

CYBERSECURITY READINESS FOR NONPROFITS

Community IT Innovators Playbook

Revised October 2026

CommunityIT Innovators®

Table of Contents

Introduction 03

Our Approach 05

Cost Estimates 07

Foundational 08

Optimized 16

Proactive 20

Cybersecurity Service Options 24

Summary 25

The challenge for a nonprofit organization is to develop an appropriate cybersecurity plan that:

- Allows them to manage the security of their data and staff,
- Engages their staff with sensible practices as an important line of defense,
- Understands risks,
- Acknowledges external compliance requirements,
- Keeps costs in line.

Whether hiring a Managed Service Provider (MSP), using an in-house IT Department, or using both, organizations need to establish a good foundation of IT policies along with proactive cybersecurity practices. Navigating the maze of cybersecurity solutions and services can be daunting. It's important to partner with a vendor that understands the unique challenges that nonprofits face.

Community IT Innovators has focused on supporting nonprofits to achieve their mission through the effective use of technology since our founding in 1993. Due to our deep commitment to the sector, Community IT has developed a robust set of capabilities when assessing, implementing and managing cybersecurity solutions for nonprofit organizations.

Our unique perspective on supporting nonprofits allows us to provide cybersecurity solutions that are aligned with the unique culture and needs of your organization.

This Playbook explores the Community IT Innovators approach to cybersecurity readiness for nonprofits.

Author

I'm very pleased to present this completely revised Cybersecurity for Nonprofits Playbook. The cybersecurity world has come a long way since we first released a Playbook for our community in 2016 and this update reflects new threats and new tools to mitigate risks. However, our underlying approach remains rooted in our knowledge of the nonprofit community and our eight-point framework to best address your risks. This playbook provides helpful levels of cost-effective solutions for any budget, from Foundational and Optimized through Proactive.

Community IT supports approximately 8000 staff across 185 nonprofit organizations. While founded in the DC Metro area, we have been supporting nonprofit organizations remotely nationwide since before the pandemic. This expansion of our geographic reach allows us to incorporate best practices from a broader cross section of the country in this Playbook.

As the Chief Technology Officer at Community IT, I am responsible for shaping Community IT's strategy around technology to be secure and productive. With a deep background in network infrastructure and a broad perspective developed from supporting hundreds of organizations, I keep technology working and interoperating both in the office and in the cloud for our clients.

I am a frequent speaker on technology and cybersecurity topics in a range of venues. You can read more about Community IT's Cybersecurity offerings here.

I join the entire Community IT team in believing that all nonprofits deserve cybersecurity and that cybersecurity best practices are within your reach, no matter what level you are starting from. Cybersecurity doesn't need to be expensive or complex, but it does require intentionality and broad adoption.

You don't need to have the perfect plan in place; you just need to start. There are many different free tools and roadmaps available. However, having an unused plan on the shelf doesn't protect your organization.

A risk assessment will show your organization the optimum investment in preventing catastrophic cybersecurity incidents, and many little changes can add up to a big protective layer around your mission and goals.

Cybersecurity is always evolving as the threats evolve. We hope you will revisit this Playbook regularly, share it with your executive team, incorporate it into your IT strategic planning roadmap, and keep in touch with me for updates and advice.



CommunityIT Innovators®

Matthew Eshleman
Chief Technology Officer
Community IT Innovators

Introduction

We live in a world with constantly increasing cybersecurity risks. Recent years have seen a dramatic increase in the change and innovation of the technology tools available to mission driven organizations. At the same time, tools like Artificial Intelligence (AI) available to cyber criminals have also grown in sophistication and decreased in cost.

IT systems can no longer be protected by a firewall at the edge of a network, as very few of us work in a traditional office with a server closet and an office firewall. The boundaries of the organization's IT systems are now our home offices and local coffee shops. The new security perimeter is now represented by each individual's online identities and devices.

It is a commonly held misconception that nonprofits are not targeted because of their size or the relative unimportance of their data and can safely "fly under the radar." As attacks have become automated, AI tools help write compelling phishing emails, and hacking software is now cheap and readily available, every computer and device is now a potential target. In addition, the trusted identity of a nonprofit can be used to target other partner organizations, board members, volunteers and donors.

Microsoft's 2025 Digital Defense Report and a 2025 analysis by BDO show that nonprofit organizations continue to face significant cybersecurity risk, and that AI is changing the nature of that risk. Their research reveals that:

- **AI-driven phishing campaigns are now three times more effective than traditional phishing.**[1]
- **28 percent of breaches investigated by Microsoft's Incident Response team began with phishing or social engineering, 18 percent through unpatched web assets, and 12 percent through exposed remote services.**
- **Nonprofits saw a 30 percent year-over-year increase in weekly cyberattacks, and 68 percent of breaches involved a human element such as phishing or user error.**[2]

The threat landscape continues to change. When we delivered this roadmap in 2021, we referenced that 94% of the account compromises were against user accounts that lacked MFA. In our most recent report, we saw that shift dramatically. Over 85% of our clients have enrolled in MFA. Now we see that the ratio of compromised accounts mirrors the MFA enrollment. Attackers are using sophisticated frameworks to steal sessions protected by MFA.[3] Meanwhile, AI has changed what we're seeing on the front lines: in our 2025 data, malicious endpoint activity, viruses and malware that make it past initial defenses, rose nearly fivefold year over year, from 13 incidents to 57. We believe AI tools are helping attackers write new malicious code faster and lowering the technical skill needed to deploy it.[4]

1 https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2025
2 https://www.bdo.com/insights/industries/nonprofit-education/the-crucial-role-of-cybersecurity-for-nonprofit-organizations-in-2025
3 https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/
4 https://communityit.com/webinar-2026-cybersecurity-incident-report-with-matthew-eshleman/

AI and Your Nonprofit's Cybersecurity: Three Things to Know

Artificial intelligence has changed the cybersecurity landscape for nonprofits in three important ways. Understanding all three will help you use this Playbook well.

1

AI has made attackers more effective. The scam emails, fake websites, and malicious code that used to take real skill to produce can now be generated quickly and convincingly by AI tools, in your recipient's language, in your funder's tone, without the spelling errors that used to give phishing away. The fundamentals in this Playbook, especially phishing awareness and email protection, matter more than ever, not less.

2

Your staff's own AI use can create new risk. Well-meaning staff using free AI tools to draft grant reports, summarize donor data, or speed up their work can unintentionally expose sensitive information, if they don't understand the difference between a free consumer tool and a protected enterprise one. This is a policy and training issue as much as a technical one.

3

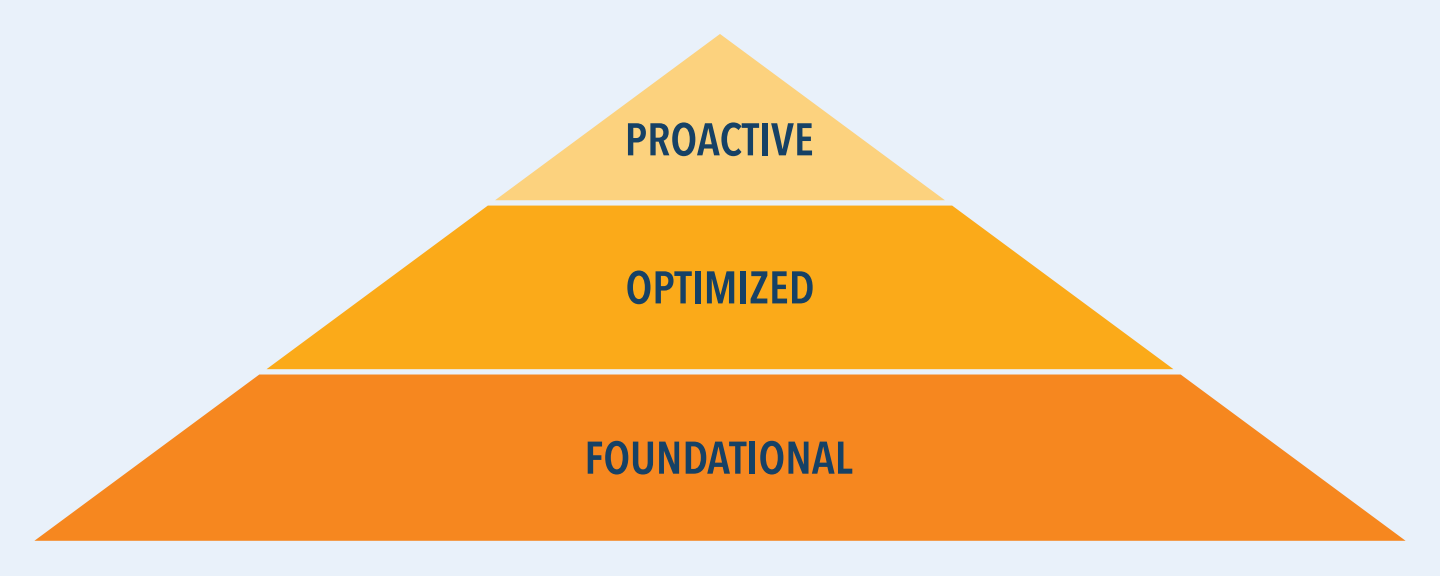
AI can also help under-resourced nonprofits become more secure. The same tools that create new risks can help you close gaps: summarizing vendor terms and conditions you don't have time to read closely, helping draft or update policies, and flagging vulnerabilities you might otherwise miss. Used thoughtfully, AI can help a small IT team or a solo "accidental techie" do more than they could before.

Throughout this Playbook, you'll see AI called out where it changes our recommendations.

Our Approach

Our approach recognizes the unique operating environments of small to mid-sized nonprofit organizations. These security controls are designed to focus on addressing the most common attacks facing nonprofit organizations.

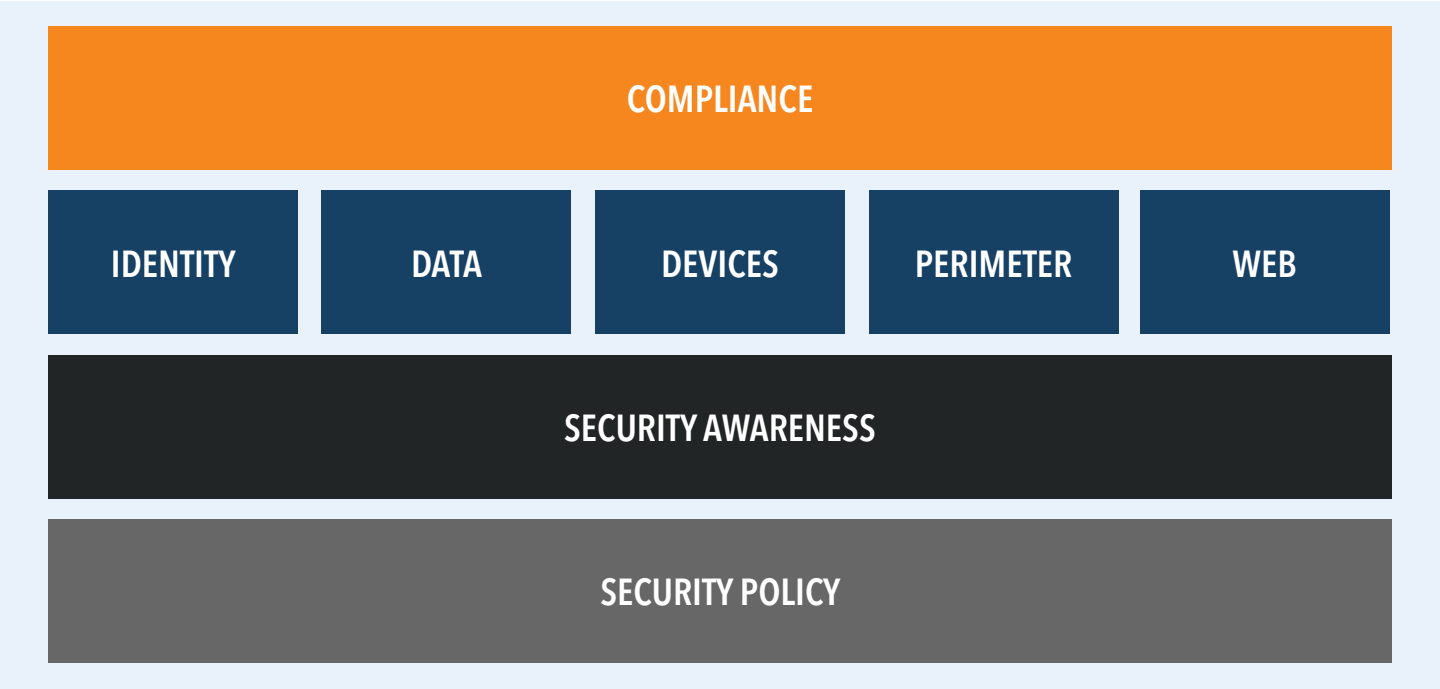
In this Playbook we have created three levels of cybersecurity goals and practices. Every nonprofit should strive to achieve foundational must-haves, and then may follow our suggestions on optimized and proactive solutions.



Our approach takes a people-centric approach and recommends investing in people and processes first. Ensuring that your organization has clear and well-defined policies and has invested in equipping staff to identify the most common threats provides a much better return on investment than spending a lot of money on one-time scans or sophisticated security products that need updating as attacks evolve.

We add to our approach a filter recognizing your organization's capacity to change, need to prioritize, and budget. Many of our suggestions are free or low-cost; we believe strongly that prioritizing cybersecurity best practices is a cultural investment and does not have to be expensive to be valuable. That is, successful cybersecurity awareness takes leadership and prioritization as much, or more than, funding.

Community IT has developed a tailored approach to evaluating and rating any organization's security controls in eight different areas illustrated here. These areas are rooted in the standards-based approach defined by NIST (National Institute of Standards and Technology) Cybersecurity Framework and the Center for Internet Security's 18 Critical Security Controls. We have adapted these large-enterprise and government institutions' standards-based approaches, which do not easily scale down for small to mid-size organizations (between 25-500 staff seats).



Policies and Security Awareness Staff Training form the solid foundation for your nonprofit's security. The concepts illustrated in the layer of blue boxes – Identity, Data, Devices, Perimeter, and Web - are also necessary for a basic defense. AI is increasingly infused into the technology elements of the blue solutions and should not be considered a separate category. Finally, Compliance caps your cybersecurity strategy; typically for organizations that need to adhere to a specific framework due to a funder requirement. These compliance frameworks provide a comprehensive framework of controls to implement. We find that organizations typically don't go down this road unless compelled to and instead focus on those protections that provide the best return on investment. What process do you have in place to monitor compliance with your expectations, policies, and technologies – to ensure that your defenses do not have gaping holes inviting hackers in?

See "AI and Your Nonprofit's Cybersecurity" on the page four for the three ways AI affects your security posture.

Beginning with these eight areas, our Playbook provides foundational must-haves, and then suggestions on optimized and proactive solutions. You have to walk before you can run. Knowing that many smaller and mid-sized nonprofits may be starting to build cybersecurity policies from the ground up, this Playbook will help you build the foundation on which you can begin to be proactive and then optimize your security approach.

Once you have read the Playbook, you may be ready to get to the foundational level. We have created a companion download "Start Here: Nonprofit Cybersecurity Basics" to help you.

Cost Estimates

To help provide some context to these recommendations we've assigned a scale from $-$$$$. These aren't exact and every situation is different. The cost model is intended to reflect the service, and people costs for what a 25-person organization would incur over the course of a year.

$	$0 - $2,000
$$	$2,000 - $8,000
$$$	$8,000 - $15,000
$$$$	$15,000+



Foundational

IT Security Policies[5] provide and document the foundation on which the organization can build, design and analyze security solutions.

- **IT Acceptable Use ($)** is the first policy an organization often defines. Our template includes information such as password policy, data retention policy, system inventory, social media policy and expectations around how work (or BYOD (Bring Your Own Device)) devices are to be handled. You can find many templates online that you can adapt to your own organizational needs. This policy should also be included in your employee handbook.
- **Data Privacy ($$)** Most nonprofit organizations have some sort of system to track either people they serve or people whom they raise money from, and often both. This policy would include elements of how both are handled. It would also address some elements of formal compliance requirements such as HIPAA, GDPR or PCI. Increasingly, this policy also needs to address how staff can use AI tools with this data; for example, prohibiting client- or donor-identifying information in free, consumer-grade AI tools, and requiring that any AI tool touching sensitive data carry enterprise-level data protection terms. This policy should also address data retention: how long you keep information and when you delete it. AI tools have made it dramatically easier to search, summarize, and surface old content across your systems, so information you assumed was effectively buried by time or disorganization can now be found and used, whether by your own staff's AI tools, by an attacker who gains access, or in response to a legal request.
- **AI Acceptable Use Policy ($)** Organizations need to take an intentional approach to adopting AI Solutions. Many SaaS applications are adding in AI tools and enabling them by default. Take the step of disabling AI tools by default and decide, as an organization, how you are going to adopt and use these tools. We have a template to help you get started.[6] Staff are often already using free AI tools on their own, whether or not there's a policy in place, so decide, as an organization, which tools are approved for use with sensitive data.
- **Backup and Disaster Recovery ($)** A policy that defines the organizational data that exists, how it's protected outside of the production system and how long it will take to restore in the case of intentional or accidental deletion or corruption. You can find many templates online that you can adapt to your own organizational needs.

5 https://communityit.com/webinar-making-it-governance-work-for-your-nonprofit/
6 https://communityit.com/template-acceptable-use-of-ai-tools-in-the-nonprofit-workplace/

- **Incident Response ($)** This policy[7] outlines the process that an organization would follow when a cybersecurity incident is suspected. This typically includes multiple elements and stakeholders and would have elements of identifying the potential breach, responding to the incident, notifying impacted stakeholders and remediating the issue.
- **Cyber Insurance ($)** Cyber insurance is one lever driving attention to cybersecurity policies and practices at nonprofits. It is fair to say most nonprofit organizations must comply with basic controls to meet insurability requirements. Inquiring with your broker about coverage and policy options involves analyzing risks and requires executive team involvement. Insurance brokers have also improved their support for nonprofits following a breach or incident, and their contact number should be first or second on your response plan. Find a broker who understands both cyber insurance considerations and nonprofit operations.

  AI is quickly becoming part of this conversation too. Insurers are beginning to ask nonprofits how they use AI tools and what guardrails are in place, much the way MFA became a standard underwriting question a few years ago, and some carriers now offer affirmative AI coverage endorsements that explicitly define what's covered. A good deal of cyber liability is centered around the cost of remediation. Having a documented AI Acceptable Use Policy may increasingly factor into your insurability, not just your security.[8]



7 https://communityit.com/how-to-create-a-nonprofit-incident-response-plan/
8 https://communityit.com/podcast-nonprofit-cybersecurity-insurance-updates-with-jenna-howard/

Security Awareness ($) Basic, ongoing, required security training and education is critical.

There is now a wealth of resources for organizations looking to enhance their security readiness. Community IT has free videos on staff training available on our website[9] along with our other cybersecurity content.

Building an AI-Literate, Security-Aware Culture

Your staff are already using AI tools, whether or not you have a policy in place. The way your organization talks about AI, openly or not at all, is itself a security factor. A few things we've seen work at nonprofits navigating this well:

- **Be intentional, not reactive.** Decide as an organization how you want to adopt AI rather than letting it happen by default through whatever tools are bundled into your existing software. Our Mission-Aligned AI Adoption Model can help you think this through.[10]
- **Talk about it often, and openly.** Treat your AI policy as a living conversation, not a one-time document. Staff will have wildly different levels of AI comfort and experience; frequent, casual check-ins surface the tools people are already using (and the risks that come with them) long before an annual policy review would.
- **Make it safe to ask "dumb" questions.** Uneven AI literacy across your staff is itself a security risk; someone unsure how a tool handles data is more likely to overshare if they're afraid to ask first. A culture where questions are welcome closes that gap faster than any policy can.
- **Name an owner.** Someone should be responsible for coordinating AI policy, professional development, and expectations across teams, the same way you'd designate an executive to own compliance. Without an owner, AI guidance tends to live in scattered messages instead of shared practice.

9 https://communityit.com/webinar-cybersecurity-training-for-nonprofits/
10 https://communityit.com/blog-mission-aligned-ai-adoption-model-for-nonprofits/

Remote Work and Cybersecurity

At Community IT, we have supported nonprofits as they have moved to the cloud and helped enable remote workers to use their own devices for remote work for years. We know that there isn't a one-size-fits-all solution for remote support that works.

Organizations worry about getting up to speed on the technology to support staff and the cybersecurity to protect them. We've found that many nonprofit organizations have already made moves to not just allow remote work but actually embrace remote workers and develop a supportive culture.

We created this Nonprofit Guide to Remote Work full of remote work tips to assist our community as you utilize free and low-cost solutions to work more effectively. And we always consider cybersecurity concerns front and foremost as we help our clients and community work successfully from home.



Identity, Data, Devices, Perimeter, Web

This layer of the framework is where most cybersecurity approaches begin and end. While critical, the technology layer is, in our view, only one layer of a comprehensive approach in the nonprofit environment.

Identity

- **Multi-Factor Authentication ($)** Also referred to by its acronym, MFA, this method of protection asks users who log into a system to provide something that they know, their password, and something they have, usually a smartphone app or a physical security key. Using MFA provides an extra layer of security so that if your password is stolen or compromised, the bad guy still needs to get your device in order to successfully login. Staff with access to privileged information at an organization such as Finance, IT and HR should move to so called "phish resistant" MFA, which commonly uses a passkey. A passkey is a modern authentication method that uses public key cryptography to connect your login with the approved device that was used to register the session. Many different technologies support this including Windows Hello, TouchID, Microsoft Authenticator, many password managers along with FIDO security keys.

  We recommend phish-resistant MFA for all staff where possible. AI has made session-theft attacks (where a hacker steals an active login rather than a password) easier to execute at scale, which is part of why we've raised our recommendation beyond standard app-based MFA. If budget or change-management makes an all-staff rollout difficult, prioritize staff with access to privileged information, such as Finance, IT, and HR, first. Yubico's Secure It Forward program donates physical security keys to nonprofits working in human rights, press freedom, election integrity, or diversity in tech; check their eligibility criteria to see if your organization qualifies.[11]

- **Password Manager ($)** You can use our tips to create an excellent password[12], but you'd be better off using a password generator to automatically generate and store complex passwords for you. Every site you log into should have a unique password so that a compromise of one system won't lead to a compromise of other accounts.

Data

- **Backups ($$)** If data is corrupted or deleted either by accident or intentionally, you'll want a way to get it back. Cloud service providers do include some data protection in their platform, but it is to protect themselves and not you. Make sure that you have data in a third-party solution so that you can meet your org's retention and recovery requirements.

11 https://www.yubico.com/why-yubico/secure-it-forward/
12 https://communityit.com/how-to-create-an-excellent-password/

Devices

- **OS and Third-Party Updates ($)** Out of date software is the cause of 60% of breaches according to the recent ServiceNow survey.[13] Having a reliable and verified patching policy to update not just the operating system, but also third-party applications is a key element of an effective protection strategy. AI enabled hackers are also using threat chaining as a way of connecting multiple software vulnerabilities into a more powerful exploit.
- **Antivirus ($)** AI is changing this cat-and-mouse game on both sides: it's helping attackers generate new malware variants faster than signature-based tools can catch them, but it's also being built into modern antivirus and endpoint detection tools to spot suspicious behavior rather than just known threats. From the PICUS security report, "The IOC-based prevention rate for malware downloads fell to 50% this year, down from 60% in 2025 and 71% in 2024."[14] To be effective, any antivirus solution must be managed and maintained regularly. This means deployment to all org devices and tools to ensure systems have active coverage. Organizations should ensure that this is included in their IT budget and plan.

Perimeter

- **Spam Filtering ($)** Spam is the number one security issue reported to our helpdesk. Help to reduce your support calls by implementing an effective spam filter.
- **Phishing Awareness ($)** Research also indicates that 90% of cybersecurity attacks start with a malicious email. Implementing a third-party email security tool can reduce the number of emails that make it to your end users. Implementing dedicated Security Awareness training can protect your organization by decreasing the likelihood that a staff member will click on a suspicious link. AI has made this training more important, not less.[15] AI-generated phishing emails are well-written, personalized, and often free of the spelling and grammar mistakes that used to be a reliable warning sign.
- **Business Email Compromise Protection ($$)** Also known as spear phishing. This is a scam using traditional confidence scheme techniques combined with email impersonation to extract funds or account access through illicit means. Ever get a spoofed message from your Executive Director asking you to do something right away? That's a good example of spear phishing. Regular spam filtering can't block this, but the good news is that there are several great products that can. Most tools now combine this protection into a single product. AI has made these scams more convincing and, increasingly, more patient: attackers now use AI to sustain a believable exchange over several messages before making a financial ask, rather than relying on one urgent email.

13 https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html
14 https://www.helpnetsecurity.com/2026/08/12/picus-security-blue-report-2026/
15 https://www.knowbe4.com/resource-center/phishing

- **DMARC / DKIM:**[16] There are now some additional acronyms to pay attention to when setting up and managing email. DKIM involves setting a signature on outbound emails to help recipients verify the integrity of a message. DMARC is a complementary control that tells mail systems what to do with messages that don't come from specified IPs or systems. You can look at your organization's DMARC record here: DMARC Record Lookup and Checker | EasyDMARC

Web

- **Secure Website Platforms ($)** Many nonprofits neglect secure website platforms. If you're unsure about your site's defense against malware or ransomware, consider upgrading to platforms like SquareSpace or WPEngine and enforce MFA for all user accounts that have admin access to the site. A website hack can be very expensive and damaging to your brand and fundraising efforts. Prioritize investing in website security.

- **Domain Registration ($)** An organization's domain name is one of its most critical assets. Having a reliable vendor, enabling privacy on the registration and implementing NS level protection can reduce the risk of automated attacks against public websites. Vendors such as Cloudflare provide affordable protection, and even offer certain nonprofits a donation on their service through Project Galileo.

Compliance

Compliance is the ability to demonstrate that the appropriate controls are in place to protect against cybersecurity threats. At the foundational level, prioritizing and investing in monitoring processes to ensure your policies, training, and technology tools are working requires leadership awareness and basic controls.

- **Designate an executive level IT leader** (this does not have to be an IT professional) and invest in their professional development to guide your organizational journey toward cybersecurity. Education and prioritization at this stage will allow your executive leader/s to "own" compliance and create a strategic roadmap to upgrade your organization's approach to cybersecurity.[17]

  The same compliance question, are staff actually following policy, not just whether a policy exists on paper, applies to your AI Acceptable Use Policy too. Depending on your organization's size and structure, that may fall to the same leader who owns broader cybersecurity compliance, or it may make more sense for whoever coordinates your AI policy to own it instead. What matters is that someone is asking the question regularly, not that one person is responsible for everything.

16 https://communityit.com/podcast-email-protection-and-deliverability-with-johan-hammerstrom/
17 https://communityit.com/leadership/



Optimized

IT Security Policy

- **Risk Assessment ($)** Take a free assessment and guided survey provided by Community IT to assess risk based on the NIST Cybersecurity Framework. Understanding your organization's unique risk profile helps to inform the different strategies that can be put into place to protect your organization's data. Community IT provides this tool, and it provides a report and online portal to review and track progress. AI tools can also help you prepare for a risk assessment: summarizing lengthy frameworks like NIST or the CIS Controls into plain language, or helping draft initial policy language based on where your gaps are. The final judgment calls about your organization's risk tolerance should still stay with your team, not the AI tool.

Security Awareness

Basic, ongoing, required security training and education is critical. Invest in security practices training regularly for entry-level employees to executives and board members.
Involve HR in setting requirements and implementing incentives.

This is also the level where AI literacy becomes part of your regular security awareness program rather than a separate, one-off training.

Identity, Data, Devices, Perimeter, Web

Identity

- **Single Sign On ($$)** is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems. SSO is a key element in protecting your organization's digital identity. SSO allows users to sign into other cloud applications using their main identity that they use to access their computer or email. It's more secure because it provides a single management and egress point to administer account access.[18]

18 https://communityit.com/webinar-single-sign-on-sso-for-your-nonprofit-organization/

- **Cloud ITDR ($$)** An organization's digital identity is the most valuable and targeted asset. We've had antivirus on the endpoint for many years. New solutions have emerged that are focused on cloud identity threat detection and response. Many of these tools now use sophisticated AI informed analytics to establish a baseline of normal behavior for each user and flag anomalies such as an unusual login location, an unusual pattern of file access and take preventative action before major data loss can occur.

Data

- **Review data management policies and processes ($$)** to develop a comprehensive cybersecurity strategy and document it. Ensure staff understand and commit to data security throughout the organization, not just in HIPAA or other data areas of extra compliance. The increasing use of AI tools by hackers increases their ability to craft well-articulated emails which have become a real threat. The ability to use AI to generate more and more varied scripts and viruses is also an increasing threat.

- **AI Permissions and Access Review ($$)** As you roll out enterprise AI tools like Microsoft Copilot, Claude or Google Gemini it's important to understand that these tools can search and summarize anything a user already has access to across your organization's files. That means it's worth auditing your permission structures before you deploy them. Content that was effectively protected by being hard to find, an old shared drive, a folder whose permissions were never tightened, is no longer hidden once AI search is turned on. There is no more security through obscurity: review who has access to what, and correct any gaps, before enabling org-wide AI search.

Devices

- **BYOD Control ($$)** When staff can access work resources from personal devices this exposes the organization to additional risk as staff can sync org files, emails and other data to their personal phone or computer. Personal devices often don't have the same level of security controls deployed on them as organization owned devices do. We encourage the use of App Protection Policies to ensure that org data can be managed and deleted when the user leaves the organization.

- **Device Encryption ($)** If your organization has compliance requirements, device encryption may be required. Even if it's not required, encrypting desktops, laptops and phones ensures that organization data is safe if a device is lost or stolen.

Perimeter

- **Endpoint Detection and Response ($$)** goes beyond traditional antivirus to provide detailed forensic analysis, automated response and support for threat hunting. These tools also help meet compliance requirements and can be integrated into other security solutions. Like the Cloud ITDR tools mentioned earlier, many EDR platforms now use AI-driven behavioral analysis to catch novel malware that signature-based approaches would miss.

Web

Web Filtering ($) There has been an evolution of malware that has moved from malicious attachments to being launched through web plugins. Adding a tool that can block your staff from accessing these known malicious websites provides another layer of protection that is not included with standard software.

Compliance

Compliance is the ability to demonstrate that the appropriate controls are in place to protect against cybersecurity threats.

At the Optimized level, prioritizing and investing in your human capital to develop IT expertise should continue as your cybersecurity foundation becomes solid. **Your executive level IT leaders should be comfortable guiding your organizations approach to cybersecurity and insisting on and verifying compliance with policies, training and tools at every level of your nonprofit.**

While there are no industry standard, one-size-fits-all tools to ensure compliance across your organization, designating an executive to "own" compliance should involve budgeting their time and any staff training and meeting time necessary to meet your compliance goals. **This should include checking compliance with your AI Acceptable Use Policy alongside your other cybersecurity policies, not treating it as a separate track.**



Proactive

IT Security Policy

- **Business Continuity Plan ($$)** A Business Continuity Plan is typically developed by an organization's executive leadership, not just IT, and includes information and processes on how an organization will respond to a variety of business risks ranging from localized impact to far reaching.[19] Develop this continuity plan then practice it. This will take dedicated time and prioritization from your leadership team.

  If your organization increasingly relies on AI tools for core operations, anticipate the impact of AI hallucinations and outages into your continuity planning, the same way you'd plan for a cloud provider outage.

Security Awareness

- **Cybersecurity Assessment ($$$)** is a detailed assessment of the current policies, configurations and controls in place at the organization. Includes a detailed report and quantified remediation efforts. An assessment may use a specific compliance framework depending on the business relationship that your organization has with a funder or government agency. Depending on the nature of your mission, even a smaller nonprofit may need to invest in a standards-based assessment to protect your data, your personnel, and your reputation. AI tools can help accelerate parts of this process, summarizing findings or cross-referencing controls against frameworks like NIST or CISv8, but the assessment itself should still involve independent, expert judgment rather than relying solely on AI-generated analysis.

Identity, Data, Devices, Perimeter, Web

Identity

- **Device Trust / Zero Trust ($$)** Most contemporary solutions allow access from any device and from anywhere. All one needs to do is enter a username / password to get in. Device trust is the opposite of that model. Instead of allowing anyone from anywhere on any device to access resources, only trusted devices with trusted users from trusted locations can access organization resources. AI has made this approach more important, not less. AI-generated deepfakes and synthetic identities are increasingly convincing enough to pass basic identity checks, so trusting the device and context, not just the credentials presented, adds a layer traditional login verification can no longer provide alone.

19 https://communityit.com/how-to-create-a-nonprofit-incident-response-plan/

Data

At the proactive level, your organization should have a strong **data management policy** in place. Leadership and staff understand and commit to data security throughout the organization and know what to do in a cybersecurity incident to quickly protect and restore data.

- **Supply Chain Management** As more organizations have fully embraced cloud transformation initiatives, most of an organization's data resides in third party cloud applications. Managing where external data resides and how those partners are handling the organization's data themselves and through third party processors requires additional oversight and management. Establish a policy regarding your vendors and review it annually. This has become more pressing as organizations depend on more third-party platforms, from payroll to cloud storage to learning management systems. When one vendor is compromised, it can become thousands of simultaneous incidents rather than one; a major learning platform breach in 2026 exposed data across thousands of institutions at once. Ask your vendors about their own security practices and incident response plans, not just your own.[20]

Devices

- **CASB / SASE ($$$)** A solution for our modern distributed and cloud architecture, it combines elements of visibility, threat protection, reporting and compliance. While it sounds like marketing jargon run amuck, the acronym actually stands for "Cloud Access Services Broker" and "Secure Access Service Edge." Typically, you would expect to see some sort of device level protection, combined with a secure portal to access approved organization applications. Only compliant devices can access approved applications. CASB tools are also increasingly useful for visibility into "shadow AI," the free AI tools staff may be using without your organization's knowledge or approval, since they can flag cloud app usage outside your sanctioned toolset.

Perimeter/Web

- **Vulnerability Scanning ($$)** These are tools that are used to scan your network internally, externally and your website to identify and report on potential weaknesses. Adding this third-party scanning is helpful to verify that you don't have any gaps in protection and that the patching, updates and configurations that are in place are successful and working. AI cuts both ways here: it's helping scanning tools identify weaknesses in your systems faster and more comprehensively, while also helping attackers scan for the same weaknesses against you. That makes regular scanning more valuable, not less.

20 https://communityit.com/podcast-nonprofit-cybersecurity-insurance-updates-with-jenna-howard/
See also https://www.npr.org/2026/05/08/nx-s1-5815956/canvas-data-breach-school-finals

- **Penetration Testing / Configuration Review($$$$)** These can vary widely in their approach and cost, but they are an exercise that mimics the activity of an adversary that is attacking the network. The pen-tester may deploy some scanning tools inside the network to identify and then exploit weaknesses. The result of the pen test may include a list of the weaknesses exploited and recommendations on how to fix them. Because a pen test is often expensive, organizations should make sure they are investing in all of the previous controls including a thorough assessment, to ensure that the pen test is providing insight into potential configuration gaps or vulnerabilities instead of just identifying the list of solutions that should be in place. Some penetration testers now incorporate AI-driven tools to simulate the kind of automated, AI-assisted attacks your organization is increasingly likely to face in the real world. For organizations that are entirely cloud centric, the traditional Pen Test may be of limited value. Increasingly we're seeing vendors develop cloud configuration review services to assess cloud platforms to ensure that all security best practices are implemented along with the appropriate security roles and permissions assigned to staff.

Compliance

- **SOC / SIEM ($$$):** stands for managed Security Operations Center and Security Information and Event Management tool. An SOC would use the SIEM tool to respond if suspicious activities are detected. In large enterprises, this may be a staffed team internally. For small to midsized organizations these services are most efficiently provided through a Managed Provider. Contemporary SIEM tools can ingest logs from endpoints and servers. They are also able to integrate with the range of cloud solutions to ensure comprehensive visibility into an organization's IT footprint.
- **Compliance Management ($$)** Organizations that have HIPAA Compliance, work with large funders, or receive government funding may need to demonstrate that they have implemented a range of controls from a formal compliance framework such as NIST 800-171 or CISv8. This is a tedious and cumbersome process that can be improved through the adoption of a GRC tool. AI tools can also help here, similar to the Risk Assessment step mentioned earlier, by summarizing framework requirements or drafting initial documentation, though accuracy remains your organization's responsibility, not the tool's.

"The single biggest benefit in using Community IT is feeling confident that we have wrapped our heads and hands around the big [cybersecurity] picture and the details simultaneously. With their expert guidance, we have a handle on where we are, what we still need to improve on, and a roadmap of how to get there with support from CIT.

Matt and the Community IT team are incredibly responsive and able to communicate in a language that non-technical people understand. I know they are on top of all the latest and greatest in the industry, which inspires real confidence in their work along with the knowledge they have our back in keeping us current with best practice... As a small company with big technology management needs, we couldn't be happier with having found CIT. They are affordable AND reliable, and always give the best advice and that produces results."

Sarah Chenven, Chief Operating & Strategy Officer
Credit Builders Alliance Community IT Cybersecurity Assessment Client



Cyber Security Service Options

As a premier MSP working with nonprofit organizations, Community IT is well versed in the threat landscape facing nonprofit organizations, especially those dealing with highly sensitive data. We can provide advanced security consulting and advice.

Our Managed IT Service device management platform for our clients offers a set of **Basic** security features such as automating OS patching, third party app patching, DNS filtering and NextGen Antivirus protection.

Organizations can enhance their protection against the most frequent and high-risk attacks by choosing to add on our **Foundational** or **Comprehensive** Cybersecurity packages. Many of the tools built into these packages, from antivirus to cloud identity protection to email security, now use AI-driven detection to catch threats that older, signature-based tools would miss.

Service Options	Basic Security	Foundational Security	Comprehensive Cybersecurity
Managed Cybersecurity			
Device Update Management	✓	✓	✓
NextGen AV	✓	✓	✓
Web Threat Filtering	✓	✓	✓
Cloud Account Monitoring	✓	✓	✓
Cloud Identity Protection	✓	✓	✓
IT Security Policy		✓	✓
Incident Response Plan		✓	✓
Cloud Based Backup		✓	✓
Multi-Factor Authentication (MFA)		✓	✓
Security Awareness Training		✓	✓
Email Protection		✓	✓
Email Deliverability		✓	✓
External Network Scanning		✓	✓
DarkWeb Scanning		✓	✓
Vulnerability Scanning			✓
Managed Detection & Response			✓
Security Event Management			✓
Annual Security Assessment			✓
Compliance Vendor Scoring			✓
Penetration Testing	***Custom***	***Custom***	***Custom***

✓ ✓ ✓ Included as part of fixed monthly price. You can customize based on your needs.

Custom Customized based on your needs.

Summary

There are lots of cybersecurity checklists out there that provide a range of roadmaps and recommendations to follow. They are only as good as your ability to execute and implement these controls at your organization.

Our Playbook provides a tested roadmap for implementing practical and effective solutions at nonprofit organizations. **Take this document and incorporate it into your annual IT planning process.**[21]

This Playbook is organized to give your nonprofit first- and next-steps at three levels of your cybersecurity readiness: **Foundational, Optimized, and Proactive**. These levels may or may not be related to your lifecycle stage or age as a nonprofit entity; they may be more related to your sector of work, your executive team capacity and your size and previous priorities. Your nonprofit should strive to achieve Foundational cybersecurity status.

At all levels of your cybersecurity development, your organization should have in place: IT Security Policies; Security Awareness; Identity, Data, Devices, Perimeter, and Web protections; and Compliance. And remember the three ways AI factors into your cybersecurity strategy: it's making attackers more effective, it's creating new risks through how your own staff use it, and it can help your organization become more secure even with limited resources. This Playbook addresses all three.

At Community IT we believe that all nonprofits deserve cybersecurity and that cybersecurity best practices are within your reach, no matter at what level you begin.

Your people are your most effective cybercrime prevention team.

Prioritization is key but does not need to be expensive. A **risk assessment** will show your organization the optimum investment in preventing catastrophic cybersecurity incidents, and many little changes can add up to a big protective layer around your mission and goals.

Cybersecurity is always evolving, however, as the threats evolve. We hope you will revisit this Playbook regularly, or talk to us for updates and advice.

21 https://communityit.com/webinar-design-an-it-roadmap-to-create-value/

Ready to reduce cybersecurity risk for your nonprofit?

At Community IT Innovators, we've found that many nonprofit organizations deal with more cybersecurity risks than they should have to after settling for low-cost IT support options they believe will provide them with the right value.

As a result, cyber damages are all too common.

Our process is different. Our techs are nonprofit cybersecurity experts. We constantly research and evaluate new technology solutions to ensure that you get cutting-edge solutions that are tailored to keep your organization secure. We ensure you get the highest value possible by bringing 25 years of expertise in exclusively serving nonprofits to bear in your environment.

If you're ready for nonprofit IT support that addresses cybersecurity risk, let's talk.



CommunityIT Innovators®

Where technology meets mission

www.communityit.com
1110 Vermont Ave NW #900
Washington, DC 20005
connect@communityit.com