

NONPROFIT LEADERSHIP CENTER · LOCK YOUR DOORS! WEBINAR

Nonprofit Operational IT & Cybersecurity

Questions to Ask Your Team, and What to Do About the Answers

OCTOBER 21, 2026 · TAYLOR DEGEARE, VINE IT & CYBERSECURITY

Today's session covered five areas of operational risk: people, email, hardware and networks, data, and artificial intelligence (AI). This document is the takeaway. Bring the questions back to your team this week. Where you get quick, confident answers, you're in good shape. Where you don't, that's where to focus first.

1 PEOPLE

RECOMMENDATIONS

- ☐ Keep one written list of every system each person has access to, including staff, volunteers, and board members. Use it as your onboarding and offboarding checklist.
- ☐ Review that list whenever a board term ends or a volunteer role changes hands, not just when staff leave.
- ☐ Turn on multi-factor authentication (MFA) everywhere it's available, not just email.
- ☐ Provide the organization a password manager so nobody reuses passwords across systems. Vine uses Keeper.
- ☐ Turn on sign-in monitoring for unusual locations and times. It's often already included in Microsoft 365.
- ☐ Know whether your files live on an office server or in the cloud, and who is responsible for each.
- ☐ Standardize on organization-controlled and protected devices, not just protected connections.
- ☐ Run cybersecurity awareness training quarterly, not annually, with leadership and board visibly participating. Vine uses Huntress Security Awareness Training (SAT).

QUESTIONS TO ASK YOUR TEAM

- ? How do staff, volunteers, and board members get access, and how quickly is all of it removed when they leave?
- ? How are passwords created and stored, and is MFA turned on for everyone, on everything?
- ? How are remote staff and volunteers accessing organization data, and from where?
- ? Are we doing any cybersecurity awareness training? If not, how do we start?

2 EMAIL

RECOMMENDATIONS

- ☐ Put a written rule in place: no wire, payment, grant disbursement, or change to payment or donor giving details without a phone call to a number you already had on file, not one in the email.
- ☐ Add filtering beyond whatever came bundled with your email. Vine uses IRONSCALES.
- ☐ Put something in place that monitors mailbox behavior after delivery, in case something slips past the filter. Vine uses IRONSCALES and Huntress Identity Threat Detection and Response (ITDR).
- ☐ Run ongoing, unannounced phishing simulations using nonprofit-targeted lures, like fake grant portal notices. Anyone who clicks gets immediate training. Never punish the click. Vine uses Huntress SAT.
- ☐ Write a one-page incident response process for email compromise, with four named roles.

QUESTIONS TO ASK YOUR TEAM

- ? If someone got into one of our email accounts today, how quickly would we know?
- ? What's the process if that happens, and who is responsible for what?
- ? Do we have advanced email filtering, or just whatever came bundled with our email?
- ? Do we run phishing simulation campaigns for our team, and if not, how do we start?

3 HARDWARE & NETWORKS

RECOMMENDATIONS

- ☐ Assign one person or partner to be accountable for updates across every machine, with a way to verify it's actually happening.
- ☐ On the Microsoft 365 nonprofit grant, confirm MFA and advanced filtering are actually turned on.
- ☐ Confirm you have a business-grade firewall that is actively managed and periodically reviewed, not just the box the internet provider dropped off.
- ☐ Run endpoint detection and response (EDR) rather than antivirus alone, with a named person or partner who responds when it flags something. Vine uses Huntress EDR with managed detection and response, or MDR.
- ☐ Build the Friday-restart habit across the organization. It's free, and it's when updates actually install.
- ☐ Get a list of every computer and network device, its age, and its support end date. Replace on a budgeted schedule, not on failure.

HARDWARE & NETWORKS, CONTINUED

QUESTIONS TO ASK YOUR TEAM

- ? Who owns making sure updates get installed on every computer, and how do they verify it?
- ? Do we have a business-grade firewall, who manages it, and when did anyone last review it?
- ? Are our computers running EDR or just antivirus, and who responds when it flags something?
- ? Are people actually restarting their machines at the end of the week, or just shutting down?
- ? Is our nonprofit Microsoft 365 grant set up with MFA and advanced filtering, or just the base version?

4 DATA

RECOMMENDATIONS

- ☐ Back up Microsoft 365 or Google Workspace with a third-party tool, separate from the provider itself. Vine uses Dropsuite.
- ☐ Test restores on a schedule. Ask to see a real file recovered, not just a report that says the backup ran.
- ☐ Confirm at least one backup copy is immutable, meaning it can't be deleted or altered even by a compromised account.
- ☐ Build in redundancy: more than one copy, in more than one place, with at least one out of reach from inside your own systems.
- ☐ Write a one-page incident response plan with four named roles, including who notifies donors and stakeholders. Put a date on it, review it annually, and make sure your board has seen it.

QUESTIONS TO ASK YOUR TEAM

- ? Is our Microsoft 365 or Google environment backed up by something separate from the provider, and how far back can we go?
- ? Are our backups actually tested with real restores, and could someone delete them if they got into our systems?
- ? Do we have a written incident response plan, could someone here describe it, and has the board seen it?
- ? If we lost access to everything tomorrow morning, how long until we're working again?

5 ARTIFICIAL INTELLIGENCE

RECOMMENDATIONS

- ☐ Have a no-consequence conversation with your team about what AI tools they're already using.
- ☐ Write an organization-wide AI usage policy: approved tools, allowed uses, and what information can never go in, especially donor and beneficiary data. Get everyone to sign it.
- ☐ Pay for business-tier accounts of approved tools rather than leaving people on free consumer versions.
- ☐ Ask whether your filtering, EDR, and monitoring have kept pace with AI-driven attacks, or if you're defending today's threats with yesterday's tools.

QUESTIONS TO ASK YOUR TEAM

- ? What AI tools is our team currently using, and are they on free or business accounts?
- ? Is there any policy about what information can go into them?
- ? Are the tools protecting us keeping pace, or are we defending today's attacks with yesterday's technology?

START HERE

- ☐ Confirm multi-factor authentication is turned on everywhere, not just email.
- ☐ Write the phone-call rule for payments, grant disbursements, and giving changes.
- ☐ Confirm your Microsoft 365 is backed up by something other than Microsoft.
- ☐ Build the Friday-restart habit.

Nothing in security gets you to zero. The goal is a clear picture of where your organization's exposure sits today, and a plan for what happens if something still gets through.

Vine IT & Cybersecurity is a Key Partner of the Nonprofit Leadership Center and works with nonprofits and professional service firms across Tampa Bay, St. Petersburg, and Nashville. Reach out to Taylor DeGeare for a conversation about where your organization stands today.

Taylor DeGeare | tdegeare@vineit.com | (727) 482-4873