Protecting Your Mission

Cybersecurity Essentials for Associations in the AI Era

Adam Jones
Director of Technology, Creative Planning Business Services

What We'll Cover Today

01 **The Threat Landscape**
Why associations are targeted, with real-world case studies

02 **Your Rapid Risk Assessment**
Baseline questions every executive should be asking

03 **The "Big 5" Security Measures**
Maximum protection, minimum investment

04 **The AI Dilemma**
Risks, opportunities, and your AI Usage Policy

05 **Culture & Your 30-60-90 Day Roadmap**
Building shared ownership and leaving with a plan

The Threat Landscape

Why associations can no longer afford to ignore cybersecurity

The Numbers Tell the Story

450%

increase in AI phishing effectiveness vs. traditional campaigns

29%

increase in spoofing and spear-phishing

~$5M

average global cost of a data breach (IBM, 2024)

The good news: Defensive measures are working: confirmed account compromises dropped 27% YoY.

Sources: Microsoft Security Blog, April 2026 | Community IT Innovators, 2025 | IBM Cost of a Data Breach Report, 2024

Why Are Associations Targeted?

1. **Valuable Data**
   Donor identities, financial records, beneficiary demographics

2. **Resource Constraints**
   Tight budgets and no full-time CISO signal easy targets

3. **Ideological Motives**
   Rising “doxxing” and personal attacks against staff whose mission conflicts with attacker beliefs

100%

of wire fraud incidents

in 2024 involved an internal compromised account.

NGOs represent 8% of global threat targets

“ Nonprofits are attractive targets for cybercrime because of the sensitive nature of data they manage. ”

BizTech Magazine, “3 Ways Nonprofits Can Strengthen Their Cybersecurity in 2025”

Sources: Community IT Innovators, 2025 | Microsoft Digital Defense Report, 2025 (8% NGO targeting)

How It Actually Happens

CASE 1

The Impersonation Phish

An attacker altered a nonprofit's name by a single letter to spoof accounting reps. They emailed major donors requesting wire transfer changes, stealing large contributions.

CASE 2

The AI Deepfake Scam

A finance worker transferred $25.6 million after joining a video call featuring an AI-generated deepfake of their CFO. Every person on the call was fake.

CASE 3

Callback Phishing

A CEO received an email mimicking QuickBooks with a PDF and phone number. Upon calling, a human scammer adapted in real-time to guide them into installing remote access software.

Case 1: Ironscales, "What is Invoice Fraud?" | Case 2: CNN, Arup deepfake incident | Case 3: Keepnet, "10 Real-Life Callback Phishing Examples," 2025

Assessing Your Risk

Where do you stand today, and what to do about it

Your Rapid Risk Assessment

Six questions every executive should be able to answer "yes" to:

- ✓ Do we have executive-level ownership of our cybersecurity function?
- ✓ Have we conducted a risk assessment within the last year to catalog all digital and physical assets?
- ✓ Do we have written governance policies: IT Acceptable Use, AI Use Policy, and Incident Response Plan?
- ✓ Is MFA fully enforced, with physical security keys for high-risk staff (ED, CFO)?
- ✓ Are we running periodic, mandatory security awareness training for all staff, volunteers, and vendors?
- ✓ Are our data backups automated, and do we routinely test our ability to restore from them?

" Cybersecurity is the top threat faced by all organizations today. "
Melissa Musser, GRF CPAs & Advisors Cybersecurity Symposium

The “Big 5” Security Measures

Maximum protection for minimum investment

The “Big 5” at a Glance

1. Phish-Resistant Multi-Factor Authentication
2. Continuous Security Awareness Training
3. Third-Party Email Filtering & Endpoint Protection
4. Tested Data Backups
5. Zero-Trust Architecture

1

Phish-Resistant MFA

Stopping Attacker-in-the-Middle attacks with hardware keys

99%+

of account compromise attacks blocked by MFA. Identity attacks rose 32% in H1 2025

- Standard MFA is necessary but not enough. AitM attacks can bypass SMS and app codes
- Upgrade executives and finance to FIDO/YubiKey physical security keys or Windows Hello
- 85% of spray-targeted usernames appeared in known credential leaks; use unique passwords
- Start with standard MFA org-wide, then phase in phish-resistant keys for high-risk roles

Source: Microsoft Digital Defense Report, 2025 | Microsoft Security Blog, Aug 2019

2 Security Awareness Training

Turning your staff into a vigilant human firewall

54%

click-through rate on AI phishing vs. 12% traditional: a 450% increase in effectiveness

- AI phishing can be up to 50x more profitable than traditional campaigns (Harvard Kennedy School)
- Human error remains the largest vulnerability, and training is the most cost-effective defense
- Include board members, volunteers, and third-party vendors, not just paid staff
- Build a blame-free culture: reward transparent reporting, don't punish honest mistakes

Source: Microsoft Security Blog, April 2026 | Community IT Innovators, 2025

3 Email & Endpoint Protection

Stop malicious content before it ever reaches an inbox

62%

of all phishing attempts were AitM attacks from one criminal platform (Tycoon2FA)

- Tycoon2FA compromised ~100K orgs: phishing is now an industrial subscription service
- Endpoint Detection & Response (EDR) monitors devices 24/7 with behavioral analysis
- EDR is working: ransomware encryption rates slowed to 7% growth as detections improve
- Implement DMARC, DKIM, SPF, and use external email banners as a visual reminder

Source: Microsoft Security Blog, April 2026 | Community IT Innovators, 2025

4

Tested Data Backups

Your ultimate failsafe, but only if the restore actually works

82%

of ransomware incidents now involve large-scale data exfiltration before encryption (MDDR 2025)

- Ransomware has shifted: attackers steal your data first, then encrypt for double leverage
- Regularly simulate data restoration. Untested backups are not backups at all
- Gold standard: 3-2-1 (3 copies, 2 media types, 1 offsite/cloud) on automated schedules
- Know your recovery time objective: how long can your mission afford to be offline?

Source: Microsoft Digital Defense Report, 2025 | US-CERT / CISA

5

Zero-Trust Architecture

"Never trust, always verify": assume the breach has already happened

96%

of enterprise permissions go unused. Each one is dormant attack surface

- Research shows 96% of granted permissions are never exercised. Enforce least-privilege access
- Attackers now target workload/non-human identities as phish-resistant MFA strengthens for humans
- Start with IAM: validate every user and device continuously, not just at login
- Segment your network so one compromised account can't reach everything

Source: Oso & Cyera, 2026 | Microsoft Digital Defense Report, 2025

The AI Dilemma

How hackers weaponize AI, and how you can use it defensively

How Hackers Weaponize AI

01

Hyper-Personalized Phishing

AI phishing hits 54% click-through vs. 12% traditional, a 450% increase. AI is embedded across the full attack lifecycle, not just volume, but precision.

02

Deepfakes & Voice Cloning

Scammers clone executive voices from seconds of public audio to authorize fraudulent transfers. $25.6M stolen in one case. AI-generated IDs up 195%.

03

Automated Social Engineering

AI powers real-time “smishing” and new techniques like “ClickFix” (47% of observed initial access methods), adapting in real time.

Sources: Microsoft Security Blog, April 2026 | Microsoft Digital Defense Report, 2025 | CNN, Arup deepfake, 2024

Safely Leveraging AI

THE OPPORTUNITY

- Eliminate “dither”: repetitive admin tasks (summaries, newsletters, formatting)
- Reinvest the “dividend of time” into high-value relationship building
- Analyze network data in real time for proactive threat detection
- Automate alert triage so your team focuses on what matters most

THE GUARDRAILS

Without clear policies, staff may feed sensitive data into public AI models, creating new vulnerabilities while trying to innovate.

Microsoft warns: the agent ecosystem will become the most attacked surface in the enterprise. AI agents inherit user permissions and systematically access everything they're allowed to touch, at machine speed. With 96% of permissions dormant, that's a massive attack surface activated overnight.

Sources: Microsoft Security Blog, April 2026 | Oso & Cyera, Least Privilege Research Report, 2026

Your AI Acceptable Use Policy

THE “TRAFFIC LIGHT” DATA SYSTEM

GREEN: Safe to Use

Public information, general research, non-sensitive content.

YELLOW: Caution

Internal reports with no personal info. Review before sharing.

RED: Never in Public AI

Donor names, health data, financial spreadsheets, member PII.

HUMAN-IN-THE-LOOP

All AI outputs must be reviewed by an expert for accuracy, bias, and tone before external use.

TRANSPARENCY

Disclose the use of AI in externally facing content to maintain community and donor trust.

Culture & Your 30-60-90 Day Roadmap

Making security a shared responsibility, and leaving with a plan

Creating Awareness Without Fatigue

Frame cybersecurity as a partnership, not a policing effort. Make every employee a risk manager.

Address Shadow AI

Acknowledge that “Shadow AI” happens because staff want to work efficiently. Build approved alternatives rather than just banning tools.

Reward Transparency

Build psychological safety by rewarding employees who report mistakes or ask about new tools. Never punish honest errors.

Tie Security to Mission

Protecting data means protecting the vulnerable communities you serve. Make that connection explicit and personal.

Integrate Into ERM

Embed cybersecurity into Enterprise Risk Management and team communications, not siloed as an IT issue.

“ A policy that arrives before trust is a document no one follows. ”

Your Cybersecurity Pathway

MONTH 1
Assess & Baseline

- Appoint executive "owner"
- Conduct rapid risk assessment
- Survey staff for Shadow AI usage
- Activate MFA organization-wide
- Ensure basic spam filtering active

MONTH 2
Policies & Training

- Draft IT Acceptable Use Policy
- Publish AI Usage Policy (Traffic Light)
- Launch security awareness training
- Create approved AI tools list
- Establish incident response plan

MONTH 3
Testing & Assurance

- Upgrade high-risk roles to FIDO keys
- Conduct threat modeling "fire drill"
- Test backup restore capabilities
- Consider third-party security audit
- Schedule quarterly review cadence

Key Takeaways

- ✓ Conduct a rapid cybersecurity risk assessment specific to your association
- ✓ Implement the Big 5 security measures: maximum protection for minimum investment
- ✓ Create an organizational culture of security among staff, volunteers, and board
- ✓ Develop AI usage policies using the Traffic Light system to protect member data
- ✓ Start today with a customized 30-60-90 day security improvement roadmap (pym.cp.tech)

“ A well-trained workforce fosters a culture of security and strengthens the organization’s overall resilience. ”

Questions & Discussion

What's your organization's biggest cybersecurity concern right now?

Protect Your Mission.

Start Today.

Adam Jones
Director of Technology
Creative Planning Business Services

866-CREATIVE | CREATIVEPLANNING.COM

FREE RESOURCE

Cybersecurity Risk Assessment Checklist

pym.cp.tech