directors · Program Leaders

MALA TECHNOLOGY ADVISORS

IT OPERATIONAL RISK
IN THE NON-PROFIT SECTOR

A Practical Guide for Leaders Who Protect Mission, Donors, and the People You Serve

What's Inside: Ransomware Defense · BEC & Wire Fraud Prevention · Beneficiary Data Protection
Donor Privacy · Grant Compliance · Board Governance · Volunteer Risk · KRI Dashboard

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Non-profit organizations face a cybersecurity paradox: they hold sensitive data on donors, beneficiaries, volunteers, and employees — yet they operate with some of the smallest IT budgets and thinnest security teams of any sector. Attackers know this. Non-profits are targeted precisely because they combine valuable data with minimal defenses.

This guide provides a practical, mission-grounded framework for non-profit leaders to understand, prioritize, and address IT risk — without requiring a large budget or a dedicated security team.

60%+
Non-profits Hit by a Cyber Incident

$130K
Avg. BEC Loss per Non-profit

43%
Have No Formal Security Policy

1.5M
Registered US Non-profits

FOR THE EXECUTIVE DIRECTOR & BOARD

Cyber incidents are the #1 operational threat to non-profit continuity. A successful ransomware attack or data breach does not just cost money — it can halt program delivery for weeks, trigger regulatory penalties, erode donor confidence, and jeopardize grant funding. This guide gives you the language and framework to govern IT risk as a board-level obligation.

FOR THE IT DIRECTOR & OPERATIONS TEAM

You likely wear many hats, manage limited resources, and support a workforce of staff, volunteers, and contractors across multiple sites. This guide gives you a risk-ranked action plan, practical controls, and the language to translate technical risk into terms that get board approval and funding.

THE FIVE THINGS EVERY NON-PROFIT LEADER MUST KNOW

1

BUSINESS EMAIL COMPROMISE (BEC) IS THE #1 FINANCIAL THREAT TO NON-PROFITS.

Fraudsters impersonate executives, board members, and vendors to redirect wire transfers and donor funds. The average BEC loss for a non-profit exceeds $130,000 — and most cyber insurance policies have low limits for this crime. Dual-approval wire controls and callback verification prevent nearly all BEC attacks.

2

RANSOMWARE CAN SHUT DOWN YOUR PROGRAMS, NOT JUST YOUR SERVERS.

Non-profits have been forced to halt case management, suspend shelter intake, cancel fundraising events, and miss grant reporting deadlines after ransomware attacks. Three controls prevent the vast majority of successful attacks: MFA, immutable backups, and network segmentation.

3

YOUR BENEFICIARIES AND DONORS HAVE TRUSTED YOU WITH SENSITIVE DATA.

Beneficiary records — especially for health, social services, immigration, and legal aid non-profits — include some of the most sensitive personal data in existence: medical histories, immigration status, legal records, mental health data, and financial need assessments. A breach of this data causes real harm to real people who came to you for help.

4

GRANT FUNDERS AND REGULATORS INCREASINGLY REQUIRE CYBERSECURITY STANDARDS

Federal grants (HHS, DOJ, HUD) are incorporating cybersecurity requirements. State regulators are expanding breach notification obligations. Foundations are adding data security questions to grant applications. Non-compliance risks grant termination, audit findings, and reputational damage with funders.

5

YOU DON'T NEED A LARGE BUDGET. YOU NEED THE RIGHT PRIORITIES5

Microsoft, Google, Cisco, and TechSoup offer deeply discounted or free security tools for eligible non-profits. CISA provides free assessments, training, and incident response assistance. A small investment in the right foundational controls — MFA, backups, training — eliminates the majority of your risk.

SECTION 01

UNDERSTANDING NON-PROFIT IT RISK

Non-profit technology risk is different from private-sector risk — and different from government risk. Understanding why is essential before investing a single dollar in security improvements.

WHY NON-PROFITS ARE DIFFERENT

You Can't Pause Your Mission

When a for-profit company is attacked, it can close temporarily and redirect resources. When a domestic violence shelter, food bank, or crisis hotline is attacked, vulnerable people lose access to services they depend on. Mission continuity is non-negotiable.

Your Data Is Deeply Personal

Non-profits serving health, legal, social services, immigration, and housing clients hold data that can cause severe harm if exposed: medical records, immigration status, domestic violence history, mental health diagnoses, financial need assessments. This data was shared in trust.

Budgets Compete with Programs

Every dollar spent on cybersecurity is a dollar not spent on program delivery. Boards and funders scrutinize overhead. This structural constraint makes non-profits chronically under-invested in IT security — and attackers know it.

BY THE NUMBERS:

Non-profit Cyber Risk

60%+
of non-profits have experienced a cyber incident (Nonprofit Risk Management Center)

43%
of non-profits have no formal cybersecurity policy

Less than 30%
of non-profits have a dedicated IT security resource

$130,000+
average BEC loss per non-profit incident, which is often not fully covered by cyber insurance

20-30%
of donor retention drops following a publicized data breach

THE UNIQUE RISK DIMENSIONS

The Volunteer and Contractor Workforce

Most non-profits have a workforce that extends well beyond paid staff. Volunteers, contractors, interns, board members, and partner-organization staff all access your systems — often on personal devices, from home networks, and with minimal security training. Every additional user is a potential phishing target and every personal device is an unmanaged endpoint.

Donor Trust as Organizational Currency

Donations depend on trust. A data breach exposing donor payment information, giving history, or personal details can cause immediate and lasting damage to fundraising capacity. In a sector where relationships and reputation are the foundation of sustainability, the reputational cost of a breach often exceeds the direct financial cost.

Grant Compliance Obligations

Federal and state government grants increasingly carry cybersecurity requirements — particularly grants from HHS, DOJ, HUD, and the Department of Education. Some funders now require data security plans as part of the application process. Grant non-compliance resulting from a cyber incident can trigger clawback provisions and funding termination.

The Legacy Technology Reality

Many non-profits run on aging donor management systems, legacy CRMs, outdated case management software, and a patchwork of free or low-cost tools. These systems often lack modern security features like MFA, encryption, or API-based integration. Your IT team must build security strategies that work with these constraints, not require their elimination.

↓

THE BOTTOM LINE

Non-profit IT risk is not just about money or data. It's about protecting the people who depend on your services, safeguarding the trust of every donor and beneficiary, and maintaining the operational capacity to fulfill your mission.

Everything in this guide flows from these realities.

SECTION 02

WHO IS ATTACKING NON-PROFITS — AND HOW

Non-profits are not overlooked by attackers — they are deliberately targeted. Understanding who is attacking, what they want, and how they get in is the first step to effective defense.

THE THREAT ACTORS

Impact Level: Critical · High · Medium

WHO	WHAT THEY WANT	HOW THEY ATTACK	IMPACT LEVEL
Ransomware Groups	Program disruption ransom; donor/ beneficiary data extortion	Phishing, unpatched remote access, compromised MSP	Critical — halts programs and operations
BEC / Financial Fraudsters	Wire transfer diversion; grant payment redirection; payroll fraud	Executive impersonation, vendor impersonation, email account takeover	Critical — direct financial loss, often unrecoverable
Cybercriminals	Donor credit card data; beneficiary PII for identity fraud; donor database for fraud	Database exploits, credential stuffing, payment skimming	High — breach notification, regulatory exposure
Insiders (Staff, Volunteers)	Personal gain; curiosity; revenge; inadvertent disclosure	Unauthorized database access; emailing data to personal accounts; misconfiguration	High — especially beneficiary data
Hacktivists	Reputational damage; political statement	DDoS, website defacement, data leaks	Medium — reputational

THE FOUR NIGHTMARE SCENARIOS

1. Ransomware Shuts Down Program Delivery

This is the most operationally devastating scenario. The attacker gets in through a phishing email or an unpatched remote access system, spends days mapping the network, then encrypts everything simultaneously: case management systems, client records, grant management software, email, and financial systems. The organization cannot serve clients, file grant reports, process donations, or communicate for weeks.

Real-World Impact: National Solidarity Fund (2021)
A ransomware attack forced a major social services non-profit offline for three weeks. Case workers could not access client records. Benefits payments were delayed. Grant reporting deadlines were missed, triggering a formal audit. Recovery cost exceeded $2M — with only $500K covered by cyber insurance. The executive director spent the following six months explaining the incident to funders, the board, and state regulators.

BEC Is the #1 Financial Threat to Non-profits: The non-profit sector loses hundreds of millions of dollars annually to BEC fraud. Attackers specifically target the sector because of:

- Lean finance teams without strong dual-control procedures
- Board member and executive impersonation opportunities ('reply to my personal email')
- High-value grant payment cycles and year-end giving campaigns
- Low security awareness among finance and development staff

→ A $25,000 investment in dual-approval controls and wire verification procedures can prevent $130,000+ losses.

2. Business Email Compromise Diverts Funds

A fraudster compromises or spoofs an executive director's email account and sends instructions to finance staff to wire funds to a "new vendor" or redirect a grant payment. Alternatively, they impersonate a board member approving an emergency expenditure. By the time the fraud is discovered, the money is gone. Wire transfers are irreversible. Most non-profits do not discover BEC incidents until days after the transfer.

3. Beneficiary or Donor Data Is Breached

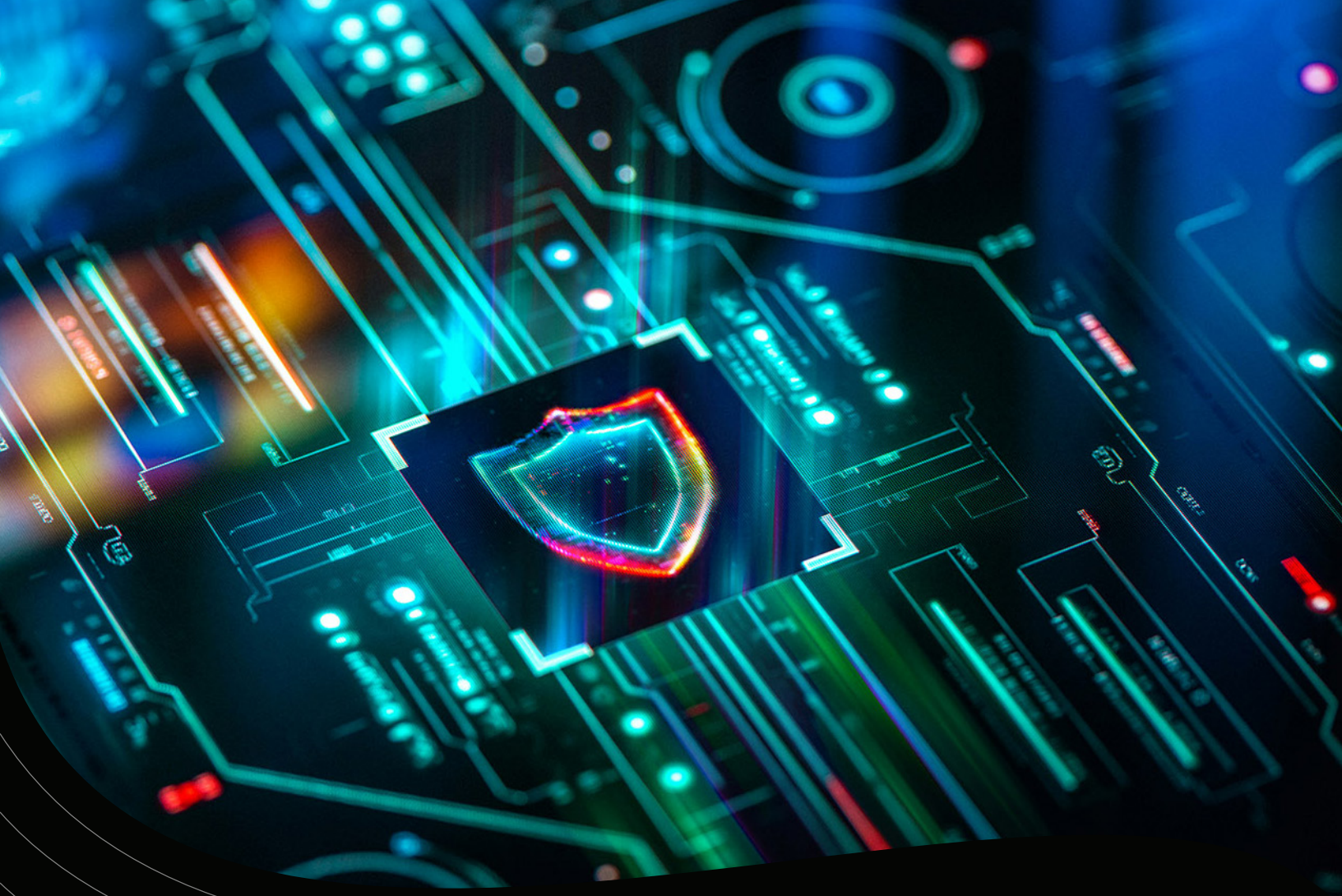
A database containing donor records, beneficiary case files, or client health information is exfiltrated by an attacker or accidentally exposed through misconfiguration. The organization must notify affected individuals, potentially notify state regulators, face class-action litigation, and manage the reputational fallout with donors and funders. For non-profits serving vulnerable populations, the human cost of exposed data — domestic violence survivors, undocumented individuals, mental health clients — can be severe.

4. Grant Funds Are Misdirected or Audit Findings Issued

An insider with financial system access misdirects grant funds, or a ransomware attack compromises the organization's ability to demonstrate proper use of restricted funds. A federal grant audit finds inadequate internal controls over IT systems. The result: grant termination, repayment demands, and exclusion from future funding cycles.

↓ THE BOTTOM LINE

Ransomware and BEC are the two dominant, near-certain threats. Phishing is how attackers gain initial access for both. If you only do two things: deploy MFA everywhere and implement dual-approval wire transfer controls. These two controls eliminate the vast majority of your financial and operational cyber risk.



SECTION 03

ASSESSING YOUR RISK

Before prioritizing investments, you need a clear picture of what you're protecting and what's most likely to go wrong. This chapter gives you practical tools to build that picture quickly.

YOUR TOP 10 IT RISKS — RANKED

Based on incident data from the non-profit sector, here are the risks that matter most:

Impact Level: Critical · High · Medium

RISK	LIKELIHOOD	IMPACT	WHAT TO DO FIRST
BEC / Wire Fraud / Financial Fraud	Almost Certain	Critical	Dual-approval wire controls; callback verification; MFA on finance email
Ransomware on Core Systems	Almost Certain	Critical	MFA + immutable backups + EDR + segmentation
Phishing / Credential Theft	Almost Certain	High	Phishing-resistant MFA; security awareness training
Beneficiary / Client Data Breach	Likely	Critical	Encryption; access controls; DLP; audit logging
Donor PII & Payment Data Exposure	Likely	High	PCI DSS compliance; encrypted payment processing; access controls
Vendor / Supply Chain Breach	Likely	High	Security requirements in all vendor contracts
Cloud Provider / SaaS Outage	Possible	High	Backup access procedures; multi-provider for critical functions
Insider Data Misuse	Possible	High	RBAC; audit logging; access reviews; offboarding controls
Grant Compliance Failure from IT Incident	Possible	High	Documentation; controls; tested continuity procedures
Volunteer / Contractor Device Compromise	Likely	Medium	BYOD policy; MFA; least-privilege access

HOW TO SET RECOVERY PRIORITIES

Not every system is equally critical to your mission. Here's how to think about recovery priority:

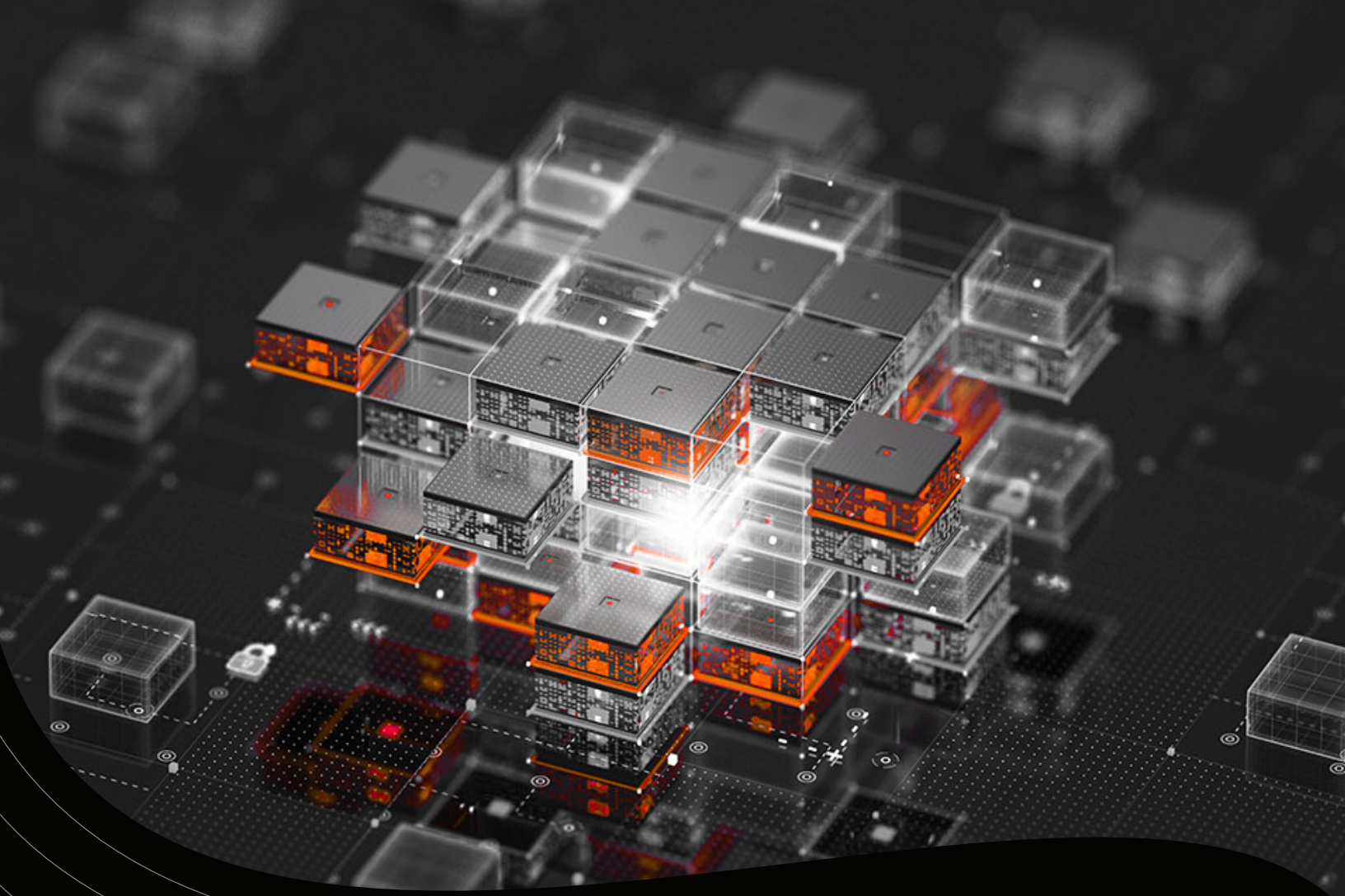
PRIORITY	SYSTEMS	RECOVERY TARGET	WHAT THIS MEANS
Mission-Critical	Case management, crisis hotlines, shelter intake systems, client health records	< 4 hours	Direct service delivery. Failure means people cannot receive care or services. Highest investment priority.
Operational	Donor CRM, grant management, payroll, email, financial systems	< 8 hours	Organizational survival. Failure threatens funding and legal obligations. Tested quarterly.
Important	Program data, volunteer management, website, HR, document management	< 24 hours	Stakeholders notice. Semi-annual DR test. Manual workarounds documented.
Support	Reporting, archives, training platforms, departmental tools	< 3 days	Manageable delays. Annual test. Manual recovery acceptable.

↓

THE BOTTOM LINE

Prioritize by mission impact, not IT complexity. Your case management and crisis service systems are Life-Safety equivalents for non-profits — they get the fastest recovery targets.

If you haven't done a formal risk assessment in the past 12 months, that is your first action item.



SECTION 04

BUILDING YOUR DEFENSES

You don't need to implement everything at once. Start with the highest-impact controls and build outward. This chapter provides a practical framework organized by what matters most.

START HERE: THE FOUNDATION CONTROLS

These five controls prevent or mitigate the vast majority of non-profit cyberattacks. If your budget only covers the basics, these are the basics:

1. MFA Everywhere
2. Dual-Approval Wire Controls
3. Immutable Backups
4. EDR on All Endpoints
5. Security Awareness Training

Framework Strategy: Start Simple, Build Smart

Start with CIS Controls v8 Implementation Group 1 (IG1) — 56 foundational controls designed for organizations with limited resources. Layer HIPAA requirements if you handle health data. Layer PCI DSS if you process donations. Map to NIST CSF for grant reporting. This gets you 80% of the security value at 20% of the cost of a full enterprise framework.

Eligible non-profits can access Microsoft 365 Business Premium (includes enterprise security features) for $3/user/month through TechSoup. This alone covers email security, MFA, EDR, and device management for most small non-profits.

BEC PREVENTION: THE NON-PROFIT PRIORITY

Business Email Compromise is the highest-probability, highest-impact financial threat specific to non-profits. Unlike ransomware, BEC losses are rarely covered by insurance and almost never recovered. The following controls must be in place before anything else:

CONTROL	WHAT IT DOES	IMPLEMENTATION
Dual-approval wire transfers	No single employee can authorize a wire transfer. Two authorized individuals must independently approve any payment above a defined threshold (e.g., $1,000).	Define threshold in financial policy; configure in banking platform; no exceptions for 'urgent' requests.
Callback verification for payment changes	Any request to change a vendor's bank account or redirect a payment must be verified by phone call to a known number — never by responding to the email that requested the change.	Train all finance staff; post the procedure at workstations; make it a non-negotiable policy.
MFA on all email accounts	An attacker who has compromised an email account can send BEC requests that look completely legitimate. MFA prevents account takeover even if credentials are stolen.	Enable Microsoft 365 or Google Workspace MFA for 100% of staff — especially executive and finance accounts.
DMARC / DKIM / SPF email authentication	Prevents attackers from spoofing your domain to send fake emails that appear to come from your executives or board members.	Implement through your email provider; free to deploy; prevents domain impersonation.
Executive account impersonation policy	Train staff to be skeptical of any urgent financial request from an executive, especially those asking to keep it confidential or use personal email.	Include in onboarding and annual training; simulate BEC attempts quarterly.

NETWORK SEGMENTATION — THE MOST IMPORTANT ARCHITECTURE DECISION

If an attacker gets into your network, segmentation determines whether they compromise one system or everything. At minimum, separate these zones:

Client/Beneficiary Data Systems: Case management, health records, client databases on an isolated segment. No direct internet access.

Financial Systems: Donor CRM, grant management, accounting, payroll on a separate segment with strict access controls.

Staff Productivity: Email, collaboration tools, general productivity — separate from sensitive data systems.

Volunteer / Guest Wi-Fi: Completely isolated from all internal networks. Volunteers never on the corporate network.

Remote Access: All remote connections through MFA-protected gateways, not open VPNs.

IDENTITY AND ACCESS: WHO GETS IN?

WHAT	TRADITIONAL NON-PROFIT APPROACH	WHAT YOU SHOULD DO INSTEAD
Authentication	Password only; shared accounts for volunteers	MFA for all staff; time-limited accounts for volunteers with the minimum access they need
Volunteer access	Same login as staff; never revoked	Separate volunteer accounts; role-limited; automatically expire; never share staff credentials
Network access	Being on the Wi-Fi = trusted	Zero Trust: verify every user, every time. Guest Wi-Fi isolated from all internal systems.
Privileged accounts	Shared admin passwords; IT handles everything	PAM for IT admins; just-in-time access; session recording for critical system changes
Offboarding	Accounts left active after departure	Automated deactivation tied to HR; same-day for terminations; quarterly access reviews
Board member access	Often ad-hoc; personal devices; minimal controls	Defined board portal with MFA; no access to production systems; org-managed devices for board members handling sensitive data

PROTECTING BENEFICIARY AND DONOR DATA

DATA CATEGORY	EXAMPLES	WHAT TO DO
Highly Sensitive	Domestic violence history, immigration status, mental health records, substance abuse treatment, HIV status, legal case details	Maximum controls. Encryption at rest and in transit. Need-to-know access only. Strict audit logging. Consider whether this data needs to be retained at all.
Confidential	Client/beneficiary PII, donor personal data and giving history, employee HR records, financial records, grant financials	Encrypted at rest/in transit. Access controlled and logged. DLP monitoring. Breach notification obligations apply.
Internal	Program data, operational procedures, draft budgets, internal communications, volunteer schedules	Standard access controls. Not publicly shared without review.
Public	Annual reports, IRS Form 990, press releases, public program information, published research	Public records obligations. No special protection after publication.

↓ THE BOTTOM LINE

Architecture beats tools. MFA, BEC controls, network segmentation, and data classification are decisions with higher return on investment than any product purchase. Fix the architecture first. Detection tools layer on top.

SECTION 05

COMPLIANCE – WHAT YOU MUST DO

Non-profit compliance obligations vary significantly by the populations you serve and the funding you receive. Understanding which requirements apply to your organization is the first step — then building IT controls to meet them.

THE NON-PROFIT COMPLIANCE LANDSCAPE

REQUIREMENT	WHO IT APPLIES TO	CONSEQUENCES OF NON-COMPLIANCE	PRIORITY ACTION
HIPAA / HITECH	Non-profits providing health care, behavioral health, substance abuse treatment, or certain social services	Fines up to $2.1M per violation category per year; criminal penalties; reputational damage	Encrypt PHI; audit access; conduct risk assessment; BAA with all vendors handling PHI
PCI DSS	Any non-profit accepting credit card donations or payments	Loss of ability to accept cards; fines; required forensic investigation after breach	Use PCI-compliant payment processors; never store card data on your systems
State Breach Notification	All non-profits in the US holding resident PII	State AG enforcement; fines; litigation; reputational damage	Document IR procedures; know your state's timeline (ranges 30–90 days)
FERPA	Education-focused non-profits, school programs, or non-profits with access to student records	Loss of federal education funding; enforcement	Restrict access to student records; data sharing agreements
Federal Grant Compliance	Non-profits receiving federal funding (HHS, DOJ, HUD, DoEd, etc.)	Grant termination; repayment demands; exclusion from future funding	Document IT controls; data security plans; incident notification requirements
State Charitable Registration	All non-profits soliciting donations in states where registered	State investigations; fines; deregistration	Maintain current registration; data practices consistent with privacy expectations
IRS Form 990	All 501(c)(3) organizations (publicly disclosed)	Public visibility into data practices; donor/funder scrutiny	Ensure governance and data policies are defensible when publicly reviewed

HIPAA Applies to More Non-profits Than You Think

If your non-profit provides healthcare services, behavioral health counseling, substance abuse treatment, or certain housing programs that receive Medicaid funding, HIPAA almost certainly applies. Many non-profits underestimate their HIPAA obligations. The consequences of non-compliance are severe: fines that dwarf the cost of controls, reputational damage with healthcare funders, and potential exclusion from government contracts.

If you're unsure whether HIPAA applies to your organization, get a legal opinion. The cost is minimal compared to the risk.

Grant Compliance: The Non-profit-Specific Obligation

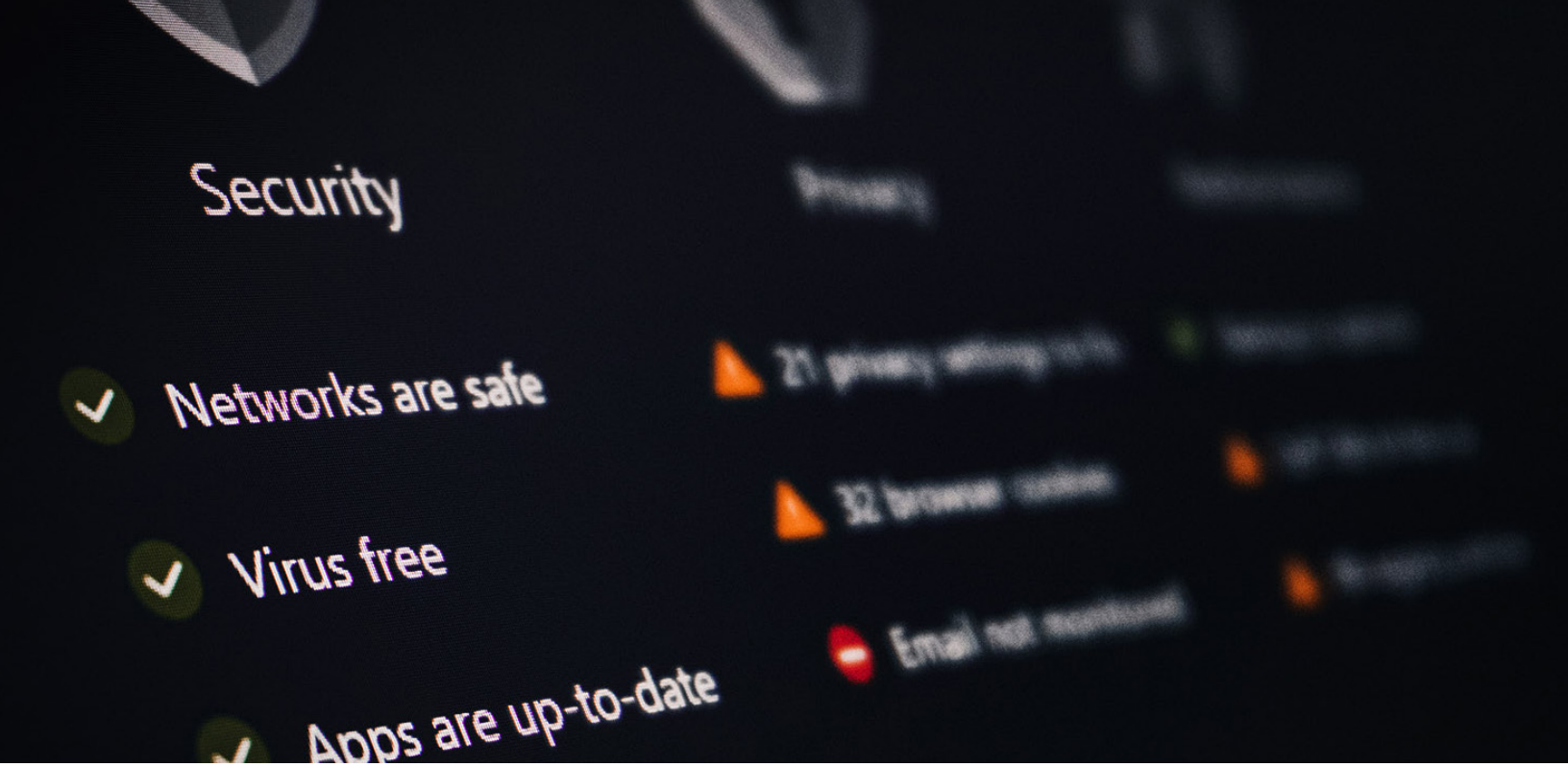
Federal grants increasingly include cybersecurity requirements that non-profits must meet to remain in good standing. Key requirements to know:

- HHS grants (healthcare, social services): Data security plans, access controls, incident notification within 1 hour of discovery for certain breaches.
- DOJ grants (legal aid, victim services): CJIS-equivalent requirements for criminal justice data, strong access controls.
- HUD grants (housing, homelessness): Data quality and security requirements for HMIS (Homeless Management Information System) data.
- Education Department grants: FERPA compliance, data sharing agreement requirements.
- State government grants: Increasingly mirroring federal requirements; review your specific grant terms.

What Funders Are Starting to Ask

A growing number of private foundations and government funders are adding data security questions to grant applications and renewal processes. Expected questions include: Do you have a written data security policy? How do you protect beneficiary data? What is your incident response plan? Do you conduct cybersecurity training?

Being able to answer these questions confidently — and point to documented controls — is increasingly a competitive differentiator in grant applications.



PRIVACY: THE SECTOR'S EVOLVING OBLIGATION

Beyond HIPAA, non-profits must navigate an expanding patchwork of state privacy laws. California (CCPA), Virginia (VCDPA), Colorado, Connecticut, and a growing list of states impose data rights obligations — the right to access, correct, and delete personal data — that affect any organization holding resident data from those states.

Non-profits that engage in digital fundraising, email marketing, or online program delivery should assess whether state privacy laws apply and ensure their privacy policies, consent mechanisms, and data deletion procedures are current.

↓ THE BOTTOM LINE

HIPAA and PCI DSS compliance are non-negotiable if they apply to you — the consequences of non-compliance far exceed the cost of controls.

Grant compliance is the non-profit-specific obligation: know what your funders require, document your controls, and have an incident notification procedure before an incident occurs.

SECTION 06

WHEN THINGS GO WRONG

A cyber incident is not a question of if — it is a question of when. What matters is how fast and how effectively you respond. For non-profits, the stakes include not just financial recovery but continued service delivery to people who have nowhere else to turn.

THE RESPONSE TIMELINE

PHASE	WHAT HAPPENS	TARGET TIME	WHO LEADS
Detect	Identify the incident. Is it ransomware, BEC fraud, or a data breach? Assess scope. Are client service systems affected? Classify severity. Notify executive director.	< 1 hour	IT / MSSP
Analyze	Determine what's compromised. Preserve evidence. Assess donor and beneficiary data exposure. Identify the attack vector.	1–4 hours	Exec Director + IT
Contain	Isolate affected systems. Protect client service systems first. Block attacker access. Freeze affected financial accounts if BEC suspected.	2–12 hours	IT + Finance + Exec
Eradicate	Remove malware. Patch the vulnerability. Reset all compromised credentials. Verify backup integrity.	12–72 hours	IT / IR Firm
Recover	Restore from backups. Resume client services first. Validate data integrity. Notify affected parties per legal requirements.	1–14 days	IT + Program Directors
Learn	Root cause analysis. Breach determination. Notify affected individuals per state law. Brief board. Notify grant funders if required. Update procedures.	1–6 weeks	Exec Director + Legal

THE RANSOMWARE DECISION FRAMEWORK

When ransomware hits, the most consequential decisions involve

Client services first: Are case management, crisis hotlines, or shelter systems affected? Activate manual procedures immediately.

Can programs continue? Activate COOP (Continuity of Operations) procedures. Know which services can run manually and which are fully technology-dependent.

To pay or not to pay? Payment does not guarantee recovery, funds criminal organizations, and may violate OFAC sanctions. Have this policy decided before an incident — not during one.

Who to call: CISA (free IR assistance), your IR retainer firm (hands-on response), legal counsel (breach obligations), cyber insurance carrier (report immediately).

Do This Before You Need it

- ✓ Establish a relationship with CISA (free, they respond to non-profits).
- ✓ Sign an incident response retainer with a qualified IR firm — pre-negotiated rates matter when you're in crisis.
- ✓ Conduct a ransomware tabletop exercise with the Executive Director, Finance Director, Program Directors, and board chair.
- ✓ Pre-define who has authority to shut down systems, freeze financial accounts, and communicate publicly.
- ✓ Know your cyber insurance carrier's incident notification requirements — most require notification within 24–72 hours.

Doing these five things before an incident will cut response time in half and recovery cost dramatically.

WHO YOU MUST NOTIFY - AND WHEN

Non-profit breach notification is multi-layered. Your notification matrix should map each data type to its specific requirements:

State breach notification law: Notify affected individuals (typically 30–90 days, varies by state).

HIPAA: Notify HHS within 60 days for health data breaches affecting 500+ individuals; notify individuals; notify media for large breaches.

Grant funders: Federal grant terms often require incident notification within 1 hour of discovery for certain data types — know your specific grant requirements.

Board of Directors: Brief the board before they hear it from a donor or the media.

Donors: Proactive communication with major donors and relevant donor segments, managed with legal counsel.

State charity regulators: Some states require notification of a breach affecting charitable assets or donor funds.

THE BOTTOM LINE

The time to prepare for a ransomware attack or BEC incident is before it happens.

Tabletop exercises, retainer contracts, and pre-defined decision authority save weeks of confusion and hundreds of thousands of dollars during a crisis.

Client service continuity is always the #1 priority. Everything else comes second.

SECTION 07

KEEPING PROGRAMS RUNNING

Non-profit programs cannot stop serving people because of a cyberattack. Continuity planning is a mission obligation, not an IT checkbox.

THE THREE PILLARS OF NON-PROFIT CONTINUITY

PILLAR 1: IMMUTABLE BACKUPS

Backups that cannot be encrypted, modified, or deleted — even by an administrator. Air-gapped from production networks. Separate credentials from your main IT systems. Tested quarterly with full restoration verification. This is the single most important control for ransomware recovery. For non-profits: ensure your case management system, donor database, and grant financial records are specifically included in backup testing.

PILLAR 2: MANUAL PROGRAM PROCEDURES

When all IT systems are down, your programs must still serve people. Documented manual procedures for: paper-based intake, manual case notes, phone-based crisis services, check-based payroll, paper grant tracking, and donor acknowledgment by phone. These procedures must be current, supplies maintained, and staff trained. Many non-profits discover during attacks that their manual procedures are outdated or non-existent.

PILLAR 3: PARTNERSHIPS & SHARED SERVICES

Individual non-profits rarely have enterprise DR capability. Leverage: state nonprofit technology associations, TechSoup shared services, peer organization mutual aid agreements, fiscal sponsor infrastructure where applicable, and cloud DR through nonprofit-discounted Microsoft or Google agreements. Regional non-profit consortia sharing IT infrastructure costs can achieve enterprise-grade resilience at a fraction of individual cost.

↓ THE BOTTOM LINE

Test your backups. Test your manual program procedures. Test your DR plan. If you haven't tested it, it doesn't work.

And do it before your annual fundraising campaign, grant reporting deadlines, or your busiest program delivery period — when continuity matters most.

SECTION 08

MANAGING VENDOR RISK

Non-profits increasingly depend on cloud-based systems — donor CRMs, case management platforms, payment processors, grant management tools, payroll providers. Many of these vendors process your most sensitive data. A vendor breach is your breach — and your breach notification obligation.

TIER YOUR VENDORS BY RISK

TIER	WHO	WHAT TO REQUIRE	REVIEW FREQUENCY
Critical	Donor CRM, case management/EHR, payment processor, primary cloud provider, payroll, grant management system	Full security assessment, SOC 2 Type II, pen test review, HIPAA BAA where applicable, breach notification within 1 hour	Annually + after any incident
High	HR platform, email/productivity suite, document management, volunteer management, fundraising platforms	Detailed security questionnaire, SOC 2 or ISO 27001, DPA/BAA where applicable	Annually
Moderate	Departmental SaaS, scheduling tools, analytics platforms, social media management	Standard questionnaire, certification check, privacy review	Every 2 years
Low	Facilities, office supplies, non-IT services with no data access	Standard contract terms	Every 3 years

WHAT TO PUT IN EVERY VENDOR CONTRACT

- SOC 2 Type II certification (or equivalent) — annual.
- HIPAA Business Associate Agreement for any vendor processing protected health information.
- Breach notification within 1 hour of discovery — not 72 hours or 30 days.
- Data ownership: your data is yours; vendor may not use beneficiary or donor data for any other purpose.
- Data deletion: vendor must certify deletion of your data within 30 days of contract termination.
- Right-to-audit: you have the right to request evidence of security controls.
- Sub-processor disclosure: vendor must disclose and obtain your approval for any sub-processors handling your data.

Your IT Managed Service Provider Is a High-Value Target

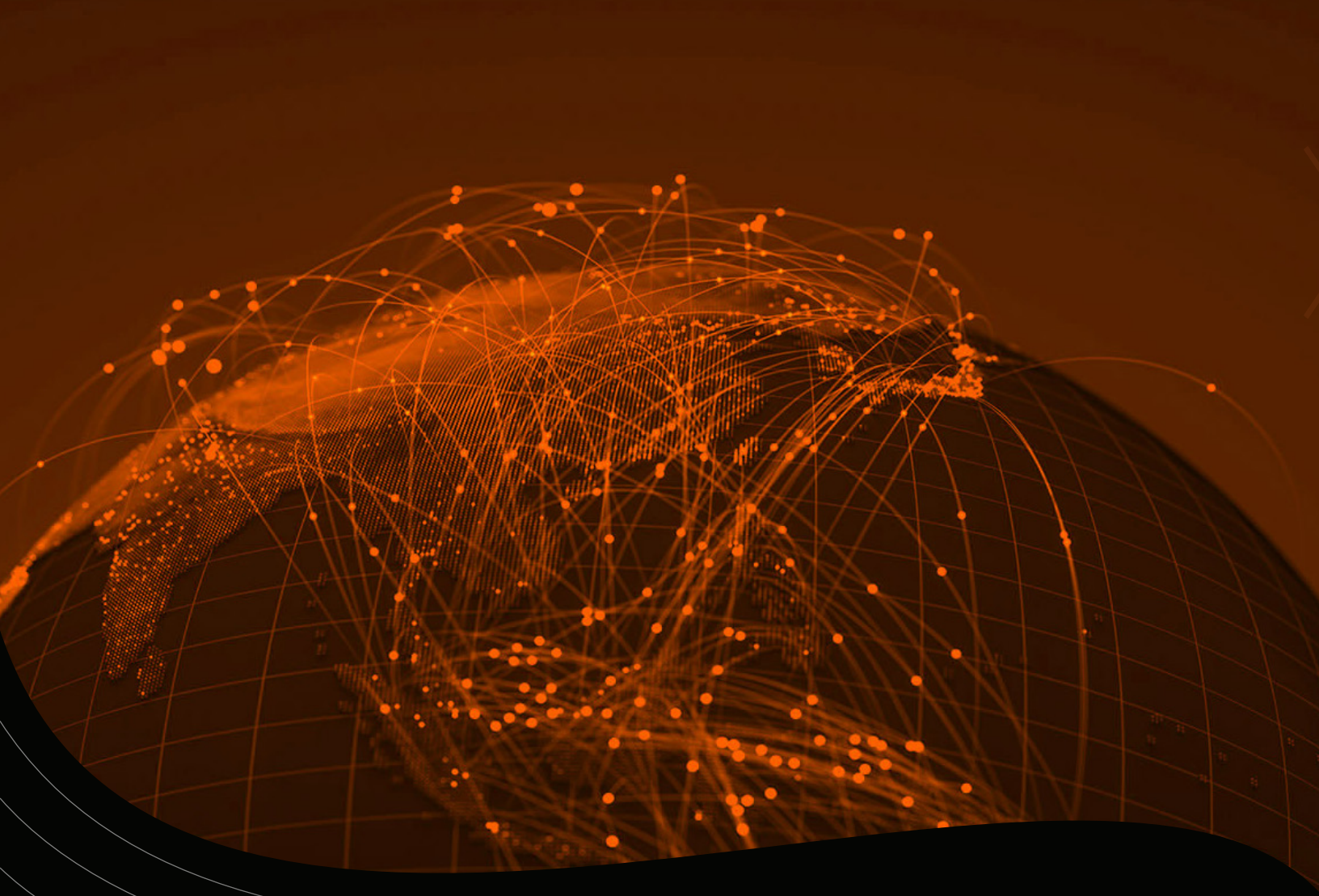
Many non-profits rely on a single MSP for all IT management. A compromised MSP gives the attacker access to every client organization simultaneously. This attack pattern — targeting MSPs to reach their non-profit clients — is well-documented.

Require your MSP to: use MFA for all access to your systems, record all administrative sessions, meet CIS Controls IG2 or better, notify you within 1 hour of any security incident, and allow you to audit their security practices annually.

THE BOTTOM LINE

If a vendor has access to your donor data, beneficiary records, or financial systems, you are responsible for their security.

Use your contracts to require security standards. And know which vendors are critical — if they go down, what programs go with them?



SECTION 09

NEW RISKS ON THE HORIZON

AI-powered tools, digital fundraising platforms, and cloud-first operations offer real mission benefits for non-profits. They also introduce risks that require governance before deployment — not after a problem occurs.

AI IN NON-PROFITS: OPPORTUNITY AND OBLIGATION

Non-profit AI applications include: AI-assisted case management, donor prospect research, grant writing assistance, chatbots for beneficiary intake, fraud detection in financial systems, and program outcome analytics. The benefits are real. So are the risks.

AI Bias Has Real Consequences for Vulnerable Populations

Non-profits using AI in case management, benefits eligibility screening, or resource referral systems must ensure these tools do not perpetuate or amplify bias against the populations they serve. An AI tool that systematically under-serves communities of color, low-income individuals, or people with disabilities creates legal liability and violates the organization's mission. Before deploying any AI in client-facing workflows, require a bias assessment and establish human review processes for high-stakes decisions.

Generative AI + Beneficiary Data = Serious Risk

A staff member pasting client records, case notes, or donor information into an external AI tool (ChatGPT, Claude, Gemini) for drafting or analysis has potentially disclosed protected data in violation of HIPAA, state privacy laws, and donor privacy expectations.

Establish a clear AI acceptable-use policy before your staff adopts ungoverned AI tools. Eligible non-profits can deploy governed enterprise AI through Microsoft 365 Copilot (nonprofit pricing) or Google Workspace AI features — where data is contractually protected.

DIGITAL FUNDRAISING: THE EXPANDING ATTACK SURFACE

Online giving platforms, peer-to-peer fundraising tools, email marketing systems, and social media accounts all represent attack surface that did not exist a decade ago.

KEY RISKS

Payment skimming: Attackers inject malicious code into donation forms to steal credit card data (Magecart attacks). Use PCI-compliant hosted payment solutions — never process card data on your own server.

Fundraising platform impersonation: Fraudsters create fake donation pages impersonating your organization to redirect funds. Monitor for impersonation; register variants of your domain name.

Email marketing account compromise: A compromised Constant Contact, Mailchimp, or similar account can be used to send phishing emails to your entire donor list. Enable MFA on all marketing platforms.

Social media account hijacking: Hijacked social accounts damage reputation and can redirect followers to fraudulent campaigns. Enable MFA; define who has access; establish account recovery procedures.

CLOUD SECURITY: SHARED RESPONSIBILITY

Most non-profits are now substantially cloud-dependent — Microsoft 365, Google Workspace, Salesforce, cloud-based case management. The 'shared responsibility model' means the cloud provider protects the infrastructure, but you are responsible for who has access, what data is stored, and how it is configured.

AI Bias Has Real Consequences for Vulnerable Populations

- Not enabling MFA (the single most important cloud security control)
- Overly permissive sharing settings (donor files shared with 'anyone with the link')
- No backup of cloud data (Microsoft 365 and Google Workspace data needs to be backed up — the provider does not back it up for you)
- Former staff and volunteers with active accounts
- No review of third-party apps connected to your cloud environment

→ All of these are fixable with existing tools at no additional cost.

↓ THE BOTTOM LINE

New technology should be adopted with eyes open. Establish AI governance and digital fundraising security policies before deployment, not after a breach or a donor complaint.

The question isn't whether to adopt AI or digital tools — it's whether to do it in a way that protects the people you serve.

SECTION 10

MEASURING WHAT MATTERS

You can't manage what you don't measure. These Key Risk Indicators (KRIs) give your board and leadership a clear dashboard of your security posture — and early warning when something needs attention.

THE NON-PROFIT CYBER HEALTH DASHBOARD

METRIC	WHAT IT TELLS YOU	HEALTHY	NEEDS ATTENTION	HOW OFTEN
MFA adoption	% of staff using MFA	>95%	<80%	Monthly
BEC simulation pass rate	% of staff correctly identifying BEC test emails	>90%	<70%	Quarterly
Wire transfer dual-approval compliance	% of wire transfers with dual approval	>99.9%	<100%	Monthly
Backup success rate	% of backup jobs completing successfully	>99%	<95%	Weekly
Phishing click rate	% of staff clicking test phishing emails	<5%	>10%	Monthly
Volunteer / contractor account hygiene	% of active accounts belonging to current volunteers	>95%	<85%	Quarterly
Patch compliance	% of critical patches applied in 30 days	>90%	<75%	Monthly
Donor data encryption coverage	% of donor PII encrypted at rest	>99%	<95%	Quarterly
DR test pass rate	% of DR tests meeting recovery targets	>90%	<75%	Semi-annual
Incident response readiness	Tabletop completed; contacts current; retainer active	All current	Any gap	Annual

GOVERNANCE: WHO'S ACCOUNTABLE?

Board of Directors: Annual cybersecurity briefing. Approve IT security investment as a budget line item. Accountable to donors, beneficiaries, and regulators.

Executive Director: Quarterly IT risk update. Final decision authority on major security incidents, ransom decisions, and public communications.

Finance Director: Owns BEC prevention controls — dual-approval procedures, wire transfer verification, financial system access. Reports BEC KRIs monthly.

IT Director / MSSP: Responsible for the security program, controls implementation, KRI reporting, and incident response. Reports to Executive Director, not buried under operations.

Program Directors: Own client data risks in their programs. Implement data classification and access controls for program-specific data.

What Funders Are Starting to Ask

Don't say: 'We have 400 unpatched vulnerabilities and no SIEM coverage.'

Do say: 'We are at high risk of a ransomware attack that could halt program delivery for 2–4 weeks, cost $200,000–$2M in recovery, and expose the personal data of every client and donor we serve. A $30,000 investment in MFA, backups, and security training eliminates 80% of this risk — and most of it can be covered through Microsoft's nonprofit grant program at no cost.'

Mission impact + constituent harm + cost with solution = board approval

↓ THE BOTTOM LINE

Track the metrics that matter. Report them to leadership in language they understand.

And ensure your IT function has direct access to the Executive Director and board — not buried three levels down under operations.

SECTION 11

BUILDING A SECURITY-AWARE ORGANIZATION

The best technology in the world won't protect your organization if your people click on phishing emails, share passwords, or send beneficiary data to personal email accounts. Culture is the most cost-effective security control available to a resource-constrained non-profit.

TRAINING THAT ACTUALLY CHANGES BEHAVIOR

Generic annual awareness training doesn't work. Different roles face different threats. Tailor your program:

ROLE	TRAIN THEM ON	WHY IT MATTERS
Direct Service / Case Workers	Beneficiary data handling, phishing awareness, social engineering, secure use of case management systems, personal device risks	They handle the most sensitive beneficiary data daily and are high-value targets for social engineering aimed at client records
Finance & Operations Staff	BEC fraud, wire transfer verification procedures, vendor impersonation, segregation of duties, W-2 / tax fraud schemes	They have authority over financial transactions and are the primary BEC target — a single mistake can cost $100K+
Development / Fundraising Staff	Donor data privacy, secure handling of payment information, email account security, social media account protection, phishing in donation context	They manage the donor database and payment channels — a compromise damages fundraising for years
Volunteer Coordinators	Volunteer account management, access provisioning and deprovisioning, risks of shared credentials, device security for volunteers	They manage the highest-turnover access population; poor access hygiene here is a persistent vulnerability
Executive Director & Senior Leaders	Whaling attacks (executive impersonation), personal email security, their role in IR decision-making, board-level cyber governance	They are high-value impersonation targets and the ultimate decision-makers in a crisis — uninformed leaders make bad decisions
Board Members	Targeted BEC attempts (board member impersonation is common), their governance obligations around cybersecurity, investment rationale	Boards are increasingly targeted; board member impersonation is used to authorize fraudulent payments
IT Staff	Privileged access discipline, change management, incident recognition, medical / HIPAA system security if applicable	They have the keys to everything — compromised IT credentials are the most damaging

THE TALENT CHALLENGE — AND WHAT TO DO ABOUT IT

Non-profit IT pay lags the private sector significantly. Most small and mid-sized non-profits have one IT generalist — or none. This is a structural challenge that requires structural solutions:

MSSP partnerships: Outsource 24/7 monitoring and response to a managed security service provider — a $30–60K/year contract provides more security coverage than an unfilled $80K security position.

vCISO (Virtual CISO): Part-time security leadership from an experienced professional at a fraction of full-time cost. Increasingly available with non-profit experience.

Peer non-profit consortia: Share security staff, tools, and services with similar organizations. Several regional non-profit technology networks offer shared IT and security services.

CISA resources: Free training, vulnerability scanning, and incident response assistance available to all organizations — not just government.

TechSoup and vendor nonprofit programs: Microsoft, Google, Cisco, and others offer deeply discounted or donated security tools to eligible non-profits. These programs can provide enterprise-grade security at near-zero cost.

↓ THE BOTTOM LINE

You don't need a 10-person security team. You need the right partnerships, the right training, and a security-conscious culture from the board down to every volunteer.

A $40K/year MSSP contract provides more security coverage than an unfilled $80K security position. Start there.

SECTION 12

YOUR ROADMAP

Here's a phased plan to take your cybersecurity posture from where it is today to where it needs to be. Organized by urgency, not complexity — and calibrated for non-profit resource realities.

PHASE 1:
IMMEDIATE (0–3 MONTHS) — STOP THE BLEEDING

INITIATIVE	WHY IT'S URGENT	SUCCESS LOOKS LIKE	ESTIMATED EFFORT & COST
MFA for all staff and systems	Stops 99% of credential-based attacks; prevents BEC account takeover	MFA >95% all staff; email, financial, and case management systems covered	Low — free with Microsoft/ Google nonprofit licenses
Dual-approval wire transfer controls	Prevents BEC financial fraud — the #1 direct financial threat to non-profits	No single-approval wire transfers >$1,000; callback verification policy documented	Low — process and policy, minimal technology
Immutable backups	Only reliable ransomware recovery path; protects donor and beneficiary data	Air-gapped backups tested; case management and donor CRM specifically tested	Medium — $5–15K/year for cloud backup
EDR on all endpoints	Detect and stop threats before they spread to critical systems	EDR on 100% of managed endpoints (free via Microsoft/Google nonprofit plans)	Low to Medium — often covered by nonprofit licenses
Join CISA mailing list and establish relationship	Free help is available before you need it	CISA regional contact established; signed up for alerts	Low — free
Sign IR retainer contract	Expert help on call before crisis; most non-profits can't afford day-rates during an incident	Retainer signed; contact list distributed to exec team	Low — $5–15K/year

PHASE 2:
BUILD (3–9 MONTHS) — STRENGTHEN THE FOUNDATION

INITIATIVE	WHY IT'S URGENT	SUCCESS LOOKS LIKE	ESTIMATED EFFORT
Network segmentation (critical zones)	Limit blast radius; isolate beneficiary data and financial systems	Client data, financial, staff, and volunteer/guest networks segmented	High — requires planning and potential infrastructure
Vendor risk management program	Control your largest attack surface — donor CRM, case management, payment processor	All critical vendors assessed; contracts include security requirements	Medium

INITIATIVE	WHY IT'S URGENT	SUCCESS LOOKS LIKE	ESTIMATED EFFORT
HIPAA / PCI compliance assessment (if applicable)	Maintain regulatory standing; protect beneficiaries and donors	Assessment complete; gaps prioritized; BAAs executed	Medium
Role-based security awareness training	Generic training doesn't change behavior; role-specific training does	Training deployed by role; BEC simulation quarterly; phishing monthly	Low-Medium — free platforms available for non-profits
COOP plan development	Continuity for essential programs during an outage	Manual procedures current and tested; program staff trained	Medium
Cyber insurance review	Ensure coverage matches actual risk; know what's covered for BEC	Policy reviewed; coverage limits and exclusions understood	Low

PHASE 2:
BUILD (3–9 MONTHS) — STRENGTHEN THE FOUNDATION

INITIATIVE	WHY IT'S URGENT	SUCCESS LOOKS LIKE	ESTIMATED EFFORT
Zero Trust Architecture	Eliminate implicit trust; protect remote and volunteer access	ZTA maturity score >3/5; ZTNA deployed for remote access	High
Data Loss Prevention (DLP)	Prevent inadvertent and intentional beneficiary data exfiltration	DLP on email, cloud storage, and web uploads	Medium
AI governance framework	Manage AI risk in program delivery and administration	AI policy published; all AI tools inventoried; staff trained	Medium
Full data classification & lifecycle management	Know what data you hold, where it is, and when to delete it	Data inventory complete; retention policies documented	Medium
MSSP 24/7 monitoring	Continuous threat detection beyond business hours	MSSP monitoring all critical systems; integrated alerting	Medium-High — $30–60K/ year
Board cybersecurity governance formalization	Board-level accountability; governance documentation for funders	Board cyber committee or liaison designated; annual briefing standard	Low

FUNDING YOUR ROADMAP

You have more funding options than you think:

Microsoft Nonprofit Program: Microsoft 365 Business Premium (includes Defender, Intune, Azure AD P1) — free for up to 10 users, deeply discounted beyond. Covers MFA, EDR, and device management.

Google for Nonprofits: Google Workspace Business Plus free for eligible non-profits — includes advanced security features.

Cisco Networking Academy and NetSol: Discounted networking and security infrastructure.

TechSoup: Discounted software, hardware, and services from 100+ technology partners.

Cyber Readiness Institute: Free cybersecurity resources and training for small and mid-sized non-profits.

Capacity-building grants: Many community foundations and larger non-profit funders will fund IT security infrastructure as part of organizational capacity grants — frame it as mission protection.

Cyber insurance premium savings: Better security posture directly reduces premiums — model the savings as ROI.

↓ THE BOTTOM LINE

You don't need unlimited budget. You need MFA, BEC controls, immutable backups, EDR, and security training. Most of the most impactful controls are available free or at deep discount through non-profit technology programs.

Start today. Your clients, donors, and beneficiaries are counting on you.

CONCLUSION: RESILIENCE AS MISSION PROTECTION

Non-profits exist to serve people who need help.

When your systems go down, clients cannot access services. When your data is breached, the personal information of your most vulnerable constituents is exposed. When your financial systems are compromised, the funds meant for programs are diverted. When donors lose trust, your mission loses resources.

IT operational resilience is not a technology problem. It is a mission protection imperative.

The non-profits that invest in resilience gain more than protection against downside scenarios. They gain the confidence to serve more people, the trust of their donors and funders, the ability to demonstrate responsible stewardship to regulators and foundations, and the operational foundation to adopt new technology that amplifies their mission impact.

THIS GUIDE IS NOT A DESTINATION - IT'S A DIRECTION

The non-profits that sustain resilience over time embed risk management into every technology decision, every vendor contract, every budget cycle, and every new program. Those who make it a shared commitment — from the board to every staff member and volunteer — will be prepared for whatever comes next.

APPENDIX A: KEY RESOURCES

FREE AND LOW-COST RESOURCES FOR NON-PROFITS

CISA: Free assessments, training, exercises, and incident assistance — cisa.gov (available to all organizations, not just government)

MS-ISAC: Multi-State ISAC threat intelligence and resources — now open to non-profits — cisecurity.org/ms-isac

TechSoup: Discounted technology products and services for eligible non-profits — techsoup.org

Microsoft Nonprofit Program: Donated and discounted Microsoft 365, Azure, and security products — microsoft.com/nonprofits

Google for Nonprofits: Free Google Workspace and other services — google.com/nonprofits

Cyber Readiness Institute: Free cybersecurity tools and training for SMOs — cyberreadinessinstitute.org

NTEN (Non-profit Technology Network): Sector-specific technology and security resources — nten.org

Nonprofit Risk Management Center: Risk management tools and resources — nonprofitrisk.org

Internet2: Community anchor institution shared services including cybersecurity — internet2.edu

FRAMEWORKS AND STANDARDS

- NIST Cybersecurity Framework 2.0 — nist.gov/cyberframework
- CIS Controls v8 — cisecurity.org/controls
- HIPAA Security Rule — hhs.gov/hipaa
- PCI DSS (Payment Card Industry) — pcisecuritystandards.org
- NIST SP 800-171 (for organizations handling federal data) — nist.gov
- ISO/IEC 27001:2022 — Information Security Management Systems

PROFESSIONAL ORGANIZATIONS

- NTEN (Non-profit Technology Network) — nten.org
- Alliance for Nonprofit Management — allianceonline.org
- BoardSource (board governance resources) — boardsource.org
- National Council of Nonprofits — councilofnonprofits.org

APPENDIX B: GLOSSARY

Non-profit IT Terms

CRM (Constituent Relationship Management): Software tracking relationships with donors, volunteers, clients, and stakeholders.

Case Management System: Platform supporting client intake, service delivery, outcomes tracking, and case notes for direct service programs.

HMIS (Homeless Management Information System): HUD-mandated data system for tracking individuals experiencing homelessness; subject to strict data security requirements.

Grant Management System: Software tracking grant applications, awards, reporting deadlines, and restricted fund usage.

BAA (Business Associate Agreement): HIPAA-required contract between a covered entity and a vendor that handles protected health information.

COOP (Continuity of Operations Plan): Documented plan for maintaining essential programs and functions during a disruption.

Security Terms

BEC (Business Email Compromise): Fraud scheme where attackers impersonate executives or vendors to redirect financial transactions.

MFA (Multi-Factor Authentication): Requiring two or more proofs of identity to log in — the single most effective control against credential-based attacks.

EDR (Endpoint Detection and Response): Security software that monitors computers for threats and enables rapid response.

MSSP (Managed Security Service Provider): Outsourced 24/7 security monitoring and response.

Phishing: Deceptive emails or messages designed to steal credentials or deliver malware; the #1 initial access method for attackers.

Ransomware: Malware that encrypts an organization's data and demands payment for decryption.

ZTA (Zero Trust Architecture): Security model requiring verification of every user and device regardless of network location.

PAM (Privileged Access Management): Controls and monitoring for accounts with elevated system access.

DLP (Data Loss Prevention): Tools that detect and prevent unauthorized data transfer or disclosure.

RTO (Recovery Time Objective): How fast a system must be restored after failure.

RPO (Recovery Point Objective): How much data loss is acceptable (measured in time).

vCISO (Virtual CISO): Part-time or contracted cybersecurity leadership — common in the non-profit sector.

PCI DSS (Payment Card Industry Data Security Standard): Security requirements for organizations that accept credit card payments.

ABOUT MALA TECHNOLOGY ADVISORS

TECHNOLOGY INNOVATION STARTS HERE

MALA Technology Advisors is a leading technology advisory firm helping businesses modernize, adapt, and grow through smart, strategic use of technology. MALA stands for Modernization, Agility, Leadership, and Advancement—the values that guide everything we do. As a vendor-neutral strategic partner, we work with forward-thinking organizations to align business and information technology goals. Using our 4-Pillar approach, we help clients reimagine, restructure, and renew business IT initiatives to create agile and resilient organizations.

Our Services

Managed Cybersecurity · Cloud Services · Network and SD-WAN · Managed IT · Communications as a Service · IoT and Wireless · Professional Services · Devices

How We Work

Our expert team of technology and business professionals works side-by-side with your organization across a proven engagement model: IT Strategy development, Environment Assessment, Vendor Identification and Selection, Proposed Solution design, and ongoing Account Management. We don't just consult—we partner to simplify complexity, accelerate progress, and unlock new opportunities for growth.

What Sets Us Apart

Our team is a diverse network of consultants and industry professionals with a global mindset and a collaborative culture. We focus on Workplace Technology Innovation, Flexibility in Integration and Implementation, Perpetual Enablement, and Human Connection. The speed of change in technology today is driving a matched evolution of the IT landscape—and more than ever, IT departments rely on MALA Technology Advisors to help them innovate and plan for the future.

GET IN TOUCH

500 Commercial Street, Suite 502, Manchester, NH 03101

(603) 802-2469 · info@malatechadvisors.com

malatechadvisors.com

MALA
TECHNOLOGY
ADVISORS